

REGULASI DATA DAN HAK PRIVASI DI INDONESIA: APAKAH NEGARA MELAMPAUI BATAS DALAM PENGAWASAN DIGITAL

Hasmaryadi¹, Tauratiya², Lailasari Eka Ningsih³

hasmaryadi99@gmail.com¹, tauratiya@gmail.com², lailasarien@gmail.com³

UIN SUNAN KALIJAGA YOGYAKARTA, YOGYAKARTA, INDONESIA¹

IAIN SYAIKH ABDURRAHMAN SIDDIK BANGKA BELITUNG,
INDONESIA²

UNIVERSITAS DARUL ULUM ISLAMIC CENTRE SUDIRMAN GUPPI,
KABUPATEN SEMARANG, JAWA TENGAH, INDONESIA³

ABSTRAK

Artikel ini membahas regulasi data dan hak privasi di Indonesia dengan fokus pada keseimbangan antara perlindungan data pribadi dan kewenangan negara dalam pengawasan digital. Melalui metode penelitian yuridis normatif dengan pendekatan konseptual dan perundang-undangan, artikel ini menelaah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Kominfo Nomor 5 Tahun 2020. Hasil analisis menunjukkan bahwa meskipun regulasi tersebut dirancang untuk melindungi data pribadi masyarakat, kewenangan negara yang luas dalam pengawasan digital berpotensi melampaui batas dan menimbulkan risiko pelanggaran hak privasi individu. Ketidakseimbangan regulasi, lemahnya mekanisme pengawasan independen, serta minimnya transparansi memperkuat potensi penyalahgunaan kewenangan oleh pemerintah. Artikel ini menekankan pentingnya pembentukan lembaga pengawas independen, mekanisme transparansi, dan penguatan akuntabilitas agar pengawasan digital tetap sejalan dengan prinsip hak asasi manusia dan kepastian hukum. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi masukan bagi pembuat kebijakan dalam menyempurnakan regulasi perlindungan data pribadi di Indonesia agar lebih adil, proporsional, dan akuntabel.

Kata Kunci: Perlindungan Data Pribadi; Hak Privasi; Regulasi Indonesia; Pengawasan Digital.

PENDAHULUAN

Pada era digital yang semakin berkembang pesat, pengumpulan dan pemrosesan data pribadi telah menjadi bagian tak terpisahkan dari kehidupan masyarakat modern. Dengan meningkatnya ketergantungan terhadap teknologi, baik di sektor pemerintahan maupun swasta, muncul tantangan baru terkait perlindungan data dan hak privasi individu. Dalam kondisi seperti ini, isu mengenai regulasi data dan hak privasi menjadi

perhatian utama di berbagai negara, termasuk Indonesia.¹ Pemerintah Indonesia telah mengambil langkah signifikan dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) pada 17 Oktober 2022.² Undang-undang ini bertujuan untuk memberikan perlindungan terhadap data pribadi warga negara dan memastikan hak konstitusional subjek data pribadi terjamin. UU PDP memberikan ketentuan mengenai bagaimana data pribadi dapat dikumpulkan, diproses, dan digunakan oleh pihak yang berkepentingan, baik sektor pemerintah maupun swasta.

Klasifikasikan data pribadi berdasarkan ketentuan Pasal 4 ayat (1) UU PDP dibagi menjadi dua kategori utama, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum.³ Data pribadi spesifik mencakup informasi seperti data kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Sementara itu, data pribadi umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan data lain yang dapat digunakan untuk mengidentifikasi seseorang.

Pengesahan undang-undang ini dilatarbelakangi oleh meningkatnya kasus kebocoran data pribadi di Indonesia. Beberapa platform digital mengalami serangan siber yang mengakibatkan data pengguna terekspos, menimbulkan kerugian materil dan non-materil bagi individu yang terdampak. Situasi ini menekankan urgensi akan regulasi yang jelas dan tegas untuk melindungi data pribadi masyarakat. Akan tetapi, di balik upaya pemerintah untuk melindungi data pribadi, muncul kekhawatiran mengenai potensi penyalahgunaan kewenangan dalam pengawasan digital oleh negara. Berbagai regulasi lain seperti Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)⁴ serta Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan

¹ Three Boy, Ariawan. (2023). Peran Undang-Undang Perlindungan Data Pribadi dan Hukum Telekomunikasi dalam SPBE di Indonesia. *UNES Law Review*, 6 (2), hlm. 5533-5538. <https://review-unes.com/index.php/law/article/view/1379/1105>

² Republik Indonesia, Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

³ Muhammad Alfaruq Nirwana. (2022). Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual. *Jurnal Al-Wasath*, 3 (2), hlm. 93-104. <https://journal.unusia.ac.id/index.php/alwasath/article/download/609/339/1789>

⁴ Republik Indonesia, Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Sistem dan Transaksi Elektronik (PP PSTE)⁵ memberikan kewenangan luas kepada pemerintah dalam pengawasan dan pemrosesan data digital. Hal ini memunculkan kekhawatiran mengenai potensi penyalahgunaan kewenangan negara dalam pengawasan digital yang dapat mengancam kebebasan dan privasi individu. Ketiadaan payung hukum yang komprehensif menyebabkan inkonsistensi dalam perlindungan data pribadi, sehingga diperlukan undang-undang khusus yang mengatur secara menyeluruh.

