

Diskresi Kepentingan Umum dalam Pengecualian Hak Subjek Data Pribadi Berdasarkan Pasal 15 UU No. 27 Tahun 2022: Analisis Parameter Hukum Perspektif *Rechtsstaat* dan *Machtsstaat*

Jose Andreas Maukar^{1*}, Horadin Saragih², Athina Kartika Sari³

^{1,2,3}Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Esa Unggul, Jl. Arjuna Utara No.9, RT.1/RW.2, Duri Kepa, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta
josemaukar@student.esaunggul.ac.id

Abstract

Article 15 of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) permits state institutions to restrict data subjects' rights based on an elastically defined "public interest" clause. Lacking rigid normative parameters and operational boundaries, this semantic ambiguity creates legal uncertainty and enables power abuse. This study critically analyses how this vague clause risks transforming the law from an instrument limiting state power (*Rechtsstaat*) into a tool legitimizing digital absolutism (*Machtsstaat*). Using normative juridical methods—comprising statutory, conceptual, and comparative approaches against Article 23 of the EU's General Data Protection Regulation (GDPR)—this research demonstrates two main findings. First, the absence of definitive criteria for "public interest" enables unilateral self-authorization by authorities without independent judicial oversight. Second, an ideal formulation must adopt strict necessity and proportionality principles, mirroring GDPR's limited scope that restricts exemptions strictly to national security, defense, public safety, serious crime prevention, vital economic interests, and public authorities' supervisory functions. To safeguard the rule of law, this study recommends urgent legal reconstruction through subordinate regulations of UU PDP. These regulations must incorporate three essential safeguards: (1) an objective emergency parameter requiring independent court authorization for data access; (2) rigid time-limitation criteria restricting access duration to the period of necessity, followed by mandatory data deletion; and (3) post-access forensic accountability via independent audits to prevent abuse. Implementing these frameworks is vital to protect the *Rechtsstaat* and prevent the rise of a surveillance state (*Machtsstaat*) in Indonesia's digital era.

Keywords: Public Interest, Personal Data Protection, *Rechtsstaat*, *Machtsstaat*, Judicial Oversight, GDPR, Digital Absolutism.

Abstrak

Pasal 15 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memberikan kewenangan negara mengecualikan hak subjek data atas nama kepentingan umum tanpa definisi normatif yang jelas dan parameter pembatasan yang rigid. Frasa "kepentingan umum" yang elastis menciptakan ketidakpastian hukum dan rentan terhadap penyalahgunaan kekuasaan. Penelitian ini menganalisis secara kritis bagaimana klausul tersebut dapat bergeser dari instrumen pembatasan kekuasaan (*Rechtsstaat*) menjadi alat legitimasi absolutisme digital (*Machtsstaat*). Metode penelitian yuridis normatif menggunakan statute approach, conceptual approach, dan komparasi normatif terhadap Pasal 23 GDPR Uni Eropa. Hasil penelitian menunjukkan: pertama, ketiadaan batasan definitif berpotensi melahirkan self-authorization oleh penguasa; kedua, formulasi kepentingan umum yang ideal harus mengadopsi standar strict necessity dan proportionality. Penelitian ini merekomendasikan rekonstruksi hukum melalui aturan turunan UU PDP yang memuat mekanisme judicial oversight, parameter kedaruratan objektif, pembatasan jangka waktu akses, dan akuntabilitas forensik pasca-akses guna membentengi *Rechtsstaat* di era digital.

Kata Kunci: Kepentingan Umum, Pelindungan Data Pribadi, Diskresi, *Rechtsstaat*, *Machtsstaat*, Judicial Oversight, GDPR.

Copyright (c) 2026 Jose Andreas Maukar, Horadin Saragih, Athina Kartika Sari

✉Corresponding author: Jose Andreas Maukar

Email Address: josemaukar@student.esaunggul.ac.id (Jl. Arjuna Utara No.9, RT.1/RW.2, Duri Kepa, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta)

Received 19 May 2026, Accepted 25 May 2026, Published 31 May 2026

PENDAHULUAN

Negara Republik Indonesia sebagai negara hukum (*Rechtsstaat*) meletakkan asas legalitas, pembatasan kekuasaan, dan perlindungan hak asasi manusia (HAM) sebagai fondasi konstitusional. Hal

ini tertuang dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945), yang menegaskan bahwa Indonesia adalah negara yang berdasarkan atas hukum, bukan sekadar berdasarkan atas kekuasaan (negara kekuasaan/Machtsstaat). Konsekuensi logis dari prinsip Rechtsstaat adalah bahwa setiap perluasan kewenangan negara dalam membatasi hak-hak warga negara harus dilandasi oleh ketentuan hukum yang jelas, transparan, dan dapat dipertanggungjawabkan (Stahl, 1870).

Dalam era digital dan big data seperti saat ini, salah satu hak fundamental warga negara yang paling terancam adalah hak atas privasi dan perlindungan data pribadi (Solove, 2004). Hak ini dijamin secara konstitusional dalam Pasal 28G ayat (1) UUD NRI 1945. Perlindungan terhadap dimensi hak asasi ini memerlukan pemahaman mendalam mengenai arsitektur hukum siber nasional yang responsif terhadap dinamika ruang siber (Qurrotuaini, 2024). Seiring dengan meningkatnya pengumpulan, pemrosesan, dan penyimpanan data pribadi skala masif oleh berbagai institusi publik dan swasta, negara dituntut untuk menghadirkan kerangka hukum yang mampu melindungi privasi warga negara tanpa mengorbankan kepentingan publik yang sah (Bygrave, 2014; Wirogioto & Belgradoputra, *in press*).

Transformasi ini memaksa adanya redefinisi kedaulatan siber (*cyber sovereignty*) di tingkat regional, di mana perlindungan data pribadi dan otonomi wilayah saling berkelindan menghadapi ancaman siber global (Amin & Marzaman, 2023; Erlangga et al., 2024). Hak atas privasi tidak lagi dipandang sekadar sebagai hak negatif untuk ditinggalkan sendiri (*the right to be let alone*), melainkan sebuah hak konstitusional yang membutuhkan perlindungan aktif dari negara berdasarkan tinjauan filosofis dan yuridis yang mendalam (Muslim, 2025). Sebagai respons atas kebutuhan tersebut, Indonesia telah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai landasan hukum komprehensif pertama dalam sejarah hukum nasional (Presiden Republik Indonesia, 2022). Kehadiran UU PDP ini menandai babak baru dalam rezim hukum perlindungan data, di mana integrasi antara keamanan data pribadi dan kedaulatan data nasional menjadi pilar utama pembangunan hukum siber (Budhijanto, 2024). Namun, di balik keunggulan regulasi ini, terdapat celah hukum yang serius pada Pasal 15 UU PDP.

Identifikasi Permasalahan (Problem Statement)

Pasal 15 UU PDP mengatur pengecualian terhadap hak-hak subjek data pribadi atas dasar kepentingan umum dalam penyelenggaraan negara. Ketentuan ini membolehkan instansi pemerintah, otoritas publik, dan aparat penegak hukum untuk mengesampingkan hak dasar pemilik data (seperti hak mengakses, memperbaiki, membatasi, atau menghapus data) demi dalih "kepentingan umum" penyelenggaraan negara, pertahanan, keamanan nasional, dan penegakan hukum (Presiden Republik Indonesia, 2022).

Permasalahan fundamental muncul ketika menelaah lebih lanjut frasa "kepentingan umum" dalam Pasal 15 UU PDP. Frasa ini bersifat sangat elastis (*rubber clause*), tanpa disertai definisi yang jelas, parameter operasional yang rigid, atau penjelasan materiil di bagian Penjelasan Undang-Undang.

Ketiadaan batasan normatif yang tegas ini menciptakan ruang diskresi (*discretion*) yang tidak terbatas bagi penguasa, sehingga berpotensi melahirkan:

1. Ketidakpastian hukum (*legal uncertainty*) yang mengakibatkan divergensi interpretasi dan praktek penerapan di berbagai institusi publik;
2. Penyalahgunaan kekuasaan (*abuse of power*), di mana penguasa dapat menggunakan dalih "kepentingan umum" sebagai justifikasi untuk melakukan pengawasan massal, eksploitasi data, dan pengaksesan data pribadi warga negara secara sepihak tanpa mekanisme kontrol yudisial (*judicial oversight*) (Greenwald, 2014);
3. Pergeseran paradigma UU PDP dari instrumen pembatasan kekuasaan (Rechtsstaat) menjadi alat legitimasi absolutisme digital (Machtstaat), di mana negara bertindak secara bersamaan sebagai pemroses data sekaligus pengawas atas tindakannya sendiri (*self-authorization*/otorisasi diri).

