

## Peran Negara dan Efektivitas Politik Hukum Nasional Melindungi Keamanan Data dan Hak Privasi Digital

M. Zainun Nasihin<sup>1\*</sup>, Hwian Christianto<sup>2</sup>

<sup>1,2</sup> Ilmu Hukum, Universitas Surabaya, Indonesia

[bagindaink@gmail.com](mailto:bagindaink@gmail.com)<sup>1</sup>, [hw\\_christianto@staff.ubaya.ac.id](mailto:hw_christianto@staff.ubaya.ac.id)<sup>2</sup>

Alamat: Universitas Surabaya

Korespondensi penulis: [\\*bagindaink@gmail.com](mailto:*bagindaink@gmail.com)

**Abstract.** *This article analyzes the role of the state and the effectiveness of national legal politics in ensuring data security and the privacy rights of citizens in the era of digital globalization. The research employs a normative juridical method using statutory, conceptual, and doctrinal approaches, supplemented by an empirical literature review on data breach incidents in Indonesia. Philosophically, personal data protection is grounded in the values of humanity and justice embodied in Pancasila, and constitutes an integral part of human rights as guaranteed by the 1945 Constitution of the Republic of Indonesia. Juridically, the enactment of Law Number 27 of 2022 concerning Personal Data Protection marks a significant milestone in developing secure and accountable data governance. The findings reveal that the implementation of this regulation remains weak, as evidenced by the absence of an independent data protection authority, the lack of comprehensive implementing regulations, poor inter-agency coordination, and low public literacy regarding digital security. From the perspective of legal politics, the state's response to digital security challenges tends to be reactive and has yet to become fully progressive in accordance with technological advancements. This article asserts that the state must function not only as a regulator but also as a facilitator and protector by strengthening the legal framework, enhancing cyber resilience, establishing an independent data protection authority, and promoting international collaboration. Through a progressive and responsive legal approach, the state can safeguard privacy rights while upholding digital sovereignty amid the rapid expansion of global digitalization.*

**Keywords:** *Personal Data Protection, Legal Politics, Cybersecurity.*

**Abstrak.** Artikel ini menganalisis peran negara serta efektivitas politik hukum nasional dalam menjamin keamanan data dan hak privasi warga negara di era globalisasi digital. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan doktrinal, yang dilengkapi dengan telaah literatur empiris mengenai kasus kebocoran data di Indonesia. Secara filosofis, perlindungan data pribadi berlandaskan pada nilai-nilai kemanusiaan dan keadilan yang terkandung dalam Pancasila, serta merupakan bagian integral dari hak asasi manusia sebagaimana dijamin dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Secara yuridis, disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi tonggak penting dalam pembangunan tata kelola data yang aman dan akuntabel. Namun, temuan penelitian menunjukkan bahwa implementasi regulasi tersebut masih lemah, yang ditandai dengan belum adanya otoritas perlindungan data yang independen, belum lengkapnya peraturan pelaksana, lemahnya koordinasi antar lembaga, serta rendahnya literasi masyarakat terkait keamanan digital. Dari perspektif politik hukum, respons negara terhadap tantangan keamanan digital cenderung bersifat reaktif dan belum sepenuhnya progresif seiring perkembangan teknologi. Artikel ini menegaskan bahwa negara tidak hanya harus berfungsi sebagai regulator, tetapi juga sebagai fasilitator dan pelindung dengan memperkuat kerangka hukum, meningkatkan ketahanan

\*Corresponding author, [\\*bagindaink@gmail.com](mailto:*bagindaink@gmail.com)

siber, membentuk otoritas perlindungan data yang independen, serta mendorong kerja sama internasional. Melalui pendekatan hukum yang progresif dan responsif, negara dapat melindungi hak privasi sekaligus menjaga kedaulatan digital di tengah pesatnya perkembangan digitalisasi global.

**Kata kunci:** Perlindungan Data Pribadi, Politik Hukum, Keamanan Siber.

## **LATAR BELAKANG**

Pemilihan kepala desa (Pilkades) merupakan instrumen demokrasi lokal yang memiliki pran strategis dalam menentukan arah pemerintahn desa serta menjamin partisipasi masyarakat secara langsung (Suratno 2017, 15). Dalam kerangka hukum nasional, pelaksanaan Pilkades telah diatur secara normatif melalui Undang-Undang Desa yang menekankan prinsip demokrasi, kepastian hukum, dan keteraturan dalam penyelenggaraannya (Satria, 2020, hlm. 14). Namun, dalam praktiknya, dinamika politik lokal kerap menghadirkan persoalan yang kompleks, salah satunya adalah kebijakan penundaan Pilkades yang terjadi di Kabupaten Sampang, Jawa Timur (Mushthofa, Aminah, & Siropi, 2023, hlm. 58).