Beberapa pihak mempertanyakan apakah negara dapat melampaui batas dalam mengawasi aktivitas digital warganya, yang dapat mengancam hak privasi individu. Permasalahan ini menjadi relevan mengingat perkembangan teknologi yang memungkinkan pemerintah untuk mengakses dan memantau data pribadi dengan lebih mudah. Salah satu kasus yang menyoroti kekhawatiran ini adalah dugaan penyalahgunaan data pribadi oleh instansi pemerintah untuk tujuan di luar kepentingan publik. Misalnya, terdapat laporan mengenai akses data pribadi tanpa izin yang dilakukan oleh oknum tertentu, yang menimbulkan pertanyaan mengenai mekanisme pengawasan dan akuntabilitas dalam pemrosesan data pribadi oleh pemerintah. Selain itu, kasus kebocoran data yang melibatkan institusi pemerintah, seperti kebocoran data BPJS Kesehatan dan KPU, menunjukkan adanya kelemahan dalam sistem perlindungan data.

Pada tahun 2022, kebijakan pemblokiran situs dan platform digital oleh pemerintah terhadap PayPal, Steam, dan berbagai layanan digital lainnya, menimbulkan pertanyaan tentang sejauh mana negara memiliki kewenangan dalam mengontrol akses informasi digital. Kasus semacam ini menekankan pentingnya keseimbangan antara perlindungan data pribadi dan kebutuhan pemerintah dalam pengawasan digital. Persoalan utama yang muncul adalah bagaimana mencapai keseimbangan antara perlindungan data pribadi dan kewenangan negara dalam melakukan pengawasan digital. Apakah regulasi yang ada telah cukup efektif dalam mencegah penyalahgunaan kewenangan oleh negara dan tidak melampaui batas? Tulisan ini akan membahas lebih dalam mengenai regulasi data dan hak privasi di Indonesia serta mengevaluasi apakah negara telah melampaui batas dalam pengawasan digital.

⁵ Republik Indonesia, Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).

METODE PENELITIAN

Metode penelitian yang digunakan dalam artikel ini bersifat yuridis normatif dengan pendekatan konseptual dan perundang-undangan. Pendekatan ini dipilih karena fokus kajian diarahkan pada analisis norma hukum positif yang mengatur perlindungan data pribadi dan hak privasi di Indonesia serta batas kewenangan negara dalam pengawasan digital. Penelitian yuridis normatif menurut Peter Mahmud Marzuki menekankan pada kajian hukum tertulis, asas-asas hukum, dan doktrin yang berkembang di dalam praktik hukum.⁶ Data yang digunakan merupakan data sekunder, yang terdiri dari bahan hukum primer seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Kominfo Nomor 5 Tahun 2020. Selain itu digunakan pula bahan hukum sekunder berupa literatur ilmiah, dan artikel jurnal. Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dengan menginventarisasi berbagai sumber hukum primer dan sekunder yang relevan. Data yang terkumpul kemudian dianalisis secara kualitatif melalui metode deskriptif-analitis, yaitu dengan memaparkan ketentuan hukum positif dan teori hukum yang berlaku kemudian dianalisis untuk menilai kesesuaian norma hukum dengan prinsip perlindungan hak asasi manusia. Analisis ini bertujuan menghasilkan argumentasi hukum yang sistematis, komprehensif, dan kritis mengenai sejauh mana negara melampaui batas dalam pengawasan digital. Pendekatan serupa juga disarankan oleh Salim HS yang menyatakan bahwa penelitian hukum normatif dengan analisis kualitatif memungkinkan peneliti menguraikan isu hukum secara mendalam dan mengaitkannya dengan asas hukum atau doktrin hukum yang relevan.⁷

HASIL DAN PEMBAHASAN

1. Tinjauan Umum Tentang Data Pribadi dan Hak Privasi

Data pribadi merupakan informasi yang dapat digunakan untuk mengidentifikasi individu secara langsung maupun tidak langsung. Dalam era digital yang semakin berkembang pesat, data pribadi menjadi aset yang sangat berharga dan sering kali

⁶ Peter Mahmud Marzuki. *Penelitian Hukum Edisi Revisi*. (Jakarta: Kencana, 2024), hlm. 136.

⁷ Salim HS & Erlies Septianan Nurbani. *Penerapan Teori Hukum pada Penelitian Tesis dan Disertasi*. (Jakarta: RajaGrafindo Persada, 2018), hlm. 45.

menjadi objek pengumpulan, pemrosesan, serta perdagangan oleh berbagai pihak, termasuk pemerintah, perusahaan swasta, dan entitas lainnya.⁸ Dengan meningkatnya penggunaan teknologi digital, perlindungan terhadap data pribadi menjadi semakin krusial guna mencegah penyalahgunaan yang dapat merugikan individu.