Urgensi problematik ini diperkuat oleh realitas empiris tata kelola data di Indonesia. Dalam lima tahun terakhir, negara telah mengalami minimal tiga insiden kebocoran data skala masif yang melibatkan institusi publik:

1. Bocornya 279 juta data BPJS Kesehatan pada 2021 yang mencakup nama, NIK, nomor rekening, dan riwayat kesehatan, yang implikasi serta dampak yuridis jangka panjangnya terhadap kepercayaan publik masih terus menjadi sorotan utama dalam kajian tata kelola data nasional (Nugraha et al., 2025).
2. Serangan *ransomware* terhadap Pusat Data Nasional (PDN) pada 2024 yang mengakibatkan gangguan masif pada layanan publik digital akibat kelalaian administratif dan kelemahan infrastruktur (Dachlan et al., 2025).
3. Kerentanan sistem eHAC (Electronic Health Alert Card) Kementerian Kesehatan yang memungkinkan akses tidak sah ke data pasien COVID-19 akibat lemahnya proteksi terhadap insider threat dan kelalaian teknis (Erlangga et al., 2024; Rendi et al., 2025)

Paradoks yang menyedihkan muncul dari fakta ini: atas nama "kepentingan umum" dan alasan keamanan nasional, Pasal 15 UU PDP memberikan otoritas kepada negara untuk mengakses data warga secara luas dan berkelanjutan. Namun, secara empiris, institusi negara sendiri telah berulang kali gagal mengamankan data yang dikuasainya dari serangan eksternal, *insider threat*, dan kelalaian administratif. Ini menciptakan "dilema kepercayaan digital": warga diminta mempercayai negara dengan data sensitif mereka, sementara negara belum menunjukkan kapabilitas untuk menjaganya. Lebih jauh, paradoks ini diperkuat oleh realitas empiris rapuhnya tata kelola keamanan digital nasional. Insiden-insiden tersebut mengungkap bahwa ketiadaan parameter objektif dalam Pasal 15 menciptakan dua risiko simultan: Pertama, negara mengklaim kebutuhan akses data masif atas nama "kepentingan umum", namun kapabilitas infrastruktur keamanannya sendiri masih lemah. Kedua, tanpa definisi jelas tentang apa itu "kepentingan umum", tidak ada mekanisme untuk memverifikasi apakah data yang dikumpulkan negara benar-benar untuk tujuan tersebut atau disalahgunakan untuk kepentingan administratif/politis yang sempit. Insiden kebocoran BPJS, misalnya, bukan hanya menunjukkan

kelalaian teknis, tetapi juga absensi akuntabilitas hukum dalam pengelolaan data yang dikumpulkan dengan justifikasi "kepentingan umum" (Scheppelle, 2018).

Fenomena ini mencerminkan paradoks hukum yang nyata: UU PDP dirancang untuk melindungi hak privasi warga negara, tetapi Pasal 15-nya membuka pintu bagi negara untuk mengecualikan hak tersebut tanpa pembatasan yang jelas.

Novelty dan Gap Penelitian (Research Gap)

Meskipun UU PDP telah diteliti oleh beberapa akademisi, mayoritas penelitian berfokus pada aspek teknis implementasi dan kepatuhan (compliance). Penelitian yang secara eksplisit menganalisis dialektika Rechtsstaat-Machtsstaat dalam konteks Pasal 15 UU PDP masih sangat terbatas. Lebih lanjut, sejauh ini belum ada penelitian yang melakukan komparasi sistematis antara Pasal 15 UU PDP dan Pasal 23 GDPR Uni Eropa dengan tujuan mengidentifikasi kekosongan normatif dan merekomendasikan rekonstruksi hukum yang konkret. Penelitian ini mengisi kekosongan tersebut dengan memberikan analisis kritis dan rekomendasi praktis untuk aturan turunan UU PDP.

Rechtsstaat dan Machtsstaat: Dialektika Fundamental

Konsep Rechtsstaat (negara hukum) berasal dari tradisi hukum Eropa Kontinental, khususnya dari pemikiran Friedrich Julius Stahl (Stahl, 1870). Rechtsstaat mengandung arti bahwa negara harus mematuhi hukum, bukan sebaliknya. Stahl merumuskan empat elemen esensial Rechtsstaat:

1. Pengakuan dan perlindungan hak asasi manusia (*recognition and protection of fundamental human rights*);
2. Pemisahan kekuasaan (*separation of powers*);
3. Pemerintahan berdasarkan undang-undang (*rule of law/rule-based government*);
4. Peradilan administrasi yang independen (*independent administrative courts*).

Sebaliknya, Machtsstaat (*power state*) adalah kebalikan dari Rechtsstaat. Dalam Machtsstaat, hukum tidak mengikat penguasa; sebaliknya, hukum menjadi instrumen legitimasi dari kekuasaan penguasa (Kelsen, 2017). Carl Schmitt mengatakan bahwa dalam situasi *state of exception* (keadaan darurat), penguasa dapat mengesampingkan hukum untuk melindungi eksistensi negara (Schmitt, 1985). Namun, dalam era digital, "*exception*" ini dapat menjadi "*rule*" (norma), menciptakan apa yang disebut *perpetual state of exception* (keadaan darurat berkelanjutan) (Agamben & Attell, 2005).

Dalam konteks Pasal 15 UU PDP, mekanisme "*perpetual state of exception*" ini beroperasi melalui dua saluran sekaligus. Pertama, frasa "kepentingan umum" yang elastis memungkinkan penguasa untuk membuat klaim "kedaruratan" yang bersifat self-referential (*self-judging*) tanpa verifikasi eksternal. Apakah suatu situasi tergolong "kepentingan umum" ditentukan sepihak oleh instansi yang sama yang menginginkan akses data. Kedua, ketiadaan batas temporal (*time limit*) dalam Pasal 15 berarti pengecualian hak-hak subjek data dapat berlangsung *in perpetuity*, mengubah "*exception*" (pengecualian sementara) menjadi "*rule*" (norma tetap). Kombinasi kedua faktor ini menciptakan apa yang Agamben sebut sebagai "*bare life*" dalam ranah digital: status warga negara di

mana hak-hak privasi mereka dapat dinonaktifkan kapan saja, tanpa batas waktu, dan atas justifikasi yang sepenuhnya ditentukan oleh penguasa sendiri (Agamben & Attell, 2005).

Pasal 1 ayat (3) UUD NRI 1945 menetapkan Indonesia sebagai negara hukum, namun rujukan elastis "kepentingan umum" dalam UU PDP menunjukkan gejala pergeseran menuju Machtstaat.

Dalam konteks siber, penyalahgunaan kekuasaan ini termanifestasi sebagai "kekuasaan tak kasat mata" (*invisible power*) yang mengontrol arus data publik secara sepihak. Oleh karena itu, diperlukan telaah konstitusional yang mendalam serta rekonstruksi model *judicial review* digital di Indonesia untuk menjinakkan dominasi absolut penguasa di ruang siber (Gobel & Muhtar, 2024).

Konsep Diskresi (Discretion) dalam Hukum Publik

Diskresi adalah kebebasan bertindak (*freedom to act*) yang diberikan kepada pejabat publik untuk membuat keputusan dalam situasi tertentu berdasarkan pertimbangan profesional. Dalam teori hukum administrasi negara dan hukum publik, diskresi dapat diklasifikasikan secara mendasar menjadi dua bentuk: (1) *Structured discretion* (diskresi terstruktur), yaitu kebebasan bertindak yang ruang lingkup penerapannya dibatasi oleh parameter normatif dan indikator objektif yang jelas; dan (2) *Unstructured discretion* (diskresi tidak terstruktur), yaitu ruang kebebasan bertindak yang sangat luas tanpa adanya pembatasan normatif yang rigid.

Pasal 15 UU PDP mengandung *unstructured discretion* karena frasa "kepentingan umum" tidak memiliki definisi operasional yang jelas, sehingga berpotensi menciptakan ruang penyalahgunaan kekuasaan (*abuse of power*).

Konsep Kepentingan Umum (Public Interest)

Kepentingan umum adalah konsep fundamental dalam hukum publik, tetapi juga konsep yang sangat elastis. Dalam hukum administrasi, kepentingan umum umumnya didefinisikan sebagai kepentingan kolektif yang melampaui kepentingan individual (Seagle, 1945; Tamanaha, 2006). Di Uni Eropa, GDPR mendefinisikan "kepentingan umum" secara limitatif (*limited definition*) hanya meliputi aspek-aspek keamanan dan pengawasan tertentu, sementara UU PDP Indonesia membukanya secara sangat luas dan seragam.