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa perubahan mendasar dalam berbagai aspek kehidupan masyarakat, termasuk cara berinteraksi, bertransaksi, dan mengelola data, Kemajuan teknologi digital menempatkan data sebagai komoditas yang sangat berharga. Peran utama negara adalah membentuk regulasi perlindungan data siber dan keamanan siber. Perlindungan terhadap data pribadi merupakan hak warga negara yang memerlukan kapasitas dan kapabilitas negara untuk menjaminnya (Aji, 2023a)

Pada era digital saat ini data pribadi menjadi sesuatu yang memiliki nilai ekonomi tinggi sekaligus memantik potensi timbulnya risiko serius apabila disalahgunakan dengan tujuan jahat oleh pihak yang tidak bertanggung jawab dan tentunya hal itu akan mengancam keamanan masyarakat, karena kerugian tidak hanya ditanggung negara namun yang mengalami kerugian besar justru masyarakat, Secara filosofis, perlindungan data pribadi dan keamanan siber berakar pada nilai kemanusiaan dan keadilan sebagaimana tercermin dalam sila kedua dan kelima Pancasila, yaitu *Kemanusiaan yang adil dan beradab* serta *Keadilan sosial bagi seluruh rakyat Indonesia*. Perlindungan data pribadi bukan sekadar isu teknis (Mardiyati, 2025), melainkan bentuk penghormatan terhadap martabat

manusia (human dignity) dan hak privasi sebagai bagian dari hak asasi manusia. Negara memiliki tanggung jawab moral dan konstitusional untuk menjamin rasa aman warganya di ruang digital sebagaimana dijamin oleh Pasal 28G ayat (1) UUD 1945, yang menegaskan hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda, Pasal 28J ayat (1) UUD 1945, yang memberikan dasar pembatasan hak individu demi perlindungan hak orang lain dan kepentingan umum. Dengan demikian, secara filosofis, regulasi perlindungan data pribadi harus berorientasi pada keseimbangan antara kebebasan individu dan kepentingan kolektif, serta menjunjung tinggi prinsip keamanan digital sebagai bagian dari keadilan sosial di era transformasi digital.

Beberapa kasus kebocoran data terus meningkat di Indonesia, salah satu contoh dikutip dari portal media antara Dilaporkan bahwa sekitar 6 juta data pembayar pajak (NPWP) di Indonesia bocor dan dijual oleh hacker dengan nama alias Bjorka. Data meliputi NPWP, NIK, alamat, email, telepon hingga beberapa pejabat negara (Finance Minister Orders Probe into Alleged Taxpayer Data Leak - ANTARA News Mataram, n.d.), contoh kejadian yang terjadi tersebut menunjukkan lemahnya sistem perlindungan dan keamanan siber serta menegaskan pentingnya regulasi yang komprehensif dalam mengatur pengelolaan data pribadi karena Dari sisi yuridis, urgensi regulasi perlindungan data pribadi dan keamanan siber di Indonesia didorong oleh meningkatnya kasus kebocoran data dan kejahatan siber.

Kebocoran data pribadi seperti kasus bocornya enam juta data pembayar pajak menunjukkan bahwa sistem perlindungan data di Indonesia masih memiliki kelemahan yang serius. Urgensi pembentukan dan penerapan regulasi yang kuat terletak pada upaya melindungi hak privasi warga negara, Hak privasi adalah hak konstitusional warga negara yang telah diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Hak konstitusional adalah kewajiban dari suatu negara terhadap warga negaranya (Kusnadi, 2021), oleh karenanya kewajiban negara terhadap warganya berguna untuk menjaga kepercayaan publik terhadap institusi pemerintah, serta memastikan keamanan informasi dalam penyelenggaraan layanan publik dan kegiatan ekonomi digital, kebijakan tersebut tanpa penguatan kerangka hukum dan kesiapan kelembagaan, kebocoran data

dapat menimbulkan kerugian sosial, ekonomi, dan bahkan mengancam keamanan nasional, Oleh karena itu, keberadaan dan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi sangat penting sebagai fondasi tata kelola data yang aman dan bertanggung jawab di Indonesia. (UU No. 27 Tahun 2022, n.d.)

Keamanan siber menjadi aspek yang tidak dapat dipisahkan dari isu perlindungan data pribadi, menurut Badan Siber dan Sandi Negara (BSSN) menyebut bahwa kita adalah target setiap detik, setiap menit. Akses kita ke dalam sistem menjadi incaran utama para penyerang dari seluruh dunia (Akun Bank hingga WhatsApp Bisa Diserang, BSSN Minta Masyarakat Waspada, n.d.). Dengan ancaman siber yang semakin kompleks dan terorganisir menuntut adanya koordinasi lintas lembaga serta kebijakan nasional yang adaptif dan berorientasi pada *resilience atau adaptasi yang positif dan berfungsi baik* saat dihadapkan pada kesulitan, trauma, tragedi, ancaman, atau sumber permasalahan yang signifikan. Dalam konteks ini, kerangka hukum ke depan perlu diarahkan pada harmonisasi antara perlindungan hak individu, kepentingan publik, dan kebutuhan industri digital, dengan mengacu pada standar global seperti General Data Protection Regulation (GDPR) yang telah diterapkan di Uni Eropa. Dalam konteks ini, teori hukum progresif yang digagas oleh Satjipto Rahardjo menjadi sangat relevan. Teori ini menegaskan bahwa hukum harus hidup dan bergerak mengikuti kebutuhan masyarakat, bukan sekadar menegakkan teks undang-undang secara kaku. Teori hukum progresif menuntut agar hukum mampu menyesuaikan diri dengan perkembangan teknologi, termasuk kecerdasan buatan dan pengelolaan data pribadi, demi melindungi kepentingan manusia. (Junaidi et al., 2024) Dengan pendekatan progresif, perlindungan data pribadi tidak hanya dipandang sebagai urusan administratif, tetapi juga sebagai manifestasi perlindungan martabat dan kebebasan individu di era digital.