Di tingkat internasional, data pribadi diakui sebagai bagian dari hak privasi yang harus dilindungi. *General Data Protection Regulation* (GDPR) Uni Eropa, yang menjadi standar global dalam perlindungan data pribadi, mendefinisikan data pribadi sebagai informasi apa pun yang terkait dengan individu yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, seperti nama, alamat, nomor identitas, data lokasi, atau elemen fisik, genetik, mental, ekonomi, budaya, dan sosial seseorang.

Di Indonesia, perlindungan data pribadi mulai mendapat perhatian serius dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ini mendefinisikan data pribadi sebagai setiap informasi yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi secara langsung maupun tidak langsung melalui sistem elektronik maupun non-elektronik. Undang-undang ini juga mengatur prinsip pemrosesan data pribadi, termasuk kewajiban memperoleh persetujuan dari pemilik data, memastikan keamanan data, serta hak individu untuk mengakses, mengubah, dan menghapus data mereka. Selain itu, regulasi lain seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 dan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) turut memberikan dasar hukum terkait pemrosesan dan perlindungan data pribadi di ruang digital.

Meskipun berbagai regulasi telah diterapkan, masih terdapat tantangan dalam implementasi perlindungan data pribadi di Indonesia, terutama terkait pengawasan dan sanksi terhadap pelanggaran yang dilakukan oleh pihak-pihak yang memiliki akses terhadap data.⁹ Kasus kebocoran data yang melibatkan lembaga pemerintah dan perusahaan teknologi menunjukkan bahwa perlindungan data pribadi masih perlu diperkuat dengan sistem pengawasan yang lebih transparan dan akuntabel. Oleh karena itu, diperlukan kerja sama antara pemerintah, sektor swasta, dan masyarakat untuk

⁸ Chaterine Grace Gunadi, Danishel Subiran, et.all. (2023). Perlindungan Hukum Atas Kebocoran Data Pribadi. *Proceeding of Conference on Law and Social Studies*. <https://prosiding.unipma.ac.id/index.php/COLaS/article/viewFile/5158/4109>

⁹ Fanisa Mayda Ayiliani, Elfia Farida. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, 6 (3), hlm. 431-455. <https://doi.org/10.14710/jphi.v6i3.%p>

memastikan bahwa data pribadi dikelola dengan aman dan sesuai dengan prinsip-prinsip perlindungan privasi.

Selanjutnya, banyak pakar hukum berupaya merumuskan definisi privasi. Namun, sejumlah teori yang ada hanya membahas aspek dasar privasi secara terbatas dan kurang memiliki penerapan praktis. Oleh karena itu, hingga saat ini belum terdapat definisi yang tegas dan komprehensif mengenai privasi.¹⁰ Hak privasi merupakan salah satu hak fundamental yang diakui secara universal sebagai bagian dari hak asasi manusia. Hak ini memberikan perlindungan bagi individu terhadap intervensi yang tidak sah dari pihak lain, termasuk negara dan korporasi, dalam aspek kehidupan pribadi, komunikasi, serta data pribadi. Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) 1948 secara tegas menyatakan bahwa tidak seorang pun boleh menjadi sasaran intervensi sewenang-wenang dalam kehidupan pribadinya, keluarga, rumah, atau korespondensi, serta berhak mendapatkan perlindungan hukum terhadap pelanggaran semacam itu. Selain itu, Pasal 17 *International Covenant on Civil and Political Rights* (ICCPR) 1966, yang telah diratifikasi Indonesia melalui Undang-Undang Nomor 12 Tahun 2005, juga menegaskan perlindungan terhadap privasi individu dari gangguan yang tidak sah.

Di Indonesia, meskipun Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) tidak secara eksplisit menyebutkan hak privasi, namun Pasal 28G ayat (1) memberikan jaminan terhadap perlindungan diri pribadi, keluarga, dan kehormatan seseorang, yang dapat diinterpretasikan sebagai perlindungan terhadap hak privasi. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memperjelas hak individu dalam mengendalikan informasi pribadinya, termasuk hak untuk memberikan persetujuan terhadap pemrosesan data, hak untuk mengakses, memperbaiki, dan menghapus data pribadi mereka.

Hak privasi juga semakin mendapat perhatian dalam era digital, di mana data pribadi dapat dikumpulkan, dianalisis, dan digunakan untuk berbagai kepentingan, baik oleh sektor swasta maupun pemerintah.¹¹ Meskipun regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 dan Peraturan

¹⁰ Thomas D.C. Bennett. (2019). *Triangulating Intrusion in Privacy Law*. Oxford Journal of Legal Studies, 39 (4), pp. 751-778. <https://doi.org/10.1093/ojls/gqz024>

¹¹ Clifford Deannova Saputra, Gilang Septiawan Saputra, Fitri Aprilliani, Imelda Martinelli. (2024). Perspektif Hukum terhadap Privasi dan Perlindungan Data Pribadi di Era Digital. JIHP: Jurnal Ilmu Hukum, Humaniora dan Politik, 5 (1), hlm. 799- 810. <https://doi.org/10.38035/jihhp.v5i1>

Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) memberikan kerangka hukum terkait perlindungan data dalam transaksi elektronik, masih terdapat kekhawatiran terhadap potensi penyalahgunaan kewenangan negara dalam pengawasan digital.