Teori Tambahan

Dalam rangka memperkuat kerangka analisis normatif dan konseptual, kajian ini juga memanfaatkan beberapa teori tambahan yang relevan dengan isu pembatasan hak dan kekuasaan dalam hukum siber, sebagai berikut:

1. Teori *State of Exception* (Keadaan Darurat) dari Giorgio Agamben: Menganalisis bagaimana penguasa dapat menggunakan frasa-frasa elastis dalam hukum untuk menciptakan "zona abu-abu" hukum, di mana hak-hak fundamental dapat ditangguhkan secara legal (Agamben & Attell, 2005).
2. Prinsip *Strict Necessity dan Proportionality*: Menentukan bahwa pembatasan hak hanya dapat dilakukan jika sangat mendesak (tidak ada cara lain) dan tindakan harus seimbang dengan tujuan yang hendak dicapai.

3. Teori Tujuan Hukum (*Der Zweck im Recht*) dari Rudolf von Jhering: Menekankan bahwa hukum harus mencapai keseimbangan antara kepentingan individual dan kepentingan sosial/kolektif secara adil (Seagle, 1945).

Dalam konteks Pasal 15 UU PDP, teori Jhering memberikan landasan filosofis yang krusial: hukum pengecualian hak subjek data hanya legitimate apabila ia benar-benar mencapai tujuan keseimbangan tersebut. Artinya, klaim "kepentingan umum" yang semata-mata menguntungkan kepentingan birokrasi atau kekuasaan negara tanpa memberikan perlindungan nyata bagi masyarakat luas, secara teleologis bukanlah "kepentingan umum" dalam arti hukum yang sesungguhnya. Jhering menegaskan bahwa hukum adalah alat untuk mencapai tujuan sosial (*Zweck*), bukan tujuan itu sendiri. Oleh karena itu, apabila Pasal 15 UU PDP digunakan sebagai instrumen yang justru merugikan hak-hak kolektif warga (melalui *surveillance* masif atau penyalahgunaan data), maka pasal tersebut telah kehilangan legitimasi teleologisnya sebagai norma hukum yang sah dalam paradigma *Rechtsstaat*.

Penerapan teori-teori tersebut diharapkan dapat memperkaya analisis serta memberikan landasan normatif yang lebih komprehensif dalam mengevaluasi pembatasan hak dalam regulasi yang dikaji.

Integrasi Konsep: Diskresi, Kepentingan Umum, dan Dialektika Rechtsstaat- Machtsstaat

Ketiga konsep ini (*Rechtsstaat-Machtsstaat*, diskresi, dan kepentingan umum) membentuk sebuah kontinum. Pasal 15 UU PDP menciptakan *unstructured discretion* dalam nama kepentingan umum yang elastis, yang memungkinkan pergeseran paradigma dari *Rechtsstaat* menuju *Machtsstaat*. Dalam *Rechtsstaat* sejati, diskresi dalam kepentingan umum harus *structured discretion* — dibatasi oleh kriteria eksplisit, prosedur ketat, dan *oversight* eksternal. Sebaliknya, dalam dinamika *Machtsstaat*, diskresi menjadi institutionalized blank check di mana penguasa sendiri yang mendefinisikan kepentingan umum dan memberi otorisasi kepada dirinya sendiri. Penelitian ini menganalisis bagaimana konstruksi normatif Pasal 15 UU PDP saat ini cenderung mereproduksi pola diskresi tidak terstruktur yang rawan mengundang watak *Machtsstaat*, dan merekomendasikan transformasi menuju *structured discretion* yang sejalan dengan amanat *Rechtsstaat*. Analisis dalam bab-bab berikutnya akan mendemonstrasikan bagaimana mekanisme ini beroperasi dalam tiga dimensi: dimensi normatif (kekaburan bahasa hukum), dimensi prosedural (absensi *judicial oversight*), dan dimensi temporal (tidak ada batas waktu akses).

Tabel Komparasi Pasal 15 UU PDP Indonesia vs. Pasal 23 GDPR Uni Eropa

Pemetaan *unstructured discretion* hukum siber nasional memerlukan analisis komparatif rigid terhadap GDPR Uni Eropa. Sandingan ini vital untuk mengidentifikasi celah institusional dan anomali normatif Pasal 15 secara tajam. Berikut dikotomi struktural sistem hukum tersebut:

Tabel 1. Komparasi Yuridis Pengaturan Pengecualian Hak Subjek Data

ASPEK	PASAL 15 UU PDP INDONESIA	PASAL 23 GDPR UNI EROPA
Definisi "Kepentingan Umum"	Tidak didefinisikan secara eksplisit. Hanya menyebutkan: penyelenggaraan negara, pertahanan, keamanan nasional,	Didefinisikan secara limitatif: keamanan nasional, pertahanan, keselamatan publik, pencegahan/penyelidikan/pendeteksian kejahatan serius, kepentingan

	dan penegakan hukum (tanpa penjelasan operasional).	ekonomi/finansial vital, fungsi pengawasan otoritas publik.
Standar Pembatasan	Tidak ada standar keharusan (<i>necessity</i>) atau proporsionalitas (<i>proportionality</i>) yang eksplisit dalam pasal itu sendiri.	Menggunakan standar STRICT NECESSITY dan PROPORTIONALITY secara eksplisit.
Mekanisme Kontrol	Tidak ada mekanisme <i>judicial oversight</i> (pengawasan yudisial) yang jelas. Penguasa <i>self-authorization</i> (otorisasi diri).	Memerlukan <i>court authorization</i> (otorisasi pengadilan) atau <i>independent oversight</i> untuk akses data dalam " <i>public interest</i> ".
Pembatasan Jangka Waktu	Tidak ada pembatasan durasi akses data. Akses dapat bersifat permanen (<i>indefinite</i>).	Data harus dihapus setelah keperluan " <i>public interest</i> " berakhir (<i>time-limited access</i>).
Akuntabilitas Pasca-Akses	Tidak ada mekanisme audit forensik (<i>forensic audit</i>) independen untuk memverifikasi penggunaan data yang sesuai.	Memerlukan <i>transparency reports</i> dan audit independen tentang penggunaan data dalam " <i>public interest</i> ".
Risiko Rechtsstaat-Machtstaat	TINGGI: Klausul elastis tanpa batasan normatif menciptakan ruang <i>unlimited discretion</i> > Machtstaat.	RENDAH: Definisi limitatif + <i>strict necessity</i> + <i>proportionality</i> + <i>judicial oversight</i> > Rechtsstaat.
Mekanisme Banding/ Remedy bagi Subjek Data	Tidak ada mekanisme khusus bagi subjek data untuk mengajukan banding jika merasa aksesnya tidak justified. Hak gugat masih sangat terbatas dan belum eksplisit dalam regulasi.	Ada right to remedy yang tegas: subjek data dapat mengajukan complaint ke Data Protection Authority (DPA) atau pengadilan jika merasa hak privasi dilanggar. DPA memiliki kewenangan investigasi dan imposing fines yang signifikan.

METODE

Penelitian hukum yang digunakan dalam naskah ilmiah ini adalah Metode Penelitian Yuridis Normatif (Legal Research), yang dikonsentrasikan pada analisis terhadap kekaburan norma, inkonsistensi regulasi, dan ketiadaan instrumen pengawas dalam teks undang-undang siber positif.

Pendekatan Penelitian

Pendekatan penelitian yang digunakan dalam kajian ini dirancang untuk menghasilkan analisis yang komprehensif dan sistematis terhadap permasalahan hukum yang diteliti, sebagai berikut:

1. Statute Approach (Pendekatan Perundang-undangan)

Digunakan untuk menelaah tata urutan vertikal regulasi secara hierarkis dari tingkat konstitusi, teks Pasal 15 UU PDP, Penjelasan UU PDP, hingga aturan turunan siber terkait. Secara operasional, pendekatan ini diterapkan melalui tiga tahap penafsiran: (a) penafsiran gramatikal terhadap kata per kata dalam rumusan Pasal 15 UU PDP, khususnya frasa "kepentingan umum" dan konstruksi "dan/atau"; (b) penafsiran sistematis yang menelaah Pasal 15 dalam konteks keseluruhan arsitektur UU PDP, termasuk relasinya dengan Pasal 4 ayat (2) huruf a; serta (c) penafsiran teleologis yang mengukur sejauh mana rumusan Pasal 15 sejalan dengan tujuan konstitusional Pasal 28G ayat (1) dan Pasal 1 ayat (3) UUD NRI 1945, guna mengidentifikasi konsistensi atau inkonsistensi normatif antarlapisan regulasi.

