IMPLEMENTASI KONSEP PRIVACY BY DESIGN DAN PRIVACY BY DEFAULT MELALUI PENDEKATAN ZERO TRUST SEBAGAI AKTUALISASI PERLINDUNGAN HUKUM DATA PRIBADI OLEH PEMERINTAH

Implementation of the Concept of Privacy By Design and Privacy By Default Through the Zero Trust Approach as an Actualization of Legal Protection of Personal Data by the Government

Abdullah Faris Mumtaz[1], Nadirah Dinta Ardiyanti[2], Nabil Afif Fauzy[3]
Fakultas Hukum Universitas Airlangga
farismumtaz0608@gmail.com

Abstrak: Perkembangan teknologi di era digital semakin mempermudah berbagai pekerjaan maupun kegiatan manusia. Sebagaimana teknologi berkembang, kemudahan pengolahan informasi secara digital ikut terus berkembang. Hal ini didasarkan pada berbagai kebutuhan dan aktivitas cyberspace, ruang virtual yang yang menciptakan komunikasi dan/atau integrasi antar media elektronik, seperti social media, e-commerce, hingga e-government. Berbagai layanan pada cyberspace mengharuskan user untuk memberikan informasi, yang tidak jarang diantaranya adalah personally identifiable information atau data pribadi. Berdasarkan permasalahan tersebut, penelitian ini bermaksud untuk mengidentifikasi bagaimana status quo perlindungan hukum terhadap data pribadi oleh pemerintah melalui instrumen hukum dan bagaimana penerapan dari mekanisme konsep privacy by design dan privacy by default berbasis pendekatan zero trust dalam menjawab permasalahan perlindungan hukum data pribadi oleh pemerintah. Adapun metode yang digunakan dalam penelitian ini adalah penelitian hukum atau yuridis normatif dengan menerapkan conceptual approach, statute approach, dan comparative approach.. Kemudian, kesimpulan yang dihasilkan dalam penelitian ini bahwa belum adanya regulasi secara rinci yang mengatur mengenai teknis pelindungan data pribadi oleh pemerintah, sehingga diperlukannya penerapan mekanisme yang jelas serta reformulasi dari rumusan norma pada UU PDP.
Kata Kunci: perlindungan hukum; data pribadi; privacy by design and default; zero trust

Abstract: *The development of technology in the digital era increasingly facilitates various human jobs and activities. As technology develops, the ease of processing information digitally also continues to develop. This is based on various needs and activities of cyberspace, a virtual space that creates communication and/or integration between electronic media, such as social media, e-commerce, to e-government. Various services in cyberspace require users to provide information, which is often personally identifiable information or personal data. Based on these problems, this study intends to identify how the status quo of legal protection of personal data by the government through legal instruments and how the implementation of the privacy by design and privacy by default concept mechanisms based on the zero trust approach in answering the problem of legal protection of personal data by the government. The*

method used in this study is normative legal or juridical research by applying the conceptual approach, statute approach, and comparative approach. Then, the conclusion produced in this study is that there is no detailed regulation that regulates the technical protection of personal data by the government, so that it is necessary to implement a clear mechanism and reformulation of the formulation of norms in the PDP Law.
Keywords: *legal protection; personal data; privacy by design and default; zero trust*

PENDAHULUAN

Perkembangan teknologi di era digital semakin mempermudah berbagai pekerjaan maupun kegiatan manusia. Sebagaimana teknologi berkembang, kemudahan pengolahan informasi secara digital ikut terus berkembang. Hal ini didasarkan pada berbagai kebutuhan dan aktivitas *cyberspace*, ruang virtual yang yang menciptakan komunikasi dan/atau integrasi antar media elektronik, seperti *social media*, *e-commerce*, hingga *e-government*.[1] Berbagai layanan pada *cyberspace* mengharuskan *user* untuk memberikan informasi, yang tidak jarang diantaranya adalah *personally identifiable information* atau data pribadi. Namun, kebutuhan manusia terhadap teknologi menuntut terciptanya kemudahan data pribadi dikumpulkan, disimpan, hingga diproses bahkan dalam jumlah besar dengan waktu yang cenderung singkat.[2] Perkembangan ini juga meningkatkan risiko kebocoran dan penyalahgunaan data yang dapat merugikan individu. Padahal, secara mendasar perlindungan terhadap risiko kebocoran dan penyalahgunaan data merupakan hak asasi yang diamanatkan dalam Pasal 28G ayat 1 Undang-Undang Dasar, bahwa "*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi*". Secara internasional, hak ini juga disebutkan dalam Pasal 12 Deklarasi Universal Hak-Hak Asasi Manusia (DUHAM), bahwa "*Setiap orang, berhak mendapatkan perlindungan hukum terhadap gangguan urusan pribadi, keluarga, rumah tangga atau hubungan surat menyuratnya*".