Disisi lain, negara juga memiliki kepentingan dalam melakukan pengawasan digital untuk kepentingan keamanan nasional dan ketertiban umum. Hal ini sering kali menjadi dalih bagi negara untuk memperluas kewenangan dalam mengakses dan memantau data pribadi warga. Oleh karena itu, perlindungan hak privasi di Indonesia perlu terus diperkuat melalui mekanisme regulasi yang lebih transparan dan akuntabel, guna memastikan keseimbangan antara kepentingan negara dan hak individu terhadap privasi mereka. Contohnya adalah regulasi yang memungkinkan aparat keamanan mengakses data komunikasi tanpa transparansi yang jelas. Ketidakseimbangan muncul ketika regulasi lebih berpihak pada kepentingan negara dibandingkan dengan perlindungan individu. Contohnya, kasus dugaan kebocoran data pribadi dari PeduliLindungi, e-KTP, dan data SIM card menunjukkan bahwa perlindungan terhadap data pribadi masih lemah. Dalam situasi ini, hak privasi sebagai hak asasi manusia belum sepenuhnya dijamin dalam implementasi regulasi di Indonesia.

2. Analisis Hukum Tentang Keseimbangan Antara Pelindungan Data Pribadi Dan Kewenangan Negara Dalam Melakukan Pengawasan Digital di Indonesia

Hak atas perlindungan data pribadi berakar dari hak untuk menjaga kehidupan pribadi, yang dikenal sebagai *the right to private life*.¹² Konsep ini berkaitan erat dengan eksistensi manusia sebagai individu, sehingga setiap orang memiliki hak utama atas perlindungan data pribadinya. Meskipun hak privasi tidak secara eksplisit disebutkan dalam Undang-Undang Dasar 1945, prinsip ini tersirat dalam Pasal 28G ayat (1) UUD NRI 1945, yang menjamin perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, serta hak untuk merasa aman dari ancaman yang dapat membatasi kebebasan individu dalam bertindak atau tidak bertindak sesuai hak asasi mereka.¹³ Selain itu, perlindungan terhadap hak privasi juga diatur dalam peraturan perundang-undangan

¹² Upik Mutiara, Romi Maulana. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. Indonesian Journal of Law and Policy Studies, 1 (1), hlm. 43-55. <http://dx.doi.org/10.31000/ijlp.v1i1.2648>

¹³ Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. JA: Jurnal Al-Wasath, 2 (1), hlm. 19-32. <https://doi.org/10.47776/alwasath.v2i1.127>

lainnya, seperti Pasal 29 ayat (1) dan Pasal 30 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.¹⁴ Konsep data pribadi sendiri mencerminkan upaya untuk mengintegrasikan berbagai regulasi yang mengatur privasi dan data pribadi ke dalam satu kerangka hukum yang lebih komprehensif. Oleh karena itu, perlindungan privasi dan data pribadi memiliki sifat khas dan unik (*sui generis*) dalam sistem hukum.

Untuk menjamin perlindungan data pribadi, Indonesia telah mengadopsi beberapa regulasi yang mengatur bagaimana data dikumpulkan, diproses, dan digunakan, baik oleh sektor publik maupun swasta. Salah satu regulasi utama dalam hal ini adalah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU PDP menekankan prinsip perlindungan data pribadi, yang mencakup persetujuan eksplisit, dimana setiap pengumpulan dan pemrosesan data pribadi harus mendapatkan persetujuan dari pemilik data. Pemilik data memiliki hak untuk mengakses, mengoreksi, dan menghapus datanya, serta pihak yang mengelola data harus menjaga keamanan dan kerahasiaan data pribadi yang mereka kelola. Namun, meskipun UU PDP memberikan dasar hukum yang lebih kuat dalam perlindungan data, tantangan utama dalam implementasinya adalah mekanisme pengawasan dan penegakan hukum yang masih lemah. Tanpa pengawasan yang ketat dan independen, perlindungan data pribadi masih berisiko dilanggar, terutama oleh lembaga negara yang memiliki akses luas terhadap data digital masyarakat.

Efektivitas pelaksanaan undang-undang ini sangat bergantung pada implementasi dan pengawasan yang ketat. Diperlukan lembaga independen yang berfungsi sebagai pengawas dalam pelaksanaan perlindungan data pribadi, sehingga dapat mencegah potensi penyalahgunaan kewenangan oleh pemerintah atau pihak lain. Pembentukan lembaga semacam ini akan memastikan adanya mekanisme *checks and balances* dalam pengawasan digital, sehingga hak privasi individu tetap terjaga. Selain itu, partisipasi aktif masyarakat dalam mengawasi pelaksanaan undang-undang ini juga sangat penting. Masyarakat perlu diberikan edukasi mengenai hak-hak mereka terkait data pribadi, serta mekanisme pengaduan jika terjadi pelanggaran. Dengan demikian, masyarakat dapat berperan sebagai pengawas tambahan dalam memastikan bahwa pemerintah dan entitas lain mematuhi ketentuan yang berlaku. Pemerintah juga harus transparan dalam kebijakan pengawasan digital yang diterapkannya. Setiap tindakan

¹⁴ Republik Indonesia. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Tahun 1999 Nomor 165, Tambahan Lembaran Negara Nomor. 3886).

pengawasan harus didasarkan pada kepentingan yang jelas dan sesuai dengan peraturan perundang-undangan yang berlaku. Transparansi ini akan membangun kepercayaan masyarakat terhadap pemerintah dalam hal pengelolaan data pribadi.