2. Conceptual Approach (Pendekatan Konseptual)

Dilakukan dengan membedah doktrin-doktrin para ahli hukum global serta konsep fundamental seperti Rechtsstaat, Machtsstaat, diskresi, dan judicial oversight, demi membangun argumentasi hukum pembatasan kekuasaan yang kokoh. Secara operasional, konsep-konsep tersebut diidentifikasi dari literatur hukum primer dan sekunder, kemudian difungsikan sebagai kerangka uji normatif untuk mengevaluasi apakah konstruksi Pasal 15 UU PDP memenuhi atau menyimpangi parameter negara hukum sejati. Empat teori utama yang dioperasionalkan adalah: (a) teori Rechtsstaat-Machtsstaat dari Stahl dan Kelsen sebagai kerangka evaluasi paradigmatis; (b) teori state of exception Agamben sebagai lensa analisis kekaburan norma; (c) teori tujuan hukum (*Der Zweck im Recht*) Jhering sebagai landasan uji legitimasi teleologis; serta (d) prinsip strict necessity dan proportionality sebagai parameter batas diskresi yang sah.

3. Comparative Legal Analysis (Analisis Hukum Komparatif)

Melakukan komparasi sistematis secara sinkronik tekstual dengan menyejajarkan Pasal 15 UU PDP Indonesia terhadap Pasal 23 General Data Protection Regulation (GDPR) Uni Eropa yang diakui sebagai standar emas (golden standard) perlindungan data global (European Data Protection Board, 2024; Official Journal of the European Union, 2016). Secara operasional, perbandingan dilakukan terhadap lima dimensi analitis yang terstruktur: (a) definisi kepentingan umum, (b) standar pembatasan hak subjek data, (c) mekanisme kontrol yudisial, (d) pembatasan jangka waktu akses dan retensi data, serta (e) akuntabilitas pasca-akses. Pemilihan GDPR sebagai objek komparasi didasarkan pada posisinya yang diakui oleh komunitas akademik dan regulatoris internasional sebagai sistem perlindungan data yang paling komprehensif, limitatif, dan terstruktur secara normatif.

Ketiga pendekatan tersebut digunakan secara terpadu dan berurutan: *statute approach* mengidentifikasi masalah normatif dalam teks undang-undang; *conceptual approach* menyediakan kerangka evaluasi teoritis terhadap masalah tersebut; dan *comparative approach* memberikan model konkret bagi rekomendasi rekonstruksi hukum yang dihasilkan.

Pengumpulan dan Analisis Data

Bahan hukum primer berupa peraturan perundang-undangan dan bahan hukum sekunder berupa jurnal ilmiah hukum serta buku teks dikumpulkan melalui studi kepustakaan yang sistematis. Teknik analisis data yang diterapkan meliputi *Analisis Hermeneutik Yuridis* untuk menginterpretasikan pasal secara konstitusional, serta metode analisis kualitatif normatif dengan *Penalaran Deduktif Hukum* guna menghasilkan kesimpulan yang bersifat preskriptif, objektif, dan solutif bagi pembaharuan hukum digital nasional.

HASIL DAN PEMBAHASAN

Struktur dan Interpretasi Pasal 15 UU PDP: Pengecualian Hak yang Menimbulkan Ketidakpastian

Pasal 15 UU PDP berbunyi: "*Pengecualian terhadap hak subjek data pribadi berdasarkan kepentingan umum sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a dapat dilakukan atas dasar*

ketentuan peraturan perundang-undangan dalam hal-hal sebagai berikut: a) penyelenggaraan negara; b) pertahanan negara; c) keamanan nasional; d) penegakan hukum; e) dan/atau kepentingan umum lainnya sebagaimana diatur dalam peraturan perundang-undangan." Teks pasal ini memperlihatkan beberapa kelemahan struktural yang kritis:

1. Elastisitas Frasa "Kepentingan Umum" (*Elastic Definition of "Public Interest"*)

Frasa "kepentingan umum" tidak didefinisikan secara operasional dalam UU PDP. Pasal 4 ayat (2) huruf a hanya menyebutkan bahwa "kepentingan umum" adalah "kepentingan nasional yang bersifat strategis", yang masih sangat abstrak. Ketidadaan batasan ini mengakibatkan penafsiran sepihak (*unilateral interpretation*) oleh penguasa digital (Ongkowiguno & Marsal, 2025; Wirogioto & Belgradoputra, *in press*).

2. Formula Hibrida (Alternatif-Kumulatif) "dan/atau"

Penggunaan kata "dan/atau" dalam Pasal 15 bukan hanya menciptakan redundansi dan ketidakjelasan interpretasi, melainkan membuka pintu ekspansi interpretasi secara kumulatif. Contoh: aparat dapat mengklaim bahwa suatu akses data diperlukan sekaligus untuk "penyelenggaraan negara" DAN "keamanan nasional" DAN "penegakan hukum" secara bersamaan, sehingga justifikasi menjadi semakin kuat dan sulit dibantah. GDPR secara rigid menghindari celah hukum ini dengan menerapkan formula pembatasan yang bersifat eksepsional dan berbasis klausul ketat (*numerus clausus*) sebagaimana diatur dalam Pasal 23 ayat (1) GDPR. Berdasarkan standardisasi tersebut, setiap pembatasan hak subjek data wajib didasarkan pada pemenuhan uji keharusan (*necessity test*) yang bersifat mandiri dan terpisah untuk setiap kategori kepentingan publik yang diajukan (European Data Protection Board, 2020). Akibatnya, dalam rezim GDPR, otoritas negara dilarang melakukan akumulasi justifikasi secara sepihak, sedangkan klausul hibrida pada Pasal 15 UU PDP Indonesia justru membuka peluang terjadinya *stacking* (penumpukan) justifikasi yang berpotensi mengaburkan serta mempersulit mekanisme kontrol yudisial (*judicial oversight*) (Budhijanto, 2024).

3. Clause Akhir "kepentingan umum lainnya"

Klausa ini memberikan daya ekspansi (*expansive power*) kepada pembuat peraturan pelaksana untuk terus-menerus menambahkan kategori baru, bertindak seperti "cek kosong" (*blank check*) bagi penguasa untuk memperluas akses data pribadi warga negara (Sidik & Wiraguna, 2025).

Dikotomi Konseptual: "Kepentingan Umum" dalam Perspektif Rechtsstaat vs. Machtstaat

Dalam optik hukum publik, frasa "kepentingan umum" dalam Pasal 15 UU PDP akan berwajah ganda tergantung pada paradigma negara yang menggunakannya. Penelitian ini membedah perbedaan radikal wajah kepentingan umum tersebut ke dalam dua kutub:

1. "Kepentingan Umum" dalam Konsep Machtstaat (Negara Kekuasaan)

Dalam paradigma *Machtsstaat*, kepentingan umum dipandang sebagai instrumen politik hukum unilateral (*self-authorization*). Penguasa mendominasi penafsiran kata "umum" untuk membenarkan tindakan pengawasan (*surveillance*) atau pembatasan hak warga demi melanggengkan kekuasaan, efisiensi birokrasi, atau stabilitas politik sepihak. Ciri utamanya adalah:

- a. Tidak memiliki batas waktu yang jelas (*indefinite access*) (Hildebrandt, 2016).
- b. Tidak memerlukan izin dari lembaga eksternal/pengadilan (Greenwald, 2014).
- c. Berwatak *rule by law*, di mana hukum dijadikan tameng legalitas untuk melanggar hak privasi warga secara masif. Dalam konteks Pasal 15 UU PDP, ketiadaan batasan materiil membuat pasal ini rawan menjadi instrumen *Machtsstaat* digital.

2. "Kepentingan Umum" dalam Konsep *Rechtsstaat* (Negara Hukum)

Sesuai amanat Pasal 1 ayat (3) UUD NRI 1945, dalam paradigma *Rechtsstaat*, kepentingan umum adalah pengecualian yang sangat ketat dan bersifat darurat (*exception strictissisimi juris*). "Umum" di sini bukan berarti kepentingan instansi atau penguasa, melainkan perlindungan kolektif terhadap hak-hak hidup warga itu sendiri (seperti menanggulangi terorisme, bencana alam massal, atau kejahatan kerah putih skala masif). Ciri utamanya wajib tunduk pada empat pilar (Barak, 2006):

- a. Legalitas Substantif : Kriterianya tertulis jelas, tidak multitafsir.
- b. Strict Necessity : Akses data hanya boleh dibuka jika benar-benar darurat dan tidak ada cara lain yang lebih minim pelanggaran privasi.
- c. Proportionality : Tindakan pembatasan harus seimbang dengan tujuan kedaruratan publik yang ingin dicapai.
- d. *Judicial Oversight* : Wajib dikontrol dan mendapat izin tertulis dari hakim/pengadilan independen sebelum data diakses.