Perlindungan data pribadi di Indonesia nyatanya masih menjadi momok bagi pengguna layanan *cyberspace*. Sepanjang tahun 2023, Indonesia tercatat menghadapi sejumlah insiden kebocoran data yang signifikan. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), telah tercatat 207 adanya insiden kebocoran data, dengan persentase 55% berasal dari administrasi pemerintahan.[3] Contohnya terjadi pada

[1] William Gibson, *Neuromancer* (New York: The Berkley Publishing Group, 1984).
[2] Suci Wahyu Fajriani, Bintarsih Sekarningrum, dan Munandar Sulaeman, "Cyberspace: Dampak Penyimpangan Perilaku Komunikasi Remaja," *Jurnal IPTEK-KOM* 23, no. 1 (2021): 64.
[3] Lenny Septiani, "BSSN Catat Ada 207 Pencurian Data, Pemerintah Paling Banyak," *Katadata* (blog), 2023, https://katadata.co.id/digital/teknologi/6537ae3a29314/bssn- catat-ada-207-pencurian-data-pemerintah-paling-banyak.

tahun 2023, Bank Syariah Indonesia (BSI) diretas oleh kelompok peretas *Lockbit* melalui serangan *ransomware*, berdampak pada 15 juta data pengguna hingga karyawan. Kasus lain, terjadi pada Juli 2023, yaitu kebocoran data paspor. Tidak hanya itu, kebocoran juga terjadi pada BPJS Ketenagakerjaan, sekitar 19 juta data pribadi pengguna BPJS Ketenagakerjaan, yang dilakukan oleh *hacker* Bjorka. Kementerian Komunikasi dan Informatika (Kominfo) Indonesia pun juga mengalami kasus kebocoran data, sebanyak 252 juta data pemilih tetap (DPT) Pemilu 2024 telah bocor.[4] Hingga pada tahun 2024, kembali terjadi kebocoran pada Pusat Data Nasional Sementara (PDNS) melalui *ransomware* oleh kelompok *hacker* bernama *Brain Chiper*.[5]

Terkait perlindungan data pribadi, pemerintah Indonesia telah mendorong upaya hukum dengan diterbitkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (PDP). Secara umum, prinsip-prinsip dan ketentuan perlindungan data pada UU PDP dipengaruhi kuat oleh pengaturan data pribadi di Uni Eropa, yaitu *General Data Protection Regulation* (GDPR) yang telah dahulu diterbitkan, yaitu pada tahun 2018.[6] Dasar pemikiran yang melahirkan GDPR adalah pandangan terkait kebutuhan pembaruan perkembangan zaman, terkhusus terkait pemenuhan masalah privasi modern. Berakar dari pemikiran tersebut, diaturlah berbagai prinsip, hak, *consent*, *data breach*, *Data Protection Officer* (DPO), hingga konsep *privacy by design* dan *privacy by default* dalam GDPR. Meski demikian, tantangan yang dihadapi dalam tata kelola siber masih cukup kompleks, meliputi infrastruktur teknologi yang tidak memadai, rendahnya kesadaran akan pentingnya privasi, dan kurangnya mekanisme aturan dan penegakan hukum yang lebih efektif. Terlebih, secara data justru menunjukkan kebocoran data besar oleh sektor Pemerintah. Diperlukan upaya dan aturan hukum dengan pendekatan yang lebih komprehensif dan implementatif. Karena berbagai kasus kebocoran data pribadi yang ada, menunjukkan masih diperlukannya mekanisme perlindungan yang lebih efektif yang tidak hanya melindungi data secara eksternal, namun juga internal.

METODE PENELITIAN

Jenis penelitian yang akan digunakan pada penelitian ini adalah yuridis normatif atau penelitian hukum (*legal research*), yakni metode menemukan sumber hukum yang bertujuan untuk memecahkan permasalahan hukum tertentu dengan menganalisis suatu bahan hukum.[7] Kemudian, penelitian ini akan memakai setidaknya

[4] Indira Lintang, "10 Kasus Kebocoran Data di Indonesia yang Paling Menggemparkan," *Inilah.com* (blog), 2024, https://www.inilah.com/kasus-kebocoran-data-di- indonesia.
[5] Indira Lintang.
[6] Graham Greenleaf, "Now 157 Countries: Twelve Data Privacy Laws in 2021/22," *176 Privacy Laws & Business International Report* 1 (2022): 3–8.
[7] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Prenada Media, 2006).

tiga jenis pendekatan, yaitu pendekatan perundang-undangan (*statute approach*) dengan cara membahas berbagai legislasi dan regulasi yang memiliki korelasi dengan hukum siber, lalu pendekatan konseptual (*conceptual approach*) yang berkenaan dengan penggunaan doktrin hukum untuk mengkaji *zero trust* pada *privacy by design and default*, serta pendekatan komparasi (*comparative approach*) atau pendekatan melalui studi perbandingan hukum dengan negara lain yang telah memanfaatkan konsep *privacy by design and default*.