Di sisi lain, negara memiliki kewenangan dalam pengawasan digital untuk tujuan keamanan nasional, penegakan hukum, serta pengelolaan sistem informasi dan transaksi elektronik. Beberapa regulasi yang memberikan kewenangan ini antara lain:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah mengalami perubahan pada tahun 2016 dan tahun 2024.¹⁵ UU ITE memberikan dasar hukum bagi pemerintah untuk mengawasi, mengontrol, dan bahkan memblokir konten digital yang dianggap melanggar hukum. Meskipun bertujuan untuk menjaga ketertiban digital, UU ITE sering dikritik karena digunakan untuk menindas kritik terhadap pemerintah, yang berpotensi melanggar kebebasan berekspresi dan privasi individu.
2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).¹⁶ Regulasi ini memberikan kewenangan kepada pemerintah untuk meminta akses terhadap sistem elektronik yang beroperasi di Indonesia, termasuk data pribadi pengguna. Regulasi ini menimbulkan kekhawatiran terkait potensi pengawasan yang berlebihan, terutama tanpa adanya mekanisme transparansi dan akuntabilitas yang kuat.
3. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.¹⁷ Aturan ini mewajibkan penyedia layanan digital untuk mendaftarkan diri ke pemerintah serta menyediakan akses bagi aparat dalam situasi tertentu. Regulasi ini menjadi kontroversial karena berpotensi memberikan akses luas kepada pemerintah terhadap data pribadi tanpa adanya mekanisme pengawasan yang independen.

Meskipun pengawasan digital oleh negara sering kali dilakukan dengan dalih keamanan nasional dan kepentingan publik, ada beberapa risiko yang bisa muncul, seperti penyalahgunaan wewenang apabila tidak adanya mekanisme control yang ketat,

¹⁵ Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

¹⁶ Republik Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).

¹⁷ Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat (Berita Negara 2020 Nomor 1376).

aparatus negara dapat menyalahgunakan kewenangan dalam mengakses data pribadi untuk tujuan politik atau kepentingan tertentu. Kurangnya transparansi dalam kebijakan pengawasan digital, sehingga masyarakat tidak memiliki akses terhadap informasi mengenai sejauh mana data mereka digunakan oleh pemerintah. Selain itu, pengawasan digital yang berlebihan dapat melanggar hak privasi, kebebasan berekspresi, serta hak-hak dasar lainnya yang dijamin dalam konstitusi dan hukum internasional.

Beberapa kasus di Indonesia menunjukkan bahwa mekanisme pengawasan terhadap lembaga negara dalam pengelolaan data masih lemah. Pemblokiran beberapa layanan digital seperti PayPal dan Steam pada tahun 2022 menunjukkan bagaimana regulasi pengawasan digital dapat berdampak langsung terhadap hak akses informasi masyarakat. Terkait pemblokiran terhadap 8 (delapan) situs dan aplikasi dengan traffic tinggi yakni PayPal, Yahoo, Epic Games, Steam, Dota, Counter Strike, Xandr.com, dan Origin (EA) dengan alasan situs dan aplikasi tersebut tidak terdaftar resmi Penyelenggara Sistem Elektronik (PSE) Lingkup Privat berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat tahun 2022 oleh Kementerian Komunikasi dan Informatika Republik Indonesia (KOMINFO RI), menurut LBH Jakarta, Pembatasan (Pemblokiran) situs internet dan aplikasi tersebut telah melahirkan apa yang disebut sebagai otoritarianisme yang memanfaatkan kuasa digital dalam rangka mengendalikan teknologi sebagai alat melindungi kepentingan (*digital authoritarianism*), sehingga memblokir atau mematikan situs internet dan aplikasi yang tidak memenuhi syarat pembatasan adalah tindakan yang tidak pernah dapat dibenarkan.¹⁸

Dalam konteks hukum, teori kepastian hukum (*legal certainty*) menjadi relevan untuk membahas bagaimana regulasi yang ada memberikan jaminan terhadap perlindungan hak individu dan batasan kewenangan negara. Kepastian hukum mengacu pada kejelasan, konsistensi, dan prediktabilitas hukum dalam memberikan perlindungan kepada warga negara serta mengatur batas-batas kekuasaan pemerintah.¹⁹ Teori kepastian hukum menekankan pentingnya hukum yang jelas, tidak ambigu, dan dapat diprediksi dalam penerapannya. Akan tetapi, adanya ketidakkonsistenan antar Regulasi

¹⁸<https://bantuanhukum.or.id/lbh-jakarta-pemblokiran-situs-internet-dan-aplikasi-oleh-kominfo-merupakan-bentuk-otoritarianisme-digital/> diakses pada 12 September 2025, Pukul. 13.00WIB.