Analisis Melalui Teori *State of Exception* Agamben

Mekanisme Kerja Digital Surveillance dalam Pasal 15 UU PDP Kekaburan norma "kepentingan umum" bertindak sebagai pintu masuk bagi penguasa untuk menciptakan "keadaan darurat digital yang terselubung" (*hidden digital state of exception*) (Agamben & Attell, 2005). Atas nama keamanan nasional, hak-hak privasi masyarakat sipil dapat dinonaktifkan secara legal tanpa transparansi data apa yang diakses, tanpa jaminan data akan dihapus, dan tanpa hak subjek data untuk mengetahui intervensi tersebut (*post-facto notification*). Dampaknya adalah ekspansi kendali pengawasan negara yang terus-menerus (*surveillance state*) yang mereduksi supremasi hukum menjadi sekadar instrumen kekuasaan (*rule by law*) (Greenwald, 2014). Kondisi ini memperparah risiko ekosistem digital nasional di tengah maraknya tantangan keamanan siber yang belum terkelola dengan matang (Rendi et al., 2025). Untuk memvisualisasikan mekanisme ini, terdapat empat skenario praktis yang menunjukkan bagaimana Pasal 15 dapat dioperasionalkan sebagai instrumen *Machtsstaat*:

1. SKENARIO 1 - Surveillance Masif atas Nama "Keamanan Nasional"

Aparat intelijen menyatakan bahwa aktivitas media sosial warga sipil perlu dipantau untuk "mengantisipasi radikalisme online dan terorisme siber" yang dianggap sebagai bagian dari "kepentingan umum penyelenggaraan negara". Karena Pasal 15 tidak mendefinisikan standar kedaruratan objektif (*objective emergency threshold*), aparat dapat mengklaim "kepentingan umum" tanpa bukti spesifik ancaman nyata. Akses data dijalankan tanpa izin pengadilan (*self-authorization*), dan data disimpan dalam jangka waktu tak terbatas di bawah alasan "pencegahan". Subjek data tidak diberitahu bahwa datanya diakses. Hasil: *surveillance state* yang *indefinite dan unaccountable* (Amin & Marzaman, 2023).

2. SKENARIO 2 - "Kepentingan Umum Ekonomi" sebagai Blank Check

Pemerintah menginginkan akses ke data pelanggan sebuah *e-commerce* platform untuk "mengoptimalkan kebijakan ekonomi digital nasional" (dapat diklaim sebagai "kepentingan ekonomi vital"). Karena Pasal 15 tidak membatasi apa yang termasuk "kepentingan ekonomi", interpretasi dapat dilenturkan untuk mencakup hal-hal seperti monitoring konsumsi warganegara, analisis pola pembelian untuk "riset pasar publik", atau bahkan deteksi *dissent* ekonomi. Tanpa mekanisme *judicial oversight*, keputusan sepihak instansi pemerintah adalah final. Subjek data tidak dapat mengajukan keberatan. Hasil: instrumentasi data pribadi untuk kontrol ekonomi-sosial (Razzaq & Nurmiati, *in press*; Zuboff, 2020). Pemrosesan data komersial skala besar tanpa batas moral ini melanggar etika privasi dalam pengelolaan *big data* dan membuka celah penyalahgunaan wewenang (Razzaq & Nurmiati, *in press*).

3. SKENARIO 3 - "Perpetual Emergency" untuk Data Kepolisian

Polda menyatakan bahwa data pribadi tersangka dalam kasus tindak pidana tertentu perlu disimpan secara permanen "untuk pencegahan kejahatan berulang" (bagian dari "kepentingan umum penegakan hukum"). Pasal 15 tidak menetapkan batas temporal akses atau kewajiban menghapus data setelah perkara diputus/vonis final. Hasilnya, data pribadi warga tetap dalam database polisi selamanya, dapat diakses tanpa izin baru, dan subjek data tidak pernah diberitahu. Ini mengubah "*exception*" menjadi "*permanent rule*". Data pribadi tergantung pada "*good will*" penegak hukum tanpa batasan hukum yang rigid. Ketika penyimpanan data tanpa batas waktu ini mengalami kegagalan sistem, kerumitan hukum akan muncul karena belum adanya sinkronisasi mengenai tanggung jawab perdata (*civil liability*) penguasa berdasarkan UU PDP dan KUH Perdata (Yanti, 2025). Hal ini berkelindan dengan absennya kejelasan pertanggungjawaban hukum pemerintah dalam kasus kebocoran data nasional pada Pusat Data Nasional (Dachlan et al., 2025), serta ketidakpastian tindakan pemulihan hak dari kementerian terkait terhadap para korban terdampak (Darmawan et al., 2025).

4. SKENARIO 4 - "Kepentingan Umum" untuk Monitoring Aktivisme Sipil

Kementerian Dalam Negeri mengklaim bahwa aktivitas organisasi masyarakat sipil di media sosial perlu dimonitor untuk "mengidentifikasi potensi kerusuhan sosial" demi "kepentingan umum penyelenggaraan negara yang stabil". Karena Pasal 15 tidak membedakan antara ancaman nyata

dan ancaman potensial, akses data dapat dibenarkan dengan standar yang sangat rendah ("*preventive monitoring*"). Tanpa mekanisme *judicial oversight*, *civil society organizations* tidak pernah tahu bahwa aktivitas mereka sedang dipantau. Pemerintah dapat mengidentifikasi aktivis, anggaran organisasi, pola donasi, bahkan internal discussions dalam grup WhatsApp organisasi. Hasil: *chilling effect* pada kebebasan berserikat dan berpendapat, serta *self-censorship* masif yang melemahkan demokrasi deliberatif. Dalam konteks ini, negara menggunakan "kepentingan umum" sebagai dalih untuk mengkonsolidasikan kekuasaan melalui kontrol informasi, bukan untuk melindungi keselamatan publik. Praktik pemantauan preventif yang meluas ini juga menjauhkan arah kebijakan teknologi dari standar tata kelola teknologi informasi (*IT governance*) yang transparan dan akuntabel (Samsumar et al., 2025).

Keempat skenario ini bukan spekulasi. Praktik serupa telah terdokumentasi dalam regulasi surveillance lain di berbagai negara (seperti *mass surveillance program* NSA di AS sebelum reform, atau sistem social credit di China). Indonesia belum memiliki track record panjang implementasi Pasal 15, tetapi kerangka normatif yang longgar menciptakan ruang untuk penyalahgunaan yang sama.

Perlu dicatat bahwa kritik terhadap penggunaan "*state of exception*" dalam Pasal 15 UU PDP bukan bermakna bahwa negara sama sekali tidak boleh mengakses data pribadi warga demi kepentingan umum yang sah. Justru, the point adalah bahwa *exception* harus tetap *exception*, bukan *rule*. Negara yang berbeda dengan *Machtsstaat* adalah negara yang dengan transparan mengakui ketika sedang dalam "*exception*" artinya: tujuan spesifik diartikulasikan, durasi dibatasi, mekanisme *oversight* berfungsi, dan warga diberitahu. Saat ini, Pasal 15 menciptakan risiko bahwa "*exception*" menjadi "*invisible rule*" seolah-olah normal bahwa negara dapat mengakses data tanpa batas dan tanpa transparansi. Inilah yang dimaksud sebagai pergeseran menuju *Machtsstaat* dalam konteks digital.

Komparasi dengan GDPR: Dari Unstructured Discretion menuju Structured Discretion

Berbeda dengan pengaturan dalam sistem hukum Indonesia, Pasal 23 *General Data Protection Regulation* (GDPR) Uni Eropa merepresentasikan penerapan *structured discretion* melalui perumusan pembatasan yang lebih rigid dan terstruktur. Meskipun GDPR dijadikan sebagai *benchmark* dalam kajian ini, perlu diakui bahwa implementasinya di tingkat praktik tidak sepenuhnya bebas dari tantangan. Sejumlah negara anggota Uni Eropa masih memanfaatkan konsep "*public interest*" untuk memperluas kapasitas pengawasan (*surveillance capability*), sebagaimana diidentifikasi dalam berbagai kajian akademik independen. Kendati demikian, keunggulan utama GDPR terletak pada perumusan norma yang bersifat limitatif dan keberadaan mekanisme *oversight* yang relatif lebih ketat dibandingkan dengan Pasal 15 UU PDP. Dengan demikian, GDPR dapat dinilai menyediakan struktur normatif yang lebih resilien terhadap potensi penyalahgunaan kekuasaan, meskipun efektivitas implementasinya tetap memerlukan pengawasan berkelanjutan dari masyarakat sipil serta mekanisme audit independen. Justru kapasitas GDPR untuk menerima kritik tersebutlah yang membuktikan keunggulan fundamentalnya: kelemahan implementasinya dapat diidentifikasi, diukur, dan diperdebatkan secara terbuka karena GDPR menyediakan parameter normatif yang eksplisit sebagai

tolok ukurnya. Berbeda dengan Pasal 15 UU PDP yang bahkan tidak menyediakan parameter normatif yang memadai untuk mendeteksi penyimpangan, arsitektur kelembagaan GDPR memungkinkan perbaikan berkelanjutan dan inilah yang menjadikannya rujukan komparatif yang paling relevan dan terstruktur bagi reformasi hukum perlindungan data di Indonesia.