Dalam penelitian ini, sumber data sekunder yang dipakai antara lain berupa bahan hukum primer, sekunder, dan primer. Bahan hukum primer diperoleh dari peraturan perundang-undangan dan catatan resminya serta putusan hakim, sedangkan bahan hukum sekunder ditelusuri lewat publikasi-publikasi hukum yang dapat menjelaskan bahan hukum primer, seperti jurnal, artikel, buku, dan sejenisnya, serta ada pula bahan hukum tersier yang didapatkan dari kamus atau ensiklopedia relevan. Mengenai prosedur pengumpulan data, akan dilakukan penelusuran peraturan perundang-undangan (*reasoning based on rules*) yang memiliki keterkaitan dengan penerapan konsep *privacy by design and default* pada peraturan nasional maupun internasional.[8] Alasan penggunaan prosedur ini adalah demi memperoleh pemahaman mengenai substansi dari bahan hukum secara seksama.

Langkah yang akan peneliti lakukan setelah itu adalah dengan menggunakan teknik hasil analisis data secara deskriptif-kualitatif berdasarkan kajian atas isu atau pendapat yang sedang berkembang.[9] Peneliti akan menelusuri problematika *status quo* terhadap perlindungan hukum data pribadi dan dilanjutkan dengan menawarkan solusi atau rekomendasi berupa penerapan konsep *request by design and default* melalui pendekatan *zero trust*. Adapun metode berpikir yang akan digunakan adalah secara deduktif atau *deductive reasoning*, yaitu penarikan kesimpulan dari yang bersifat umum ke khusus.[10] Dari bahan hukum primer dan sekunder, akan menghasilkan penggabungan dua premis yang dapat menyimpulkan jawaban dari permasalahan hukum yang dibahas dalam penelitian ini. Dalam merumuskan saran maupun rekomendasi, penelitian ini akan bersifat preskripsi, yaitu dengan menguraikan hal-hal yang sepatutnya dilakukan sebab ilmu hukum bersifat sarat nilai.

ANALISIS DAN DISKUSI 1

[8] Philipus Hadjon, *Argumentasi Hukum* (Yogyakarta: Gadjah Mada University Press, 2017).
[9] Soerjono dan Sri, *Penelitian Hukum Normatif Suatu Tinjauan Umum* (Jakarta: Raja Grafindo Persada, 2007).
[10] Sri Soemantri Martosoewignjo, *Persepsi terhadap Prosedur dan Sistem Perubahan Konstitusi dalam Batang Tubuh Undang-Undang Dasar 1945* (Bandung: Alumni, 1987).

1. *Status Quo* Perlindungan Hukum terhadap Data Pribadi oleh Pemerintah Melalui Instrumen Hukum Nasional

a. Dinamika Pengaturan Perlindungan Hukum Data Pribadi di Indonesia

Pada dasarnya, esensi mengenai perlindungan atas data pribadi merupakan salah satu hak konstitusional milik warga negara sebagaimana yang tertuang dalam Pasal 28G ayat (1) UUD NRI Tahun 1945 bahwa "*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi*." Peran negara jelas dalam hal ini, sebab pemerintah memegang tanggung jawab penuh untuk memberikan jaminan perlindungan sebagai wujud dari perlindungan hak asasi manusia warga negaranya.[11] Berangkat dari konstitusi yang memegang hierarki tertinggi peraturan-perundang-undangan, perlu adanya regulasi khusus dan jelas untuk mengatur persoalan perlindungan data pribadi. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) merupakan undang-undang pertama yang mengatur kerangka spesifik mengenai *cyberlaw* di Indonesia dan yang terdiri dari 13 bab dan 54 pasal. Salah satu dari 14 aspek penting dalam UU ini adalah aspek perlindungan *privacy*, bahwa informasi yang menyangkut data pribadi seseorang harus dengan atas persetujuan dari seseorang tersebut.[12]

Adanya aspek ini secara tidak langsung ditujukan untuk memberikan kontrol dan persetujuan kepada seseorang atas data pribadinya agar tidak disalahgunakan. Namun, Undang-Undang ini kemudian mengalami perubahan-perubahan seiring berjalannya waktu, menjadi Undang-Undang Nomor 19 Tahun 2016 yang diubah lagi dengan Undang-Undang Nomor 1 Tahun 2024. Dengan segala dinamika perubahan ini, Undang-Undang ITE nyatanya masih belum mampu mengimbangi ketentuan-ketentuan yang diatur dalam GDPR.[13] Implikasinya, perlindungan data pribadi di Indonesia pun belum cukup maksimal, terutama dalam konteks perlindungan oleh badan publik seperti instansi pemerintahan. Lebih lanjut, sebagai detail dari perwujudan perlindungan data pribadi, Indonesia pun telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Pada dasarnya, banyak substansi dari undang-undang ini yang mengadopsi dari standar yang ada pada GDPR.[14] Namun dalam Undang-Undang ini, tidak ada standar pedoman yang mengatur secara teknis bagaimana institusi pemerintahan sebagai pengendali dalam memproses data-data milik warga negaranya.

b. Urgensi Spesifikasi Pengaturan Perlindungan Data Pribadi oleh Pemerintah

---

[11] Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)* (Jakarta: Sinar Grafika, 2023).

[12] Dannrivanto Budhijanto, *Revolusi Cyberlaw Indonesia: Pembaruan dan Revisi UU ITE 2016* (Bandung: PT Reika Aditama, 2017).