Secara sosiologis, keberadaan regulasi perlindungan data pribadi sangat penting untuk menjawab kebutuhan masyarakat akan rasa aman dan kepercayaan di ruang digital, Masyarakat kini bergantung pada layanan digital seperti e-commerce, e-banking, dan media sosial yang melibatkan pengumpulan data secara

masif. Namun, masih terdapat tantangan implementasi, Seperti dikemukakan dalam *Jurnal Humaniora dan Ilmu Sosial (JHSS)* (Universitas Pakuan, 2024), Pemerintah Indonesia berkomitmen kuat untuk mengatasi ancaman keamanan siber dan kebocoran data, namun lemahnya kesadaran publik, keterbatasan anggaran, dan minimnya edukasi menjadi hambatan dalam memperkuat keamanan siber di Indonesia. (Nurulita, 2025) , Karena itu, keberhasilan perlindungan data pribadi tidak hanya bergantung pada aturan hukum tertulis, tetapi juga pada perubahan perilaku sosial, edukasi publik, dan sinergi lintas sector. Sedangkan dalam perspektif sosiologi hukum, urgensi regulasi perlindungan data dan keamanan siber muncul karena transformasi digital telah menimbulkan konsekuensi sosial yang signifikan.

Regulasi yang responsif dan adaptif merupakan elemen kunci dalam menjaga keseimbangan antara kepentingan publik, keamanan individu, dan pembangunan sosial-ekonomi di era digital. Perkembangan teknologi seperti Artificial Intelligence (AI), Internet of Things (IoT), big data analytics, hingga sistem berbasis cloud telah mendorong perubahan signifikan dalam perilaku masyarakat dan tata kelola informasi. Perubahan ini menuntut kerangka hukum yang mampu bergerak seiring percepatan digitalisasi, agar negara tidak tertinggal dalam melindungi kepentingan warganya. Sejumlah penelitian global menunjukkan bahwa regulasi yang lambat merespons perkembangan teknologi berpotensi meningkatkan risiko manipulasi data, eksploitasi privasi, serta pelemahan legitimasi negara dalam tata kelola digital (Hartzog, 2018). Oleh karena itu, kebutuhan akan pembaruan hukum yang antisipatif menjadi semakin mendesak (Simhadri, 2025)

Di tengah meningkatnya angka kebocoran data dan serangan siber, regulasi adaptif berfungsi sebagai mekanisme mitigasi risiko yang strategis. Negara tidak hanya dituntut membentuk regulasi, tetapi juga memperkuat tata kelola keamanan siber, meningkatkan kapasitas lembaga pengawas, serta menyelaraskan regulasi nasional dengan standar global seperti GDPR. Literatur internasional menunjukkan bahwa perlindungan data yang efektif hanya dapat terwujud apabila terdapat kerangka hukum yang kuat, mekanisme pengawasan yang independen, dan tingkat literasi digital yang memadai di masyarakat (Greenleaf, 2021). Selain itu, tata kelola

data modern membutuhkan pendekatan lintas sektor yang memperhatikan risiko ekonomi, sosial, dan geopolitik dalam ruang digital yang semakin terhubung.

Bertolak dari urgensi tersebut, penelitian ini merumuskan dua pertanyaan utama. Pertama, bagaimana peran negara dalam menjamin keamanan data digital di tengah transformasi digital yang semakin kompleks? Kedua, sejauh mana politik hukum nasional mampu memberikan perlindungan yang memadai terhadap hak privasi warga negara di tengah pesatnya perkembangan teknologi informasi dan globalisasi digital? Rumusan masalah ini penting karena literatur internasional menegaskan bahwa efektivitas tata kelola digital sangat dipengaruhi oleh kapasitas negara dalam mengintegrasikan kebijakan, regulasi, dan pengawasan secara konsisten (Gstrein, 2023). Dengan demikian, pertanyaan tersebut berfungsi untuk menguji kemampuan negara dalam menyeimbangkan kemajuan teknologi dan perlindungan hak asasi.

Penelitian ini bertujuan mengevaluasi kesiapan negara baik secara regulatif, institusional, maupun kebijakan politik hukum dalam menghadapi tantangan perlindungan data pribadi dan keamanan siber. Pendekatan hukum progresif sangat diperlukan agar negara tidak hanya berperan sebagai regulator, tetapi juga sebagai fasilitator dan pelindung dalam ekosistem digital. Literatur terkini menegaskan perlunya pembentukan otoritas perlindungan data yang independen, tata kelola berbasis akuntabilitas, serta kerja sama internasional yang lebih kuat untuk menjamin kedaulatan digital (Hofmann & Pawlak, 2023). Melalui pendekatan tersebut, diharapkan negara mampu menyusun politik hukum yang adaptif dan berorientasi pada perlindungan hak privasi serta ketahanan siber nasional.