¹⁹ Mario Julyano dan Aditya Yuli Sulistyawan. (2019). Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum. JURNAL CREPIDO, 1 (1), hlm. 13-22. <https://doi.org/10.14710/crepido.1.1.13-22>

seperti, UU PDP yang secara eksplisit menetapkan hak individu atas data pribadi serta kewajiban pengendali data, sedangkan UU ITE, PP PSTE, dan Permenkominfo No. 5 Tahun 2020 memberikan kewenangan luas bagi pemerintah dalam pengawasan digital, tetapi tidak secara spesifik mengatur batasan yang jelas untuk mencegah penyalahgunaan kewenangan.

Ketidakseimbangan dalam regulasi ini berpotensi menciptakan ketidakpastian hukum bagi warga negara karena tidak adanya jaminan bahwa pengawasan digital dilakukan secara proporsional dan tidak sewenang-wenang. Selain itu, dapat berakibat pada lemahnya perlindungan terhadap privasi individu dan kurangnya mekanisme hukum yang transparan bagi masyarakat untuk menggugat kebijakan pengawasan digital yang dianggap melanggar hak mereka. Oleh karena itu, diperlukan penyempurnaan regulasi dengan menekankan transparansi, akuntabilitas, serta pembentukan lembaga independen yang bertugas mengawasi pelaksanaan kebijakan pengawasan digital agar tetap sejalan dengan prinsip hak asasi manusia dan kepastian hukum.

3. Analisis Kewenangan Negara dalam Pengawasan Digital

Teknologi pemrosesan data modern menawarkan banyak keunggulan dibandingkan metode manual yang lebih lambat. Namun, kemajuan teknologi ini juga menghadirkan berbagai tantangan. Salah satu permasalahan utama adalah potensi ancaman terhadap hak privasi individu. Saat ini, data pribadi dapat dikumpulkan, disimpan, dan dikombinasikan tanpa batasan yang jelas, serta lebih mudah diakses dibandingkan dengan era sebelum perkembangan teknologi ini. Selain itu, data pribadi dapat disebarluaskan dan dimanipulasi informasinya di berbagai sektor, sering kali tanpa sepengetahuan pemiliknya. Terlebih lagi, ada kemungkinan pemerintah dan perusahaan mengumpulkan informasi pribadi warga negara, yang dapat berpotensi mengancam kebebasan individu.²⁰

Dalam UU PDP, pengawasan terhadap perlindungan data pribadi berada di bawah Kementerian Komunikasi dan Informatika (Kominfo).²¹ Namun, banyak kritik menyebutkan bahwa Kominfo bukanlah lembaga yang sepenuhnya independen dan

²⁰ J Lee Riccardi, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?*, Boston College International and Comparative Law Review, 6 (1), hlm. 24. <https://core.ac.uk/download/pdf/80399406.pdf>

²¹ <https://www.komdigi.go.id/berita/artikel/detail/era-baru-perlindungan-data-pribadi> diakses pada tanggal 12 September 2025, Pukul 13.20 WIB.

masih memiliki konflik kepentingan, mengingat pemerintah juga memiliki kepentingan dalam pengelolaan data dan pengawasan digital. Sebagai perbandingan, Uni Eropa memiliki *European Data Protection Board* (EDPB) sebagai lembaga pengawas independen yang bertugas menegakkan *General Data Protection Regulation* (GDPR). Hal ini berbeda dengan Indonesia, di mana belum ada lembaga independen yang benar-benar memiliki kewenangan penuh untuk mengawasi implementasi UU PDP.

Beberapa regulasi yang ada bertujuan untuk menjaga keamanan nasional dan ketertiban publik, tetapi di sisi lain, implementasinya memicu kekhawatiran terkait privasi dan kebebasan berekspresi. Indonesia memiliki beberapa regulasi yang memberikan dasar hukum bagi pemerintah dalam melakukan pengawasan digital, di antaranya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 (revisi 2016 dan 2024). Regulasi ini memberikan kewenangan kepada pemerintah untuk mengontrol dan memblokir konten yang dianggap melanggar hukum. UU ITE memberikan landasan hukum bagi pemerintah dalam melakukan pengawasan terhadap aktivitas digital warga negara. Dalam ketentuan Pasal 40 Ayat (2A) dan (2B) Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik,²² Pemerintah berwenang melakukan pemutusan akses terhadap informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar hukum, termasuk ujaran kebencian, terorisme, serta penyebaran berita bohong. Selanjutnya, pada pasal 43 Ayat (5), Aparat penegak hukum dapat melakukan penyadapan dalam rangka penegakan hukum, namun harus dilakukan sesuai dengan peraturan perundang-undangan yang berlaku. Kritik utama terhadap UU ITE adalah pasal karet yang berpotensi mengekang kebebasan berekspresi dan membuka ruang bagi penyalahgunaan wewenang.