[13] Bambang Pratama, "Perspektif UU-ITE Perlindungan Data Pribadi dan Kebutuhan Pengaturannya," *Binus University* (blog), 2020, https://business- law.binus.ac.id/2020/09/25/perspektif-uu-ite-dalam-perlindungan-data-pribadi-dan-tantangannya/.

[14] Glenn Wijaya, "Pelindungan Data Pribadi di Indonesia: Ius Constitutum dan Ius Constituendum," *Law Review* 19, no. 3 (12 Agustus 2020): 326–61, https://doi.org/10.19166/lr.v19i3.2510.

Salah satu cara penting untuk melaksanakan fungsi penertiban bagi pemerintah adalah dengan dibuatnya produk hukum yang dapat menjamin rasa keadilan bagi rakyatnya. Hal ini pun berkorelasi terhadap persoalan data pribadi yang kian banyak terancam oleh serangan-serangan luar di ruang digital. Hadirnya rentetan-rentetan kasus yang telah diuraikan sebelumnya secara tidak langsung menggambarkan ketidaksiapan pemerintah sebagai pengendali data badan publik dalam praktik perlindungan data pribadi. Negara (dalam hal ini pemerintah) perlu memfasilitasi Teknologi Informasi dengan tujuan pemberian perlindungan atas gangguan pada *cyberspace*, yang mana sesuai dengan tiga tanggung jawab negara, yaitu *the obligation to respect*, *protect*, *and fulfill*.[15]

ANALISIS DAN DISKUSI 2

1. Penerapan dari Mekanisme Konsep *Privacy by Design* dan *Privacy by Default* berbasis Pendekatan *Zero Trust* dalam Menjawab Permasalahan Perlindungan Hukum Data Pribadi oleh Pemerintah

a. Komparasi General Data Protection Regulation (GDPR) di Uni Eropa

Sebelum diatur dalam GDPR, hak atas privasi telah termaktub dalam *European Convention on Human Rights article 8 section 1* tahun 1950, yang menyatakan bahwa setiap orang berhak atas penghormatan kehidupan pribadi, keluarga, rumah, dan korespondensinya. Yang dalam perkembangannya kemudian mengadopsi norma-norma yang diatur dalam *Organization for Economic Cooperation and Development* (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* yang dirilis pada tahun 1980 yang dimaksudkan untuk pedoman anggota-anggota OECD dalam memberikan suatu kebijakan.[16] Delapan prinsip dasar yang telah dirilis oleh OECD dinilai dapat memberikan hak privasi yang diperlukan, khususnya pada prinsip batasan pengumpulan data, penggunaan terbatas, serta hak akses dan koreksi bagi individu, sehingga kemudian diadopsi pada *European Union* (EU) *Data Protection Directive* pada tahun 1995. Uni Eropa telah lama memiliki perhatian yang serius terhadap isu dan hak atas privasi serta perlindungan data pribadi. Sebelum adanya *European Union* (EU) *Data Protection Directive* di tahun 1995, Uni Eropa juga telah membentuk *Council of Europe* (CoE), konvensi yang dibentuk oleh Dewan Eropa untuk memperkuat perlindungan data di Eropa pada tahun 1981. Yang kemudian lahir *CoE Convention 108* sebagai dasar aturan pengolahan data pribadi dalam sektor privat maupun publik. Perkembangan perlindungan hukum data pribadi di Uni Eropa menunjukkan ketegasan hak privasi sebagai bagian dari hak dasar yang harus

[15] Endah Dewi Nawangsasi, *Hukum Administrasi Negara dalam Perspektif Cyber Law terkait Data Privasi dan Beschikking Digitalisasi* (Bandung: PT Alumni, 2021).
[16] Sinta Dewi Rosadi, *Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional (Revisi)* (PT Refika Aditama, 2022).

dilindungi di Uni Eropa.[17] Tak ayal, dalam perkembangannya prinsip pada aturan-aturan perlindungan data di Uni Eropa banyak menjadi standar/pedoman yang diadopsi oleh negara-negara lain.