## **METODE PENELITIAN**

Metode penelitian yang digunakan dalam kajian ini adalah metode yuridis normatif dengan pendekatan multidimensional yang mencakup pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan doktrinal (*doctrinal approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang berkaitan dengan

perlindungan data pribadi dan keamanan siber, khususnya Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pendekatan konseptual digunakan untuk mengkaji konsep hak privasi, keamanan digital, serta teori hukum progresif sebagai landasan analisis dalam memahami dinamika hukum di era transformasi digital. Sementara itu, pendekatan doktrinal dilakukan dengan menelaah pandangan para ahli hukum dan literatur ilmiah yang relevan guna memperkuat argumentasi penelitian.

Selain itu, penelitian ini juga dilengkapi dengan studi literatur empiris terhadap berbagai kasus kebocoran data di Indonesia untuk memberikan gambaran faktual mengenai kondisi perlindungan data dan keamanan siber. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan mengkaji bahan hukum primer, sekunder, dan tersier. Analisis data dilakukan secara kualitatif dengan metode deskriptif-analitis, yaitu menguraikan, menginterpretasikan, dan mengevaluasi efektivitas politik hukum nasional dalam menjamin perlindungan data pribadi serta merumuskan rekomendasi yang bersifat progresif dan adaptif.

## **HASIL DAN PEMBAHASAN**

### **Peran negara dalam menjamin keamanan data digital di era transformasi digital saat ini**

Arus digitalisasi di berbagai sektor publik dan privat membawa konsekuensi terhadap meningkatnya risiko kebocoran data, Disini peran negara dalam menjamin keamanan data digital menjadi bagian integral dari pelaksanaan fungsi negara sebagaimana termaktub dalam Pembukaan UUD 1945 untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia(Winata, 2020), Menurut Danrivanto Budhijanto, pembentukan regulasi keamanan data tidak hanya berkaitan dengan aspek teknis pengelolaan sistem elektronik, tetapi juga merupakan implementasi kewajiban negara dalam menegakkan hak konstitusional warga atas privasi dan perlindungan diri pribadi. Ia menegaskan bahwa Pemberlakuan legislasi dan regulasi yang dikombinasikan dengan penegakan hukum yang serius tetap diperlukan untuk memandu perilaku masyarakat.

Kecepatan perkembangan teknologi menjadi permasalahan tersendiri bagi hukum, Saat ini perkembangan teknologi sangatlah pesat sementara pengaturan hukum terhadap perkembangan teknologi baru dijalankan setelah teknologi tersebut telah diterapkan di masyarakat luas. Oleh sebab itu penerapan hukum sangatlah diperlukan seiring dengan perkembangan teknologi agar perkembangan teknologi tersebut dapat bermanfaat bagi pengguna terutama masyarakat di Indonesia. (Sinaga, 2024) Pelanggaran data dapat menyebabkan rusaknya reputasi korporasi, tuntutan hukum berisiko tinggi, dan kerentanan keamanan nasional (Budhijanto, 2023a), Kelemahan sistem hukum dan lemahnya penegakan regulasi yang ada mengindikasikan bahwa pembentukan dan pembaruan aturan keamanan digital harus bersifat adaptif terhadap perkembangan teknologi yang berjalan cepat, dalam teori hukum progresif sebagaimana dikembangkan oleh Prof. Dr. Satjipto Rahardjo, S.H., dalam orientasinya Hukum untuk manusia, bukan manusia untuk hukum, hal ini jika di implikasikan terhadap perlindungan data pribadi dapat bermakna Undang-Undang data pribadi harus melindungi hak individu, bukan sekadar formalitas administratif, maka negara harus berperan dalam pembentukan serta pembaharuan serta melaksanakan aturan tersebut.

Menurut Badan Siber dan Sandi Negara (BSSN) dalam *Laporan Tahunan Keamanan Siber Indonesia tahun 2023* Dalam konteks keamanan siber, peran negara bukan hanya sebagai regulator, tetapi juga sebagai fasilitator dan pelindung, guna menjamin ketahanan ruang siber dari ancaman baik internal maupun eksternal. (BSSN, 2025), statement tersebut dapat dimaknai dalam hal ini negara harus hadir tidak hanya sebagai regulator atau pembuat Undang-Undang, tetapi juga sebagai pelaksana dalam menjamin keamanan digital, dalam pendapat lain Negara tidak cukup hanya menetapkan aturan hukum, tetapi juga wajib memastikan tersedianya infrastruktur dan mekanisme perlindungan yang menjamin keamanan data serta kepercayaan masyarakat terhadap sistem digital nasional. (Rosadi, 2023), oleh karena itu tugas negara tidak hanya menjadi regulator atau pembuat peraturan, namun juga memastikan peraturan tersebut berjalan dan dapat melindungi masyarakat Indonesia khususnya di dunia digital dengan segenap kemampuan negara demi menjaga kedaulatan negara. Sedangkan dari sudut pandang perspektif

hukum progresif, pembentukan regulasi tersebut belum cukup hanya berhenti pada *pembuatan aturan*, tetapi juga harus menjamin keadilan substantif. Artinya, hukum harus menjadi alat pembebasan dan perlindungan, bukan sekadar kontrol. Satjipto Rahardjo menyatakan bahwa *hukum bukan untuk dirinya sendiri, melainkan untuk manusia. selain itu* Perkembangan teknologi digital telah membawa transformasi besar dalam sistem hukum di Indonesia (Dinata, 2025) Oleh karena itu, negara melalui politik hukumnya harus terus memperbaharui regulasi digital agar sesuai dengan perkembangan teknologi dan kebutuhan sosial masyarakat.