Regulasi selanjutnya, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). PP PSTE memberikan kewenangan lebih luas kepada pemerintah dalam pengawasan digital. Ketentuan Pasal 5 dan 6, menetapkan kewajiban bagi setiap Penyelenggara Sistem Elektronik (PSE), baik domestik maupun asing, untuk memberikan akses bagi pemerintah terhadap sistem elektronik mereka dalam keadaan tertentu. Pasal 41 Ayat (1) menegaskan bahwa

²² Republik Indonesia, Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905).

pemerintah dapat meminta akses terhadap sistem elektronik untuk kepentingan penegakan hukum, keamanan nasional, serta ketertiban umum. Selanjutnya, ketentuan Pasal 83, PSE wajib menyimpan data pengguna di Indonesia, yang memberikan kesempatan bagi pemerintah untuk mengakses data tersebut jika diperlukan. PP PSTE menjadi dasar bagi kebijakan pemerintah dalam mengatur PSE yang beroperasi di Indonesia, tetapi juga menuai kritik karena berpotensi membuka peluang pengawasan yang berlebihan terhadap aktivitas digital masyarakat tanpa mekanisme pengawasan yang transparan.

Ada pula Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 5 Tahun 2020. Aturan ini mewajibkan penyelenggara layanan digital, termasuk perusahaan teknologi global seperti Google, Facebook, dan WhatsApp, untuk mendaftarkan diri ke pemerintah. Pemerintah juga diberikan wewenang untuk meminta akses terhadap data pengguna dalam situasi tertentu, yang menimbulkan kekhawatiran mengenai potensi penyalahgunaan. Dalam ketentuan Pasal 7 Ayat (2), Pemerintah dapat meminta akses terhadap data pengguna dari PSE dalam rangka kepentingan penegakan hukum. Pada Pasal 9 ditegaskan bahwa PSE wajib memastikan sistemnya tidak digunakan untuk menyebarkan informasi yang melanggar hukum, termasuk berita bohong dan ujaran kebencian. Selanjutnya, pada Pasal 13 Ayat (1) dijelaskan bahwa Pemerintah dapat melakukan pemblokiran terhadap PSE yang tidak mematuhi peraturan yang berlaku.

Selain itu, ada pula Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) bertujuan untuk melindungi data pribadi masyarakat dengan memberikan hak kepada individu atas pengelolaan data mereka. UU PDP merupakan regulasi utama yang mengatur bagaimana data pribadi dapat dikumpulkan, diproses, dan digunakan oleh berbagai pihak, termasuk pemerintah. Beberapa poin penting terkait pengawasan digital dalam UU PDP antara lain terdapat pada ketentuan Pasal 35 dan 36, dimana diatur bahwa Pemerintah dapat mengakses atau memproses data pribadi dalam keadaan tertentu, seperti untuk kepentingan keamanan nasional, pertahanan, dan penegakan hukum. Pada Pasal 20 diatur setiap pengelolaan data pribadi harus mendapatkan persetujuan dari pemilik data, kecuali dalam situasi tertentu yang ditetapkan oleh hukum. Selanjutnya, Pasal 55 menegaskan bahwa larangan penyalahgunaan data pribadi oleh pihak yang mengelolanya, termasuk lembaga negara, dengan ancaman sanksi pidana jika terjadi pelanggaran. Melalui UU PDP, negara

diberikan kewenangan untuk mengakses data warga negara dalam situasi tertentu, tetapi dengan batasan yang ketat agar tidak melanggar hak privasi.

Pengawasan digital oleh negara merupakan praktik yang dilakukan untuk menjaga keamanan nasional, mencegah kejahatan siber, serta mengawasi aktivitas digital yang berpotensi melanggar hukum. Namun, batas kewenangan negara dalam melakukan pengawasan digital harus tetap memperhatikan prinsip-prinsip perlindungan hak asasi manusia, khususnya hak atas privasi dan kebebasan berekspresi. Beberapa aspek dalam implementasi regulasi ini dapat dianggap berlebihan. Beberapa indikasi kelebihan kewenangan negara dalam pengawasan digital, seperti:

- a) **Minimnya mekanisme pengawasan independen.** Regulasi yang memberikan kewenangan kepada pemerintah untuk mengakses sistem elektronik dan data pribadi tidak disertai dengan mekanisme pengawasan yang cukup ketat. Tidak ada lembaga independen yang berwenang untuk memastikan bahwa akses terhadap data pribadi tidak disalahgunakan oleh pemerintah atau aparat penegak hukum.
- b) **Potensi penyalahgunaan pasal karet dalam UU ITE** karena pasal-pasal yang multitafsir, terutama terkait pencemaran nama baik dan ujaran kebencian. Banyak kasus di mana individu atau jurnalis dikriminalisasi berdasarkan interpretasi yang luas terhadap UU ITE, yang menunjukkan bahwa pengawasan digital dapat digunakan sebagai alat untuk membungkam kritik.
- c) **Pengawasan yang tidak transparan dan kurangnya akuntabilitas.** Masyarakat sering kali tidak memiliki akses terhadap informasi tentang bagaimana pengawasan digital dilakukan dan bagaimana data mereka dikelola oleh pemerintah. Serta, tidak adanya laporan publik yang transparan mengenai sejauh mana pemerintah menggunakan kewenangannya dalam mengakses dan mengontrol data digital.