General Data Protection Regulation (GDPR) diberlakukan (secara efektif) pada seluruh Uni Eropa sejak tahun 2018. Dalam article 25, GDPR telah mewajibkan *privacy by design* dan *privacy by default*, bahwa setiap pengolah data, termasuk otoritas publik, harus menerapkan perlindungan privasi sejak awal proses pengembangan sebuah sistem layanan pada *cyberspace* dan menerapkan pengaturan bawaan terkait privasi sebaik mungkin dalam sistem secara otomatis-tanpa diperlukan lebih dulu tindakan tambahan dari *user* (seperti menyetujui atau tidak terhadap perlindungan tinggi). Lebih khusus untuk otoritas publik, telah diatur hal yang perlu diperhatikan untuk diterapkannya *privacy by design* dan *privacy by default*.[18] Pertama, *Lawfulness*, *Fairness, and Transparency*, yang diatur dalam *article 5*, bahwa harus diberikannya informasi yang jelas tentang bagaimana, oleh siapa, dan di mana data mereka akan disimpan sehingga adil dan transparan. Kedua, *data minimization* and *purpose limitation*, sebagaimana diatur dalam *article 5 number 1 (c)* dan *6 number 1 (e)*, otoritas publik dapat memproses data harus terbatas dan hanya ketika sesuai tugasnya atau kepentingan umum-dengan tujuan spesifik, eksplisit, dan sah.[19] Ketiga, *confidentiality and security*, bahwa data harus diolah dengan tepat. Seperti adanya untuk identifikasi risiko privasi *(article 35)*, *pseudonimitas* dan enkripsi yaitu teknik keamanan yang menggantikan pengenal pribadi dalam data dengan nilai pengganti atau alias *(art 6 number 3 (e)), accuracy* yaitu data haruslah akurat dan diperbarui dengan memastikan bahwa data yang tidak akurat harus dihapus atau diperbaiki tanpa penundaan untuk menghindari data ganda *(article 5 number 1 (d))*, serta memiliki *Independent Supervisory Authorities* untuk memantau penerapan perlindungan privasi oleh entitas publik.[20]

Sedangkan di Indonesia, perlindungan data pribadi secara umum diatur dalam UU PDP. Apabila dikomparasikan maka dapat ditemukan berbagai pengaturan hukum

[17] Sinta Dewi Rosadi dan Garry Gumelar Pratama, "Urgensi Pelindungan Data Privasi dalam Era Ekonomi Digital di Indonesia," *Veritas et Justitia* 4, no. 1 (28 Juni 2018): 88–110, https://doi.org/10.25123/vej.2916.

[18] Pagona Tsormpatzoudi, Bettina Berendt, dan Fanny Coudert, *Privacy By Design: from Research and Policy to Practice - The Challenge of Multi-disciplinarity* (Lecture Notes in Computer Science (LNCS), 2016).

[19] Muhammad Akbar Eka Pradana, Horadin Saragih, dan Universitas Esa Unggul, "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya," *INNOVATIVE: Journal Of Social Science Research* 4, no. 4 (2024): 3412–25.

[20] Lukas Irwin, "Summary of The GDPR's 10 Key Requirements," *Itgovernance.eu* (blog), 2024, https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key- requirements.

pada GDPR terkait perlindungan data pribadi yang ada dan tidak ada dalam UU PDP.[21] Secara terbatas dan spesifik, berdasar hukum, transparan, *purpose limitation* → telah diatur pada Pasal 28, jaminan dan dapat dipertanggungjawabkan, akurat, lengkap, tidak sesat, mutakhir serta ketentuan penghapusan data → pada Pasal 29-30 dan 44, lembaga pengawas terkait → Pasal Pasal 51-59. Sedangkan pada Pasal 21 mengatur terkait kewajiban pengendali data untuk melakukan perlindungan data pribadi dalam setiap proses pengolahan dan Pasal 28 yang mengatur mengatur tentang kewajiban pemrosesan data pribadi sesuai dengan tujuan pemrosesan, tidak mengatur secara terang *privacy by design* dan *privacy by default*, melainkan secara implisit dengan adanya pengaturan prosedur dan pertanggungjawaban, berbeda halnya dengan GDPR yang menerangkan secara jelas sebuah keharusan pertimbangan dan indikator-indikator desain perlindungan privasi sejak proses awal.

b. Komparasi Zero Trust Architecture (ZTA) oleh Amerika Serikat dengan Sistem Siber Indonesia

Digitalisasi mendorong *zero trust* menjadi unsur penting untuk diterapkan. Pendekatan *zero trust* hadir sebagai respon terhadap model keamanan tradisional dengan prinsip *trust but verify*. Penerapan *zero trust* mengharuskan seluruh pengguna untuk membuktikan identitas dan memberikan kepercayaan yang kuat, serta menegakkan otorisasi yang berbasis identitas yang terperinci dengan verifikasi terus menerus untuk dapat masuk dalam suatu akses. Pada dasarnya penerapan keamanan *zero trust* terhadap kontrol akses berbasis identitas yang ketat serta tidak mempercayai siapapun secara default untuk memastikan jika jaringan tersebut tidak dapat dijangkau. Sehingga penerapan ini sangat penting untuk mencegah kejahatan yang berasal dari eksternal maupun internal. *Zero trust* menawarkan pendekatan yang lebih modern dan efektif untuk keamanan jaringan dengan pendekatan prinsip *Never Trust, Always Verify*.[22] Dengan fokus pada autentikasi yang ketat, segmentasi jaringan, dan *monitoring* yang berkelanjutan, serta dapat membantu melindungi organisasi dari berbagai ancaman siber, Ancaman siber menjadi keresahan seluruh negara, masing masing negara mempertahankan agar terhindar dari seluruh ancaman. Ancaman siber dapat berasal dari berbagai sumber seperti *hacker*, kelompok teroris, serta dapat berasal dari internal yang mempunyai akses tersebut sehingga menyebarkan dan menjual data tersebut.