Negara dengan otoritas dan kemampuan serta kedaulatan yang dimilikinya bisa melakukan beberapa cara agar dapat memenuhi kewajibannya tersebut yang pertama adalah dengan melalui kebijakan strategis, salah satu kebijakan strategis yang bisa dilakukan adalah karena Undang-Undang yang mengatur perlindungan data pribadi telah ada maka selanjutnya membuat aturan turunan terkait teknis dalam hal keamanan data digital, selanjutnya pemerintah memastikan tegaknya aturan tersebut melalui lembaga atau badan dibawah Pemerintah,

Aturan saat ini Undang-Undang yang mengatur khusus tentang keamanan data digital, adalah Undang - Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, namun Undang undang tersebut belum memiliki aturan turunan teknis terkait pelaksanaannya, Selain itu Lembaga Pengawas dalam undang-undang tersebut belum Independen dan sanksi yang Dinilai belum memberi efek jera, Selain itu Tantangan Pelaksanaan dan Kepatuhan terhadap Undang-Undang tersebut merupakan tantangan tersendiri yang belum diperhitungkan, kuncinya negara harus berfikir kedepan dalam menantisipasi kemungkinan kemungkinan yang akan terjadi kedepan, dan negara seharusnya memiliki sumber daya yang cukup dalam melaksanakan itu.

Beberapa hal yang telah diuraikan tersebut merupakan pekerjaan rumah yang harus segera dibereskan oleh negara guna menjamin perlindungan data digital sebagaimana yang di amanatkan dalam Pembukaan UUD 1945 untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, negara harus aktif memberikan perlindungan dengan segera membuat aturan turunan contohnya

seperti PP (peraturan Pemerintah) yang mengatur secara teknis perlindungan data pribadi, Kemudian aturan teknis tersebut harus memiliki sifat resposif terhadap perubahan zaman dan adaptif terhadap cepat nya arus digitalisasi, negara harus melangkah tiga kali lebih cepat guna mengantisipasi percepatan arus Perkembangan teknologi informasi dan komunikasi

### **Politik hukum dalam pembentukan Regulasi perlindungan data pribadi & keamanan siber di Indonesia**

Politik hukum pada dasarnya merupakan arah kebijakan hukum (legal policy) yang ditetapkan oleh negara dalam rangka membentuk, menerapkan, dan menegakkan hukum demi tercapainya tujuan nasional, Menurut Mahfud MD, politik hukum merupakan kebijakan dasar yang menentukan arah, bentuk, dan isi hukum yang akan diberlakukan dalam suatu negara, sehingga hukum tidak dapat dilepaskan dari dinamika politik dan sosial masyarakat yang melingkupinya (Moh. Mahfud MD, 2020), selanjutnya terkait konteks era digital, politik hukum Indonesia harus diarahkan untuk menjamin hak konstitusional warga negara atas privasi dan perlindungan data pribadi, sekaligus memperkuat kedaulatan negara di ruang siber, Politik hukum di ruang siber merupakan arah dan kebijakan negara dalam membangun tata kelola hukum digital yang menjamin keamanan, kebebasan, dan keadilan dalam penggunaan teknologi informasi.

Beda halnya jika dilihat dari konteks regulasi keamanan digital dan perlindungan data pribadi di dunia digital arah politik hukum Indonesia tercermin dari upaya pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi serta penguatan mandat kelembagaan seperti Badan Siber dan Sandi Negara (BSSN) sebagai pelaksana keamanan siber nasional, Namun, politik hukum Indonesia dalam isu keamanan data digital masih menghadapi sejumlah tantangan, seperti lemahnya koordinasi antar lembaga, keterbatasan sumber daya manusia di bidang keamanan siber, serta belum adanya regulasi turunan yang komprehensif untuk menegakkan norma norma dalam Undang - Undang Pelindungan Data Pribadi. Selain itu, dari banyaknya kejadian yang terjadi bisa disimpulkan politik hukum Indonesia terkait maslah keamanan digital dan

perlindungan data pribadi masih bersifat reaktif, baru bergerak setelah terjadi insiden kebocoran data besar yang menimbulkan tekanan publik, tentu hal ini bukan sesuatu yang diharapkan oleh masyarakat yang berharap negara hadir untuk melindungi masyarakat khususnya di dunia digital sebagaimana Pembukaan UUD 1945 untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia.

Pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebenarnya adalah sebuah tonggak penting dalam politik hukum Indonesia guna menghadapi disrupsi atau gangguan besar dalam dunia digital global, Regulasi ini merupakan jawaban atas adanya kekosongan hukum sebelumnya dalam hal perlindungan data pribadi di dunia digital, sebelumnya perlindungan data hanya diatur secara sektoral dalam berbagai peraturan seperti UU ITE dan PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Menurut Danrivanto Budhijanto, pembaruan legislasi siber merupakan bagian dari kewajiban negara untuk memastikan keseimbangan antara kemajuan teknologi dan perlindungan hak-hak warga negara (Budhijanto, 2023b), pembaharuan legislasi ini bisa dimaksudkan negara harus membuat aturan turunan guna melaksanakan dan menegakan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dalam aturan turunan tersebut negara dapat membentuk suatu badan atau lembaga yang memiliki tugas khusus memberikan perlindungan data pribadi masyarakat, serta memberikan pemahaman kepada masyarakat terkait data pribadi di dunia digital

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur pembentukan sebuah badan oleh pemerintah yang bertugas untuk melaksanakan penyelenggaraan perlindungan data pribadi di Indonesia, sebagaimana dalam Pasal 58 UU Nomor 27 Tahun 2022 pada pokoknya dalam pasal tersebut menyatakan bahwa guna mewujudkan penyelenggaraan perlindungan data pribadi maka, dibentuk Lembaga yang melaksanakan penyelenggaraan perlindungan data pribadi yang bertanggung jawab kepada presiden, namun hingga tulisan ini di buat pada bulan Oktober 2025 lembaga ini masih dalam tahap pembentukan oleh pemerintah dan oleh karena belum terbentuk maka

sebagaimana termuat dalam Pasal 74 ayat (2) UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang pada pokoknya berbunyi Sebelum Lembaga sebagaimana dimaksud dalam Pasal 58 dibentuk, tugas dan fungsi penyelenggaraan perlindungan data pribadi dilaksanakan oleh unit yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika. Maka perlindungan data pribadi untuk sementara dijalankan oleh Kementerian Komunikasi dan Informatika (Kominfo) melalui Direktorat Jenderal Aplikasi Informatika (Ditjen Aptika).

Politik hukum Indonesia dalam ranah ini tidak boleh hanya bersifat regulatif, tetapi juga transformatif dalam mengarahkan perubahan sosial dan tata kelola digital menuju masyarakat yang aman, beretika, dan berdaulat secara digital dengan mempercepat pembentukan lembaga yang khusus melaksanakan penyelenggaraan perlindungan data pribadi sebagaimana diatur dalam Pasal 58 UU Nomor 27 Tahun 2022, Menurut Prof. Henri Subiakto, pembentukan Lembaga perlindungan data pribadi (PDP) merupakan bukti keseriusan negara dalam menjamin hak privasi warga negara, bukan sekadar respons administratif terhadap kebocoran data.(newsunair, n.d.), harapannya lembaga tersebut harus dirancang sebagai otoritas independen dalam bidang perlindungan data pribadi, yang mirip dengan Data Protection Authority (DPA) di banyak negara lain (misalnya CNIL di Prancis, ICO di Inggris, atau PDPC di Singapura), maksudnya adalah lembaga yang akan dibentuk tersebut tidak sekadar unit di bawah kementerian, tetapi memiliki kewenangan pengawasan dan penegakan hukum administratif atas pelanggaran perlindungan data pribadi.

Menurut teori salah satu tujuan utama dibentuknya negara adalah untuk memberikan keamanan, ketertiban, dan kesejahteraan kepada rakyatnya. Dalam aspek ekonomi politik, kedaulatan data suatu negara dihadapkan pada posisi negara dengan sektor swasta dalam konteks global, Negara pada hakikatnya dibentuk untuk menjamin tercapainya kesejahteraan rakyat. Fungsi negara tidak hanya sebagai penjaga ketertiban, tetapi juga sebagai penyelenggara kesejahteraan melalui kebijakan ekonomi, sosial, dan politik yang berpihak pada kepentingan masyarakat.(Putra, 2021), Peran negara utamanya adalah untuk menghasilkan regulasi perlindungan data siber dan keamanan siber. (Aji, 2023b) Tanpa adanya

jaminan perlindungan, negara kehilangan justifikasi keberadaannya, oleh karena itu negara tidak boleh abstain diruang digital dengan memberikan perlindungan terhadap masyarakat di dunia digital, maka negara dituntut untuk hadir dan berdaulat di dunia digital negara dengan kemampuan yang dimilikinya. Kehadiran negara di ruang digital adalah sebuah bentuk kedaulatan negara, (kedaulatan digital) menjadi aspek penting perlindungan data nasional dalam kerangka nilai-Pancasila, (Rahman et al., 2025)

Hubungan internasional dalam era digital tidak lagi terbatas pada diplomasi konvensional, tetapi juga mencakup kerja sama lintas negara dalam menghadapi ancaman siber yang bersifat transnasional dan tanpa batas wilayah. Negara, melalui pemerintah, memiliki tanggung jawab utama untuk melindungi data pribadi digital warga negaranya dari berbagai bentuk kejahatan siber, seperti peretasan, pencurian data, dan penyalahgunaan informasi pribadi. Bainus dan Rachman menegaskan bahwa hubungan internasional digital menghadirkan paradoks, yakni di satu sisi memberikan kemudahan konektivitas global, namun di sisi lain meningkatkan kerentanan negara terhadap serangan siber yang bersifat asimetris dan sulit dilacak (Bainus & Rachman, 2023). Ancaman ini diperkuat oleh meningkatnya aktivitas state-sponsored cyber attacks dan kejahatan siber terorganisir yang menjadikan data pribadi sebagai komoditas bernilai tinggi (Buchanan, 2020).