PENUTUP

Kesimpulan

Dalam konteks global, banyak negara yang menghadapi tantangan serupa dalam menyeimbangkan antara perlindungan data pribadi dan kebutuhan pengawasan oleh negara. Beberapa negara telah membentuk lembaga independen yang bertugas mengawasi pelaksanaan undang-undang perlindungan data pribadi, sehingga dapat menjadi contoh bagi Indonesia dalam mengimplementasikan kebijakan serupa.

Pengawasan digital yang dilakukan oleh negara memang diperlukan untuk menjaga keamanan siber dan mencegah kejahatan digital. Namun, di Indonesia, regulasi yang ada memberikan kewenangan yang cukup luas bagi pemerintah tanpa adanya mekanisme pengawasan yang ketat dan transparan. Beberapa aturan seperti PP PSTE dan Peraturan Menteri Kominfo Nomor 5 Tahun 2020 memungkinkan pemerintah untuk mengakses data pengguna tanpa kontrol yang memadai, sehingga meningkatkan risiko penyalahgunaan kewenangan. Untuk mencegah pengawasan digital yang berlebihan.

Saran

Perlu dilakukan revisi regulasi yang lebih jelas mengenai batas kewenangan negara dalam pengawasan digital, mekanisme pengawasan independen untuk memastikan transparansi dalam akses data pengguna oleh pemerintah, serta jaminan perlindungan hak asasi manusia agar pengawasan digital tidak digunakan untuk membatasi kebebasan berekspresi dan privasi individu. Dengan pendekatan yang lebih seimbang antara kepentingan keamanan dan perlindungan hak privasi, regulasi pengawasan digital di Indonesia dapat lebih adil dan akuntabel.

DAFTAR PUSTAKA

Buku

- HS, Salim & Erlies Septianan Nurbani. Penerapan Teori Hukum pada Penelitian Tesis dan Disertasi. Jakarta: RajaGrafindo Persada, 2018.
- Marzuki, Peter Mahmud. "Penelitian Hukum Edisi Revisi". Jakarta: Kencana, 2024.

Artikel Jurnal

- Ayiliani, Fanisa Mayda, Elfia Farida. Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, Vol. 6 no. 3, 2024, 431-455.
- Bennett, Thomas D.C. Triangulating Intrusion in Privacy Law. *Oxford Journal of Legal Studies*, Vol. 39, no. 4, 2019 751-778.
- Boy, Three, dan Ariawan. "Peran Undang-Undang Perlindungan Data Pribadi dan Hukum Telekomunikasi dalam SPBE di Indonesia", *UNES Law Review*, Vol. 6, no. 2, 2023
- Gunadi, Chaterine Grace, Danishel Subiran, et.all. "Perlindungan Hukum Atas Kebocoran Data Pribadi. Proceeding of Conference on Law and Social Studies". 2023.
- Julyano, Mario dan Aditya Yuli Sulistyawan. Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum. *JURNAL CREPIDO*, Vol. 1, no. 1, 2019: 13-22. <https://doi.org/10.14710/crepido.1.1.13-22>
- Kusnadi, Sekaring Ayumeida dan Andy Usmina Wijaya. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi". *JA: Jurnal Al-Wasath*, Vol. 2, no. 1, 2021: 19-32. <https://doi.org/10.47776/alwasath.v2i1.127>
- Mutiara, Upik, Romi Maulana. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi". *Indonesian Journal of Law and Policy Studies*, Vol. 1, no. 1, 2020: hlm. 43-55. <http://dx.doi.org/10.31000/ijlp.v1i1.2648>
- Nirwana, Muhammad Alfaruq. "Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual". *Jurnal Al-Wasath*, Vol. 3, no. 2, 2022: 93-104. <https://journal.unusia.ac.id/index.php/alwasath/article/download/609/339/1789>
- Riccardi, J Lee. "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?", *Boston College International and Comparative Law Review*, Vol. 6, no. 1, 1983: 24. <https://core.ac.uk/download/pdf/80399406.pdf>
- Saputra, Clifford Deannova, Gilang Septiawan Saputra, Fitri Aprilliani, Imelda Martinelli. "Perspektif Hukum terhadap Privasi dan Perlindungan Data Pribadi di Era Digital". *JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik*, Vol. 5 no. 1, 2024: 799- 810. <https://doi.org/10.38035/jihhp.v5i1>

Peraturan Perundang-Undangan

Republik Indonesia, Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Republik Indonesia, Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Republik Indonesia. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Tahun 1999 Nomor 165, Tambahan Lembaran Negara Nomor. 3886).

Republik Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat (Berita Negara 2020 Nomor 1376).

Website

<https://www.komdigi.go.id/berita/artikel/detail/era-baru-perlindungan-data-pribadi> diakses pada tanggal 12 September 2025.

<https://bantuanhukum.or.id/lbh-jakarta-pemblokiran-situs-internet-dan-aplikasi-oleh-kominfo-merupakan-bentuk-otoritarianisme-digital/> diakses pada 12 September 2025.