[21] Beni Kharisma Arrasuli dan Khairul Fahmi, "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi," *UNES Journal of Swara Justisia* 7, no. 2 (1 Juli 2023): 369–92, https://doi.org/10.31933/ujsj.v7i2.351.

[22] William Yeoh dkk., "Zero Trust Cybersecurity: Critical Success Factors and A Maturity Assessment Framework," *Computers & Security* 133 (Oktober 2023): 1–13, https://doi.org/10.1016/j.cose.2023.103412.

Keamanan Siber Indonesia menurut *National Cyber Security Index* (NSCI) tingkat keamanan siber di Indonesia tergolong rendah. Indonesia menempati peringkat ke-49 dari 176 negara dengan perolehan skor hanya 63,64. Berdasarkan data tersebut, serangan siber di indonesia yang terjadi dengan kenaikan yang mencolok sehingga merugikan seluruh warga Indonesia. Dengan contoh yang terjadi pada tahun ini pada pusat data nasional sementara yang menyebabkan 239 atau 84,75 persen instansi pengguna yang terdampak pada layanan seperti kementrian sebanyak 10,6 persen, provinsi 5,32 persen, kabupaten 52,48 persen, kota 16,31 persen.[23] Dapat disimpulkan bahwa sistem keamanan siber sangat membutuhkan perhatian khusus. Negara Amerika Serikat salah satu penganut serta mengadopsi penerapan berlandaskan prinsip *zero trust*, yaitu *Zero Trust Architecture* atas perintah eksekutif langsung oleh Presiden Joe Biden sebagai bentuk penanganan ancaman siber di Amerika. Hadirnya penerapan tersebut didalangi oleh *National Institute of Standards and Technology* (NIST) menawarkan pendekatan *Zero Trust Architecture* yang lebih aman dengan menggabungkan manajemen risiko dan memperketat kendali pada perangkat dan identitas pengguna. Implementasi ini sesuai dengan kerangka kerja keamanan federal di Amerika. Hal ini sudah ditetapkan oleh pemerintah amerika serikat sebagai syarat dan strategi yang mewajibkan organisasi pemerintah Amerika Serikat guna memperkuat keamanan.

Apabila kita membandingkan sistem yang terdapat pada Indonesia, dapat diklasifikasi dalam beberapa aspek.

Tabel 1. Komparasi Amerika dengan Indonesia

Regulasi dan Kebijakan	
Amerika Serikat	**Indonesia**
Adanya *Cybersecurity Executive Orde*r yang mendorong adopsi *Zero Trust Architecture* di lembaga pemerintah dan NIST 800-207 sebagai panduan resmi untuk mengimplementasikan.	Hingga saat ini belum terdapat Undang Undang yang mengatur. Namun terdapat kebijakan dari Badan Siber dan Sandi Negara terkait keamanan informasi.

[23] Syahlan Hidayat Alfarizi, "Perbandingan Regulasi Keamanan dan Ketahanan Siber di Indonesia dengan Regulasi Keselamatan Siber di Malaysia" (Jakarta, Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta, 2025).

Penerapan Teknologi	
Amerika Serikat	**Indonesia**
Lembaga federal atau Departemen Pertahanan yang menerapkan *Zero Trust Architecture*.	Penerapan yang dilakukan pemerintah mulai mengimplementasikan *Zero Trust Architecture*.

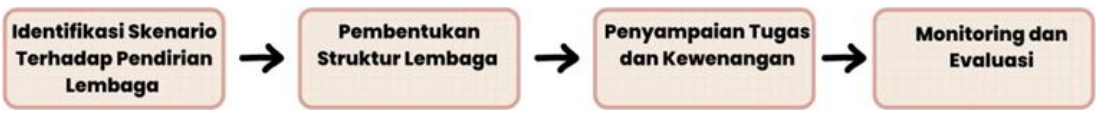
Tantangan Implementasi	
Amerika Serikat	**Indonesia**
Biaya operasional yang besar.	Minimnya kesadaran dan pemahaman tentang dalam kalangan organisasi *Zero Trust Architecture*.

Setelah melakukan komparasi penerapan pada negara Amerika Serikat, kedua negara tersebut memiliki pendekatan yang berbeda, dengan Amerika jauh lebih unggul dari seluruh aspek dibandingkan dengan Indonesia. Peraturan yang jelas, serta dukungan pemerintah guna mengatasi ancaman siber. Sehingga Indonesia dapat perlu meningkatkan kesadaran akan pentingnya keamanan siber dan membangun peraturan yang mendukung penerapan *Zero Trust Architecture* secara efektif. Dengan segala tantangan terkait perlindungan ancaman siber, pemerintah memiliki tantangan terkait Penerapan *Zero Trust Architecture* dapat menjadi solusi dalam menghadapi perkembangan yang signifikan untuk menangani semakin tingginya frekuensi dan kompleksitas ancaman. Langkah penerapan ini cocok diterapkan karena pemerintah belum terdapat solusi dalam menangani permasalahan dengan melakukan penerapan untuk meningkatkan keamanan. Sehingga dapat memberikan dampak yang signifikan terhadap keamanan siber di Indonesia.