Dalam konteks tersebut, negara dituntut untuk aktif membangun kerja sama internasional melalui pertukaran informasi, penyelarasan standar keamanan data, serta penguatan mekanisme respons insiden siber secara kolektif. Kerja sama bilateral dan multilateral menjadi instrumen strategis karena tidak ada satu negara pun yang mampu menghadapi ancaman siber secara unilateral (Kshetri, 2021). Forum internasional seperti ASEAN, G20, dan Perserikatan Bangsa-Bangsa berperan penting dalam membangun norma global terkait keamanan siber dan perlindungan data pribadi, termasuk prinsip due diligence, akuntabilitas negara, dan penghormatan terhadap hak asasi manusia di ruang digital (Moore Jr & Pubantz, 2022). Harmonisasi kebijakan ini diperlukan untuk mencegah fragmentasi regulasi yang justru dapat melemahkan perlindungan data lintas negara.

Lebih lanjut, kerja sama internasional harus diarahkan tidak hanya pada aspek normatif, tetapi juga pada pemenuhan Transfer of Technology (ToT) dari negara maju kepada negara berkembang guna meningkatkan kapasitas nasional dalam melindungi data pribadi digital masyarakat. Kesenjangan teknologi dan sumber daya manusia menjadi faktor utama yang menyebabkan negara berkembang lebih rentan terhadap serangan siber dan ketergantungan pada infrastruktur digital asing (Bannelier & Christakis, 2017). Oleh karena itu, penguatan kerja sama teknis melalui pelatihan keamanan siber, pengembangan computer security incident response team (CSIRT), serta peningkatan kemampuan forensik digital menjadi kebutuhan mendesak (Mishra, 2025). Berbagai bentuk kerja sama keamanan siber yang telah dilakukan menunjukkan bahwa hubungan internasional digital bukan sekadar sarana diplomasi, tetapi juga instrumen strategis negara dalam menjamin perlindungan data pribadi dan kedaulatan digital di tengah eskalasi ancaman global (Kerja Sama Dalam Keamanan Data Di Era Digital Halaman 2 - Kompasiana.Com, n.d.).

## **KESIMPULAN DAN SARAN**

Peran negara dalam pembaruan dan pembentukan regulasi keamanan data digital merupakan wujud pelaksanaan amanat konstitusi untuk melindungi seluruh bangsa Indonesia, terutama di tengah cepatnya transformasi digital yang menuntut negara tampil tidak hanya sebagai regulator, tetapi juga sebagai fasilitator dan pelindung ketahanan siber nasional. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi tonggak penting dalam tata kelola hukum digital, implementasinya masih menghadapi berbagai kendala seperti belum terbentuknya lembaga independen pelindungan data pribadi, lemahnya koordinasi antarinstansi, dan ketiadaan aturan pelaksana yang komprehensif. Politik hukum yang selama ini bersifat reaktif perlu diarahkan menjadi progresif dan transformatif agar mampu melindungi hak digital warga negara serta beradaptasi dengan dinamika teknologi. Keberhasilan Indonesia dalam menjamin keamanan data digital sangat bergantung pada keseriusan negara membangun kerangka hukum yang progresif, termasuk mempercepat pembentukan lembaga PDP independen, menyusun regulasi teknis UU PDP, memperkuat penegakan hukum siber,

meningkatkan literasi publik, serta menjalin kerja sama internasional. Selain itu, hukum harus menjadi instrumen perubahan sosial yang mendorong masyarakat berperan aktif dalam melindungi data pribadinya, karena ketahanan data nasional tidak hanya bergantung pada negara, tetapi juga pada perilaku dan kesadaran digital masyarakat.

## **DAFTAR REFERENSI**

- Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 13(2), 222–238.
- Bainus, A., & Rachman, J. B. (2023). Hubungan Internasional Digital (Digital International Relations). *Intermestic: Journal of International Studies*, 8(1), 1–18.
- Bannelier, K., & Christakis, T. (2017). *Cyberattaques-Prévention-Réactions: Rôles des Etats et des acteurs privés (Cyber-Attacks. Prevention-reactions: The Role of States and Private Actors)*. Les Cahiers de La Revue Défense Nationale, Paris.
- Budhijanto, D. (2023). *Hukum Pelindungan Data Pribadi Di Indonesia Cyberlaw & Cybersecurity*. Bandung: Refika Aditama.
- Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.
- Dinata, R. K. (2025). Pengaruh Teknologi terhadap Perkembangan Hukum di Indonesia. *Arus Jurnal Sosial Dan Humaniora*, 5(1), 630–635.
- Greenleaf, G. (2021). *Global tables of data privacy laws and bills (january 2021)*.
- Gstrein, O. J. (2023). Data autonomy: Recalibrating strategic autonomy and digital sovereignty. *European Foreign Affairs Review*, 28(4).