1. **Definisi Limitatif:** Kategori kepentingan umum dihitung secara jelas dan eksklusif (keamanan nasional, pertahanan, keselamatan publik, kejahatan serius, moneter/ perpajakan, dan fungsi pengawasan otoritas publik) tanpa klausul sapujugat.
2. **Klausul Proteksi Prosedural:** Mewajibkan setiap legislasi pengecualian mencantumkan tujuan pemrosesan, kategori data yang diakses, batas waktu penyimpanan (*retention period*), serta jaminan perlindungan prosedural dari penyalahgunaan.

Untuk mereplikasi struktur ini di Indonesia, diperlukan proyeksi kedudukan lembaga pengawas (Lembaga PDP) yang mandiri untuk menjamin sekuritas data digital di era disrupsi (Santosa et al., 2025). Penataan ini sangat krusial agar pembangunan hukum siber nasional sejalan dengan agenda makro pembangunan budaya hukum digital yang berintegritas di Indonesia (Pusat Analisis dan Evaluasi Hukum Nasional, 2023)

Formulasi Kriteria "Kepentingan Umum" yang Ideal dalam Perspektif Rechtsstaat: Sintesis Analisis

Keseluruhan analisis yang telah dipaparkan dalam sub-bagian sebelumnya kini memungkinkan penelitian ini untuk merumuskan sintesis normatif tentang seperti apa seharusnya wajah 'kepentingan umum' yang legitimate dalam perspektif Rechtsstaat.

Berdasarkan analisis normatif terhadap struktur Pasal 15 UU PDP (Bagian 4.1), dikotomi konseptual Rechtsstaat-Machtstaat (Bagian 4.2), mekanisme state of exception digital (Bagian 4.3), dan komparasi dengan Pasal 23 GDPR (Bagian 4.4), penelitian ini merumuskan bahwa "kepentingan umum" yang sah dalam perspektif Rechtsstaat harus memenuhi lima kriteria kumulatif sebagai berikut:

1. Kriteria Substansialitas Ancaman (Substantial Threat Criterion)

Kepentingan umum hanya dapat diklaim apabila terdapat ancaman nyata, konkret, dan terukur terhadap keselamatan kolektif warga negara, bukan sekadar ancaman potensial atau hipotetis. Dalam perspektif teori Jhering, tujuan hukum (Zweck) pembatasan hak privasi hanya terpenuhi apabila manfaat kolektif yang diperoleh secara proporsional melampaui kerugian individual yang ditimbulkan. Klaim kepentingan umum yang bersifat preventif-spekulatif tanpa bukti konkret tidak memenuhi ambang batas substansialitas ini.

2. Kriteria Definisi Limitatif (Limitative Definition Criterion)

Kategori yang tergolong "kepentingan umum" harus didefinisikan secara enumeratif dan tertutup (numerus clausus) dalam peraturan perundang-undangan, sebagaimana dipraktikkan dalam Pasal 23 GDPR. Keterbukaan klausa seperti "kepentingan umum lainnya" dalam Pasal 15 UU PDP adalah anomali normatif yang bertentangan dengan asas legalitas substantif (lex certa) yang menjadi fondasi Rechtsstaat. Dalam Rechtsstaat sejati, pembatasan hak fundamental hanya dapat dilakukan

berdasarkan norma yang jelas, tidak multitafsir, dan dapat diprediksi oleh warga negara (foreseeability).

3. Kriteria Keharusan Ketat (Strict Necessity Criterion)

Pengecualian terhadap hak subjek data hanya dapat dibenarkan apabila tidak terdapat alternatif lain yang lebih minim pelanggaran privasi untuk mencapai tujuan yang sama. Prinsip ini, yang juga dikenal sebagai prinsip intervensi minimal (least restrictive means), merupakan elemen inti dari proporsionalitas dalam hukum hak asasi manusia internasional. Pasal 15 UU PDP saat ini tidak mengandung klausul necessity test yang eksplisit, sehingga membuka ruang bagi penguasa untuk memilih cara yang paling mudah bagi mereka, bukan cara yang paling minim dampak pelanggarannya bagi warga.

4. Kriteria Pengawasan Yudisial Independen (Independent Judicial Oversight Criterion)

Setiap tindakan pengecualian hak subjek data atas dasar kepentingan umum wajib mendapatkan otorisasi dari lembaga yudisial yang independen sebelum atau sesegera mungkin setelah akses dilakukan. Absennya mekanisme ini dalam Pasal 15 UU PDP menciptakan kondisi self-authorization yang merupakan ciri khas Machtsstaat. Dalam Rechtsstaat, tidak ada lembaga negara yang boleh menjadi hakim atas tindakannya sendiri (nemo judex in causa sua). Pengawasan yudisial bukan sekadar prosedur administratif, melainkan jaminan konstitusional bahwa kekuasaan tetap tunduk pada hukum.

5. Kriteria Temporalitas dan Akuntabilitas (Temporality and Accountability Criterion)

Kepentingan umum yang sah bersifat temporer, bukan permanen. Setiap pengecualian hak harus disertai batas waktu yang rigid dan kewajiban penghapusan data setelah tujuan berakhir, serta mekanisme notifikasi dan audit pasca-akses. Ketiadaan temporalitas dalam Pasal 15 UU PDP memungkinkan terjadinya "*perpetual exception*" yang dalam kerangka teori Agamben merupakan tanda paling nyata dari pergeseran menuju Machtsstaat digital.

Kelima kriteria ini bersifat kumulatif, artinya seluruhnya harus terpenuhi secara bersamaan agar suatu klaim "kepentingan umum" dapat dibenarkan dalam paradigma Rechtsstaat. Ketiadaan salah satu kriteria saja sudah cukup untuk mengindikasikan pergeseran ke arah Machtsstaat. Tabel berikut merangkum posisi Pasal 15 UU PDP saat ini terhadap kelima kriteria tersebut:

Tabel 2. Pemenuhan Kriteria Rechtsstaat oleh Pasal 15 UU PDP

No	Kriteria Rechtsstaat	Pasal 15 UU PDP Saat Ini	Status
1.	Substansialitas Ancaman	Tidak ada ambang batas objektif	✗ Tidak Terpenuhi
2.	Definisi Limitatif	Klausula terbuka "kepentingan umum lainnya"	✗ Tidak Terpenuhi
3.	Strict Necessity	Tidak ada necessity test eksplisit	✗ Tidak Terpenuhi
4.	Judicial Oversight	Tidak ada mekanisme otorisasi yudisial	✗ Tidak Terpenuhi

5.	Temporalitas & Akuntabilitas	Tidak ada batas waktu dan kewajiban hapus data	✗ Tidak Terpenuhi
----	------------------------------	--	-------------------

Fakta bahwa Pasal 15 UU PDP tidak memenuhi satu pun dari lima kriteria Rechtsstaat di atas merupakan temuan sentral penelitian ini. Hal ini secara normatif mengkonfirmasi bahwa konstruksi Pasal 15 saat ini lebih mencerminkan watak Machtstaat daripada Rechtsstaat, dan menjadi justifikasi ilmiah yang kuat bagi urgensi rekonstruksi hukum melalui aturan turunan UU PDP sebagaimana direkomendasikan dalam bagian berikutnya.