c. *Mekanisme Pendekatan Zero Trust Sebagai Implementasi Privacy by Design dan Privacy by Default*

Berdasarkan aturan yang berlaku di Indonesia yang sudah mengesahkan Undang-Undang Pelindungan Data Pribadi, Indonesia juga memerlukan Pembentukan Otoritas Pengawas Independen. Dalam Pembentukan Otoritas Independen di Indonesia terdapat beberapa tahapan, yakni:

Gambar 1. Bagan Mekanisme Pembentukan Otoritas Independen di Indonesia



- Identifikasi Skenario Terhadap Pendirian Lembaga
  Dalam tahapan ini membahas mengenai ruang lingkup kelembagaan yang berwenang yaitu sebagai Lembaga Independen Non Kementerian yang sekaligus menegakkan Undang-Undang. Hal ini penting karena turut mengawasi pengelola data. Berdasarkan pada Undang Undang Nomor 27 tahun 2022 Pasal 58 Lembaga Independen langsung bertanggung jawab dengan Presiden.
- Pembentukan Struktur Lembaga
  Tahap ini ditujukan sebagai pemilihan pemilihan komisioner yang dipilih DPR dan ditetapkan oleh Presiden, Dalam pemilihan Ketua Otoritas Data Pribadi dipilih langsung oleh komisioner tanpa campur tangan pihak luar.
- Penyampaian Tugas dan Kewenangan
  Tahapan berisi penyampaian dan berkoordinasi dengan instansi pemerintah serta seluruh sektor swasta guna menyusun dan merencanakan segala kebijakan, pemberlakuan serta sebagai pelatihan dan edukasi kepada seluruh *stakeholder* yang terlibat.
- Monitoring dan Evaluasi
  Tahapan ini dilaksanakan guna memastikan bahwa tidak terjadinya pelanggaran apapun terhadap seluruh tahapan. Sehingga sesuai standar minimum sebuah mekanisme dalam pembentukan Otoritas Independen.

Kemudian apabila melihat pada pengaturan tata kelola siber oleh Pemerintah dalam UU PDP hanya diatur secara umum saja sebagai Pengendali Data Pribadi. Mengingat data kebocoran banyak terjadi pada otoritas publik, tentu pengaturan lebih lanjut terkait tata kelola sistem siber oleh pemerintah dinilai penting. Oleh sebab itu, diperlukan penambahan materi muatan dalam UU PDP dengan memasukkan mekanisme *Zero Trust* sebagai implementasi *Privacy by Design* dan *Privacy by Default*, lebih lanjut pasal yang akan ditambahkan pada pokoknya sebagai berikut:

- *Privacy by design* dan *privacy by default* untuk dapat mendorong kewajiban Pemerintah selaku Pengendali Data Pribadi untuk menjamin kepastian dasar rancangan yang telah menerapkan perlindungan data privasi dapat diatur kewajiban memiliki dasar rancangan teknis perlindungan data dalam Pasal 20 sebagai ayat (1) dan menjadi ayat (1) pada awalnya, menjadi kewajiban setelahnya (ayat (2)).
- Bentuk teknis *privacy by design* dan *privacy by default* dengan aturan *Data Protection Impact Assessments* (DPIA) atau identifikasi risiko privasi → bab

yang mengatur indikator minimal yang diperlukan dalam membuat dasar rancangan teknis perlindungan data dalam sebuah layanan siber oleh pemerintah.

- *Zero Trust* dengan pengaturan *data minimization* disamping *purpose limitation*, penambahan norma "terbatas" untuk minimalisasi dan memberi segmentasi jaringan disamping sesuai dengan tujuan, sehingga tidak dapatnya memperluas pengumpulan maupun akses data.

PENUTUP

Dari uraian penjelasan yang telah dipaparkan dalam penelitian ini, benang merah yang dapat peneliti tarik untuk menghasilkan kesimpulan komprehensif adalah berdasarkan *status quo*, pengaturan-pengaturan mengenai perlindungan data pribadi khususnya oleh pemerintah sebagai pengendali data masih belum diatur secara rinci. Hal ini dapat dilihat dari regulasi terkait yang tidak mengatur teknis yang jelas, sehingga menjadi salah satu penyebab banyaknya rentetan problematika mengenai *cybercrime* yang merugikan subjek data pribadi. Oleh karena itu, terdapat urgensi untuk pemerintah agar memfasilitasi teknologi informasi secara terperinci untuk melindungi data pribadi warga negaranya. Demi mengimplementasikan konsep *privacy by design* dan *privacy by default* melalui pendekatan *zero trust*, langkah-langkah yang dapat dilakukan sebagai penerapan mekanismenya, yakni; Identifikasi Skenario Terhadap Pendirian Lembaga, Pembentukan Struktur Lembaga, Penyampaian Tugas dan Kewenangan, Monitoring dan Evaluasi.