- Hartzog, W. (2018). *PrivacyOs Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press.
- Hofmann, S. C., & Pawlak, P. (2023). Governing cyberspace: Policy boundary politics across organizations. *Review of international Political Economy*, 30(6), 2122–2149.
- Junaidi, J., Pujiono, P., & Fadzil, R. M. (2024). Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory. *Journal of Law and Legal Reform*, 5(2), 587–612.
- Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach*. University of Toronto Press.
- Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *AL WASATH Jurnal Ilmu Hukum*, 2(1), 9–16.
- Mardiyati, S. (2025). Konstitusionalitas Perlindungan Data Pribadi sebagai Bagian dari Hak atas Rasa Aman. *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda*, 31(3), 209–222.
- Mishra, N. (2025). *Cybersecurity and International Trade*.
- Moore Jr, J. A., & Pubantz, J. (2022). *The new United Nations: International organization in the twenty-first century*. Routledge.
- Nurulita, S. (2025). Political Will of The Indonesian Government in Addressing Data Leakage and Cybersecurity in the Era of Digital Transformation. *JHSS (Journal of Humanities and Social Studies)*, 9(1), 028–038.
- Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.
- Simhadri, S. Y. (2025). 25. The Intersection of Ethics and Artificial Intelligence. *Multidisciplinary Explorations: A Scholarly Compilation*, 170.
- Sinaga, R. A. M. (2024). Konvergensi Teori Hukum dan Teknologi: Membahas Perubahan dalam Era Digital. *JURNAL HUKUM STAATRECHTS*, 7(1), 18–35.

Winata, F. J. (2020). Remedi Novum: Rekonsepsi Mekanisme Penegakan Hak Asasi Manusia Dalam Melindungi Hak Asasi Manusia di Indonesia. *ANTOLOGI ESAI HUKUM DAN HAM Afiliasi Hukum Dan HAM Dalam Mewujudkan Perlindungan Hak Asasi Masyarakat Indonesia*, 1, 47.

Artikel Internet:

Akun Bank hingga WhatsApp Bisa Diserang, BSSN Minta Masyarakat Waspada. (n.d.). Retrieved December 4, 2025, from <https://www.suarasurabaya.net/senggang/2025/akun-bank-hingga-whatsapp-bisa-diserang-bssn-minta-masyarakat-waspada/>

Bersama, I. (2025, March 31). Laporan Tahunan Layanan Honeynet BSSN Tahun 2023 | BSSN -. <https://ilmubersama.com/2025/03/31/laporan-tahunan-layanan-honeynet-bssn-tahun-2023-bssn/>

Politik Hukum di Indonesia / Moh. Mahfud MD | Perpustakaan Mahkamah Konstitusi. (n.d.). Retrieved December 4, 2025, from <https://simpus.mkri.id/opac/detail-opac?id=10372>

Finance Minister orders probe into alleged taxpayer data leak—ANTARA News Mataram. (n.d.). Retrieved December 4, 2025, from [https://mataram.antaranews.com/berita/377555/finance-minister-orders-probe-into-alleged-taxpayer-data-leak?utm\\_source=chatgpt.com](https://mataram.antaranews.com/berita/377555/finance-minister-orders-probe-into-alleged-taxpayer-data-leak?utm_source=chatgpt.com)

Kerja Sama dalam Keamanan Data di Era Digital Halaman 2—Kompasiana.com. (n.d.). Retrieved December 5, 2025, from [https://www.kompasiana.com/ludiro/66915730c925c41a53063005/kesadaran-keamanan-data-di-era-digital?page=2&page\\_images=2](https://www.kompasiana.com/ludiro/66915730c925c41a53063005/kesadaran-keamanan-data-di-era-digital?page=2&page_images=2)

newsunair. (n.d.). Guru Besar FISIP UNAIR Henri Subiakto Paparkan Urgensi RUU Perlindungan Data Pribadi – Unair News. Retrieved December 5, 2025, from <https://news.unair.ac.id/2021/09/07/guru-besar-fisip-unair-henri-subiakto-paparkan-urgensi-ruu-perlindungan-data-pribadi/>

Putra, M. D. (2021). Negara Kesejahteraan (Welfare State) dalam Perspektif Pancasila. *Likhitaprajna*, 23(2), 139–151. <https://www.neliti.com/publications/501075/>

Rahman, Z. D. A., Ramadani, M., Latifah, N. A., Gusti, F. P. A., Universitas Islam Negeri Raden Mas Said Surakarta, I., & Atqiya, A. N. (2025). Pancasila dan Kedaulatan Digital: Implikasi Hukum Internasional Terhadap Perlindungan Data Nasional: Indonesia. *Jurnal Pendidikan Dan Kewarganegara Indonesia*, 2(2), 199–206. <https://doi.org/10.61132/jupenkei.v2i2.367>

Peraturan Perundang-undangan

UU No. 27 Tahun 2022. (n.d.). Database Peraturan | JDIH BPK. Retrieved December 5, 2025, from <http://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>