Rekomendasi Rekonstruksi Hukum

Untuk membentengi Rechtsstaat dan mencegah watak Machtstaat, aturan turunan UU PDP di Indonesia, baik dalam bentuk Peraturan Pemerintah (PP) maupun Peraturan Otoritas Pelindungan Data Pribadi, mendesak untuk mengonstruksi kriteria kepentingan umum ke dalam lima parameter hukum berikut:

Definisi Limitatif dan Kasuistik dari "Kepentingan Umum"

Aturan turunan harus mendefinisikan "kepentingan umum" secara limitatif mengadopsi model GDPR (European Data Protection Board, 2024; Official Journal of the European Union, 2016). Cakupan harus dibatasi pada: keamanan nasional (ancaman kedaulatan *territorial* nyata), pertahanan militer eksternal, keselamatan publik (kejahatan serius dengan ancaman pidana minimum 5 tahun), dan perlindungan kepentingan ekonomi/finansial vital negara.

Mekanisme Judicial Oversight (Pengawasan Yudisial)

Dengan Prosedur Konkret Setiap pengaksesan data warga demi kepentingan umum wajib mendapatkan otorisasi persetujuan tertulis dari pengadilan (*court order/judicial warrant*) yang dikeluarkan oleh hakim independen, bukan diputuskan sendiri oleh instansi yang bersangkutan (*self-authorization*).

Mekanisme judicial oversight harus beroperasi dalam tiga tahap. Pertama, tahap pre-access authorization, di mana setiap institusi publik wajib mengajukan permohonan tertulis kepada pengadilan independen dengan justifikasi objektif, dan hakim melakukan review dalam maksimum 48 jam. Kedua, tahap emergency exception, di mana akses darurat tanpa otorisasi awal hanya diizinkan dalam ancaman iminen, dengan kewajiban notifikasi ke hakim dalam 24 jam pasca-akses dan review ex post facto oleh hakim tersebut. Ketiga, tahap post-access accountability, di mana aparat wajib melaporkan data yang diakses, relevansinya dengan justifikasi awal, dan rencana penghapusan data kepada hakim yang menerbitkan deletion order yang mengikat (Muslim, 2025; Samsumar et al., 2025).

Parameter Kedaruratan Objektif (Objective Emergency Parameter)

Pengecualian tanpa otorisasi awal (*pre-authorization*) hanya diizinkan dalam kondisi kedaruratan ekstrem yang objektif, seperti situasi mengancam nyawa massal, serangan siber aktif terhadap infrastruktur kritis, atau ancaman terorisme siber nyata. Tindakan ini wajib dilaporkan ke pengadilan dalam waktu 24 jam pasca-akses.

Pembatasan Jangka Waktu Akses dan Data Retention (Time-Limited Access)

Negara hanya diberikan otoritas memproses data selama masa kegentingan berlangsung dengan batas waktu maksimum yang rigid (misalnya maksimum 30 hingga 90 hari). Data wajib dimusnahkan secara permanen segera setelah tujuan penegakan hukum atau keadaan darurat tersebut berakhir (Dachlan et al., 2025).

Akuntabilitas Forensik Pasca-Akses (Post-Access Forensic Accountability) dan Roadmap Implementasi

Aturan turunan UU PDP wajib memerintahkan adanya pencatatan akses terperinci (*detailed access logging*) dan audit forensik digital secara berkala oleh lembaga pengawas independen guna menjamin adanya transparansi pasca-tindakan (Hildebrandt, 2016; Zuboff, 2020). Hasil audit tersebut harus dilaporkan secara akuntabel kepada Otoritas Pelindungan Data Pribadi (OPDP) dan Parlemen, serta menjamin hak notifikasi pasca-akses (*post-facto notification*) bagi subjek data. Melalui mekanisme notifikasi ini, warga negara dapat mengetahui apabila data pribadi mereka telah diakses oleh negara, sekaligus memberikan mereka landasan hukum yang kuat untuk mengajukan gugatan jika ditemukan unsur penyalahgunaan wewenang (*abuse of power*) oleh aparat (Santosa et al., 2025). Pada akhirnya, guna mewujudkan seluruh parameter ideal Rechtsstaat digital ini, perumusan regulasi pelaksana memerlukan pendekatan bertahap (*roadmap*) yang komprehensif, mulai dari pelaksanaan konsultasi publik yang inklusif, program penguatan kapasitas (*capacity building*) bagi lembaga peradilan, hingga evaluasi kebijakan secara berkala dengan target penyelesaian aturan turunan dalam kurun waktu dua tahun sejak berlakunya UU PDP secara penuh (Pusat Analisis dan Evaluasi Hukum Nasional, 2023).

KESIMPULAN

Penelitian ini menghasilkan dua temuan utama yang saling menguatkan. *Pertama*, dari perspektif normatif, frasa "kepentingan umum" dalam Pasal 15 UU PDP terbukti bersifat elastis tanpa definisi operasional yang memadai, tanpa parameter keharusan (*necessity test*) yang eksplisit, tanpa mekanisme pengawasan yudisial, dan tanpa batas temporal akses data. Kekosongan normatif ini beroperasi dalam tiga dimensi sekaligus: dimensi bahasa (kekaburan norma), dimensi prosedural (absensi *judicial oversight*), dan dimensi temporal (tidak ada batas waktu akses). Pasal 15 UU PDP secara struktural terbukti lebih mencerminkan watak Machtsstaat daripada Rechtsstaat, sebagaimana dikonfirmasi oleh ketidakpenuhan Pasal 15 terhadap seluruh lima kriteria kumulatif Rechtsstaat yang dirumuskan dalam penelitian ini: (1) substansialitas ancaman, (2) definisi limitatif, (3) *strict necessity*, (4) *judicial oversight* independen, serta (5) temporalitas dan akuntabilitas.

Kedua, dari perspektif komparatif, hasil perbandingan dengan Pasal 23 GDPR Uni Eropa mengungkap ketertinggalan Indonesia yang signifikan dalam empat aspek: definisi kepentingan umum (GDPR menggunakan *numerus clausus*, Pasal 15 menggunakan klausa terbuka), standar *strict necessity* dan *proportionality* (eksplisit dalam GDPR, tidak ada dalam Pasal 15), mekanisme *judicial oversight*

(wajib dalam GDPR, tidak ada dalam Pasal 15), dan akuntabilitas pasca-akses (diwajibkan dalam GDPR, tidak diatur dalam Pasal 15).

Implikasi Teoritis

Secara teoritis, penelitian ini memberikan kontribusi bagi pengembangan wacana dialektika Rechtsstaat-Machtstaat dalam konteks hukum siber nasional. Dengan mengintegrasikan teori *state of exception* Agamben, teori tujuan hukum (*Der Zweck im Recht*) Jhering, dan konsep *structured discretion* ke dalam satu kerangka analisis yang koheren, penelitian ini mendemonstrasikan bahwa pergeseran paradigma dari Rechtsstaat menuju Machtstaat di era digital tidak selalu terjadi melalui perubahan rezim yang dramatis dan terbuka, melainkan dapat berlangsung secara gradual dan tidak kasat mata melalui kekaburan normatif dalam regulasi perlindungan data. Selain itu, penelitian ini memperkenalkan konstruk "lima kriteria kumulatif Rechtsstaat" sebagai instrumen uji normatif yang dapat digunakan oleh peneliti, pembuat kebijakan, dan hakim dalam mengevaluasi legitimasi klaim "kepentingan umum" dalam regulasi digital nasional.

Implikasi Praktis dan Rekomendasi

Berdasarkan temuan-temuan tersebut, penelitian ini merekomendasikan agar pemerintah segera menyusun aturan turunan UU PDP—baik dalam bentuk Peraturan Pemerintah maupun Peraturan Otoritas Pelindungan Data Pribadi—yang memuat lima parameter kumulatif kepentingan umum dalam perspektif Rechtsstaat: substansialitas ancaman yang mensyaratkan ambang batas objektif dan terukur; definisi limitatif berbasis *numerus clausus* yang menutup klausa ekspansif; *strict necessity* dengan *necessity test* eksplisit; *judicial oversight* independen melalui mekanisme *court order*; serta temporalitas dan akuntabilitas yang mensyaratkan batas waktu akses yang rigid dan kewajiban penghapusan data setelah tujuan berakhir. Tanpa rekonstruksi hukum yang segera dan komprehensif, Pasal 15 UU PDP berisiko bertransformasi menjadi instrumen legitimasi *surveillance state* yang secara konstitusional bertentangan dengan amanat Pasal 1 ayat (3) UUD NRI 1945 sebagai fondasi negara hukum Indonesia di era digital.