Kemudian, mekanisme-mekanisme tersebut akan dituangkan dalam bentuk reformulasi rumusan norma pada UU PDP. Pemerintah dalam hal mewujudkan perlindungan hukum terhadap data pribadi warga negara perlu mengatur pedoman secara teknis bagi pemerintah itu sendiri di samping badan-badan privat lain. Dalam memproses data pribadi, perlu adanya akomodasi terhadap konsep *privacy by design* dan *privacy by default* dengan berprinsip pada pendekatan *zero trust*. Selain itu, perlu diatur mengenai independensi lembaga dan kolaborasi antara *stakeholders* demi menyukseskan pengembangan mekanisme. Keterlibatan lembaga-lembaga sebagai salah bentuk dari perwujudan *good governance* dalam persoalan perlindungan hukum data pribadi.

DAFTAR PUSTAKA

Arrasuli, Beni Kharisma, dan Khairul Fahmi. "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi." *UNES Journal of Swara Justisia* 7, no. 2 (1 Juli 2023): 369–92. https://doi.org/10.31933/ujsj.v7i2.351.

Bambang Pratama. "Perspektif UU-ITE Perlindungan Data Pribadi dan Kebutuhan Pengaturannya." *Binus University* (blog), 2020. https://business-

law.binus.ac.id/2020/09/25/perspektif-uu-ite-dalam-perlindungan-data-pribadi-dan-tantangannya/.

Dannrivanto Budhijanto. *Revolusi Cyberlaw Indonesia: Pembaruan dan Revisi UU ITE 2016*. Bandung: PT Reika Aditama, 2017.

Dewi Rosadi, Sinta, dan Garry Gumelar Pratama. "Urgensi Pelindungan Data Privasi dalam Era Ekonomi Digital di Indonesia." *Veritas et Justitia* 4, no. 1 (28 Juni 2018): 88–110. https://doi.org/10.25123/vej.2916.

Endah Dewi Nawangsasi. *Hukum Administrasi Negara dalam Perspektif Cyber Law terkait Data Privasi dan Beschikking Digitalisasi*. Bandung: PT Alumni, 2021.

Fajriani, Suci Wahyu, Bintarsih Sekarningrum, dan Munandar Sulaeman. "Cyberspace: Dampak Penyimpangan Perilaku Komunikasi Remaja." *Jurnal IPTEK-KOM* 23, no. 1 (2021): 64.

Greenleaf, Graham. "Now 157 Countries: Twelve Data Privacy Laws in 2021/22." *176 Privacy Laws & Business International Report* 1 (2022): 3–8.

Indira Lintang. "10 Kasus Kebocoran Data di Indonesia yang Paling Menggemparkan." *Inilah.com* (blog), 2024. https://www.inilah.com/kasus-kebocoran-data-di-indonesia.

Lenny Septiani. "BSSN Catat Ada 207 Pencurian Data, Pemerintah Paling Banyak." *Katadata* (blog), 2023. https://katadata.co.id/digital/teknologi/6537ae3a29314/bssn- catat-ada-207-pencurian-data-pemerintah-paling-banyak.

Lukas Irwin. "Summary of The GDPR's 10 Key Requirements." *Itgovernance.eu* (blog), 2024. https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key-requirements.

Pagona Tsormpatzoudi, Bettina Berendt, dan Fanny Coudert. *Privacy By Design: from Research and Policy to Practice - The Challenge of Multi-disciplinarity*. Lecture Notes in Computer Science (LNCS), 2016.

Peter Mahmud Marzuki. *Penelitian Hukum*. Jakarta: Prenada Media, 2006.

Philipus Hadjon. *Argumentasi Hukum*. Yogyakarta: Gadjah Mada University Press, 2017.

Pradana, Muhammad Akbar Eka, Horadin Saragih, dan Universitas Esa Unggul. "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya." *INNOVATIVE: Journal Of Social Science Research* 4, no. 4 (2024): 3412–25.

Sinta Dewi Rosadi. *Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional (Revisi)*. PT Refika Aditama, 2022.

———. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta: Sinar Grafika, 2023.

Soerjono dan Sri. *Penelitian Hukum Normatif Suatu Tinjauan Umum*. Jakarta: Raja Grafindo Persada, 2007.

Sri Soemantri Martosoewignjo. *Persepsi terhadap Prosedur dan Sistem Perubahan Konstitusi dalam Batang Tubuh Undang-Undang Dasar 1945*. Bandung: Alumni, 1987.

Syahlan Hidayat Alfarizi. "Perbandingan Regulasi Keamanan dan Ketahanan Siber di Indonesia dengan Regulasi Keselamatan Siber di Malaysia." Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta, 2025.

Wijaya, Glenn. "Pelindungan Data Pribadi di Indonesia: Ius Constitutum dan Ius Constituendum." *Law Review* 19, no. 3 (12 Agustus 2020): 326–61. https://doi.org/10.19166/lr.v19i3.2510.

William Gibson. *Neuromancer*. New York: The Berkley Publishing Group, 1984.

Yeoh, William, Marina Liu, Malcolm Shore, dan Frank Jiang. "Zero Trust Cybersecurity: Critical Success Factors and A Maturity Assessment Framework." *Computers & Security* 133 (Oktober 2023): 1–13. https://doi.org/10.1016/j.cose.2023.103412.