Keterbatasan Penelitian dan Agenda Penelitian Lanjutan

Penelitian ini memiliki beberapa keterbatasan yang perlu diakui secara akademis. *Pertama*, analisis berfokus pada aspek normatif-tekstual dan belum mencakup studi empiris terhadap praktik penerapan Pasal 15 UU PDP oleh instansi publik sejak pemberlakuannya. *Kedua*, komparasi hukum terbatas pada satu sistem perbandingan (GDPR Uni Eropa) dan belum melibatkan regulasi perlindungan data dari kawasan Asia Tenggara yang mungkin lebih kontekstual secara sosio-kultural dan historis. *Ketiga*, rekomendasi rekonstruksi hukum yang diajukan masih bersifat normatif-konseptual dan memerlukan kajian lanjut mengenai *feasibility* implementasinya dalam konteks kapasitas yudisial dan kelembagaan Indonesia yang aktual. Penelitian selanjutnya disarankan untuk melakukan studi empiris terhadap praktik diskresi "kepentingan umum" oleh instansi publik, serta analisis komparatif yang lebih luas dengan regulasi perlindungan data di kawasan ASEAN, khususnya PDPA Thailand dan PDPA Singapura.

REFERENSI

- Agamben, Giorgio, & Attell, Kevin. (2005). *State of Exception*. University of Chicago Press.
- Amin, N. A., & Marzaman, A. P. (2023). *Triwikrama: Jurnal Ilmu Sosial Redefinisi Kedaulatan Di Era Digital: Keamanan Siber, Tata Kelola Data, Dan Otonomi Regional Di Asia Tenggara*.
- Barak, Aharon. (2006). *The judge in a democracy*. Princeton University Press.
- Budhijanto, D. (2024). *Hukum Pelindungan Data Pribadi & Nasional DANRIVANTO 2024*.
- Bygrave, L. A. (2014). *Data Protection Law-Approaching Its Rationale, Logic and Limits*. Kluwer Law International.
- Dachlan, A. A., Nabila, A., Putri, N. A., & Nurmasitha, N. (2025). Pertanggungjawaban Hukum Pemerintah Dalam Kebocoran Data Pribadi Pada Penyelenggaraan Pusat Data Nasional. *Journal of Education Research*, 5(3), 3368–3379. <https://doi.org/10.37985/jer.v5i3.1491>
- Darmawan, F., Arianto, H., & Artikel, I. (2025). *Arus Jurnal Sosial dan Humaniora (AJSH) Upaya Perlindungan Hukum dan Tanggung Jawab Kemkomdigi terhadap Korban Kebocoran Data Pribadi di Indonesia*. <http://jurnal.ardenjaya.com/index.php/ajsh>
- Erlangga, M., NurhalizahAisyah, Badjeber, H., Wildan, A., & Rahmadia, H. (2024). Implementasi Uu Pelindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia. *Esensi Hukum*, 5(2), 115–131. <https://doi.org/10.35586/esensihukum.v5i2.240>
- European Data Protection Board. (2024). *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*. https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf
- Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Hamish Hamilton.
https://books.google.co.id/books/about/No_Place_to_Hide.html?id=ye8EnwEACAAJ&redir_esc=y
- Gobel, F. R., & Muhtar, M. H. (2024). Rekonstruksi Judicial Review Digital dalam Perspektif Hukum Tata Negara Indonesia. *Jurnal Konstitusi*, 21(1), 112–138.
- Hildebrandt, Mireille. (2016). *Smart technologies and the end(s) of law : novel entanglements of law and technology*. Edward Elgar Publishing.
- Kelsen, H. (2017). *General Theory of Law & State*. Routledge. <https://doi.org/10.4324/9780203790960>
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. (1945). https://www.mpr.go.id/uploads/jdih/UUD_1945_DALAM_SATU_NASKAH.pdf
- Muslim, P. H. (2025). Konsep Hak Atas Privasi dalam Era Digital: Tinjauan Filosofis dan Yuridis. *HARISA: Jurnal Hukum, Syariah, dan Sosial*, 2(1), 96–109. <https://ejournal.eddhuhacenter.com/index.php/harisa/article/view/65>

- Nur Azizah Qurrotuaini. (2024). Hak Privasi sebagai Hak Konstitusional di Era Digital: Kajian Yuridis dalam Perspektif Hukum Siber. In *Jurnal Hukum Kenegaraan dan Politik Islam* (Vol. 4, Number 2).
- Nugraha, R. A., Pratama, D. S., & Hidayat, M. F. (2025). Analisis Kebocoran Data BPJS Kesehatan: Implikasi Hukum dan Teknis terhadap Pelindungan Data Pribadi di Indonesia. *Jurnal Hukum dan Teknologi Informasi*, 3(1), 45–62.
- Presiden Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Official Journal of the European Union. (2016). Regulations (EU) 2016/679 of The European Parliament and of The Council of The Council of 27 April 2016. In *Official Journal of the European Union*. Official Journal of the European Union. <https://gdpr-info.eu/>
- Ongkowiguno, C. M., & Marsal, I. (2025). Politik Hukum Perlindungan Data Pribadi dalam Layanan Publik Digital di Indonesia. *Hakim: Jurnal Hukum*, 06(04), 1321–1326. <https://doi.org/10.54209/judge.v6i04.1851>
- Pusat Analisis dan Evaluasi Hukum Nasional, Badan Pembinaan Hukum Nasional. (2023). *Dokumen Pembangunan Hukum Nasional Tahun 2023: Pembangunan Budaya Hukum di Indonesia*. Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia. https://bphn.go.id/data/documents/00_laporan_dphn_2023_231115_fin_cetak.pdf
- Rendi, M., Tamza, F. B., Ahmad, D., & Fardiansyah, I. (2025). Pelindungan Data Pribadi Dalam Era Digitalisasi Dan Tantangan Keamanan Siber Di Indonesia Protection Of Personal Data In The Digital Era And Cybersecurity Challenges In Indonesia. In *Jurnal Hukum Lex Generalis* (Vol. 6, Number 12). <https://jhlrg.rewangrencang.com/>
- Samsumar, L. D., Nasiroh, S., Farizy, S., Anwar, C., Mursyidin, I. H., Rosdiyanto, R., Widiyanto, W., Mutiarawan, R. A., Mukin, R., & Yusnanto, T. (2025). *Keamanan Sistem Informasi: Perlindungan Data dan Privasi di Era Digital*. Henry Bennett Nelson.
- Santosa, M. H., Faried, F. S., & Zaelani, M. A. (2025). Proyeksi Kedudukan dan Fungsi Lembaga PDP Dalam Menjamin Keamanan Data Digital di Era Disrupsi. *Unes Journal of Swara Justisia*, 9(2), 268–277. <https://doi.org/10.31933/e26bpe26>
- Schmitt, C. (1985). *Political Theology: Four Chapters on the Concept of Sovereignty*. MIT Press.
- Scheppele, K. L. (2018). Autocratic Legalism. *The University of Chicago Law Review*, 85(2), 545–584.
- Seagle, W. (1945). Rudolf von Jhering: Or Law as a Means to an End. *The University of Chicago Law Review*, 13(1), 71. <https://doi.org/10.2307/1597562>
- Sidik, B. P., & Wiraguna, S. A. (2025). Tinjauan Hukum Terhadap Aplikasi Digital Sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 2(April), 219–232.

- Solove, D. J. (2004). *D. Solve, The Digital Person: Technology and Privacy in the Information Age. The Digital Person: Technology and Privacy in the Information Age, NYU Press (2004).*
<https://doi.org/https://ssrn.com/abstract=2899131>
- Stahl, F. J. 1802-1861. (1870). *Die Philosophie des Rechts: Rechtsphilosophie: V. 1.* Heidelberg : J.C.B. Mohr.
- Razzaq, R. S. D., & Nurmiati, E. (*in press*). Tantangan Etika dan Privasi terhadap Cyber Crime Big Data (Studi Literatur). *Jurnal Komputer dan Pusat Informatika*, 3(2). Retrieved from <https://jurnal.kopusindo.com/index.php/jkhkp/1646>
- Tamanaha, B. Z. (2006). *Law as a Means to an End.* Cambridge University Press.
<https://doi.org/10.1017/CBO9780511511073>
- Wirogioto, A. J., & Belgradoputra, J. S. (*in press*). Memahami Hukum Siber dan Implementasi Perlindungan Data Pribadi dalam Skala Nasional. *Jurnal Hukum Digital Indonesia.*
<https://repository.unkris.ac.id/id/eprint/5292/1/Memahami%20Hukum%20Siber.pdf>
- Yanti, M. (2025). Analisis Tanggung Jawab Perdata dalam Kebocoran Data: Sinkronisasi UU Perlindungan Data Pribadi dan KUH Perdata. *Jurnal Ilmu Sosial Dan Humaniora*, 1(4), 1539–1549. <https://doi.org/10.63822/n9bwps44>
- Zuboff, Shoshana. (2020). *The age of surveillance capitalism : the fight for a human future at the new frontier of power.* PublicAffairs.