https://www.jurnal-umbuton.ac.id/index.php/Pencerah
https://doi.org/10.35326/pencerah.v11i2.7268

Open Access

SANG PENCERAH
Jurnal Ilmiah Universitas Muhammadiyah Buton

E-ISSN: 2621-6159, P-ISSN: 2460-5697 Volume 11, No 2, Tahun 2025

Tanggung Jawab Kemenkominfo Terhadap Keamanan Pusat Data Nasional (Studi Putusan Nomor: 269/G/TF/2024/PTUN.JKT)

Dicky Ariansyah[1]*, Akhmad Safik[1]

[1]Fakultas Hukum, Universitas Al Azhar Indonesia
*Korespondensi: dickymobile94@gmail.com

Info Artikel

Diterima 25 Februari 2025

Disetujui 30 Mei 2025

Dipublikasikan 31 Mei 2025

Keywords:
PDN; Peretasan Data; Perlindungan Data Pribadi

Abstrak

Perkembangan digitalisasi menempatkan keamanan data sebagai prioritas utama untuk melindungi informasi sensitif dari ancaman peretasan. Penelitian ini bertujuan untuk menganalisis tanggung jawab negara dalam menjamin keamanan data, khususnya melalui studi kasus Putusan PTUN Nomor 269/G/TF/2024/PTUN.JKT terkait insiden peretasan Pusat Data Nasional (PDN). Penelitian menggunakan metode yuridis-normatif dengan pendekatan studi kasus, mengkaji regulasi seperti UU PDP, PP 71/2019, dan Perpres tentang SPBE. Hasil penelitian menunjukkan bahwa meskipun PDN dirancang untuk mendukung tata kelola data terpadu, tantangan seperti fragmentasi data, kurangnya tenaga ahli, serta ancaman siber masih signifikan. Insiden peretasan PDN pada Juni 2024 mengakibatkan kerugian ekonomi hingga Rp6,3 triliun, gangguan layanan publik di berbagai sektor, dan penurunan kepercayaan masyarakat terhadap pemerintah. Analisis terhadap putusan PTUN mengungkap pendekatan formalistik hakim dalam menolak legal standing Komunitas Konsumen Indonesia (KKI), yang dinilai mengabaikan keadilan substantif dan prinsip Public Interest Litigation. Kesimpulannya, perlindungan data memerlukan penguatan regulasi, peningkatan infrastruktur keamanan, serta fleksibilitas hukum untuk mendukung akses keadilan. Penelitian ini menekankan pentingnya peran negara dalam melindungi hak privasi dan keamanan data guna membangun kepercayaan publik serta mendukung transformasi digital yang berkelanjutan.

Abstract

The development of digitalization places data security as a top priority to protect sensitive information from the threat of hacking. This research aims to analyze the state's responsibility in ensuring data security, specifically through a case study of State Administrative Court Decision Number 269/G/TF/2024/PTUN.JKT related to the National Data Center hacking incident. The research uses a juridical-normative method with a case study approach, examining regulations such as Law Number 27 of 2022 on Personal Data Protection, Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions, and Presidential Regulation Number 95 of 2018 on Electronic-Based Government Systems. The results show that although the National Data Center is designed to support integrated data governance, challenges such as data fragmentation, lack of experts, and cyber threats are still significant. The hacking incident of the National Data Center in June 2024 resulted in economic losses of up to IDR6.3 trillion, disruption of public services in various sectors, and decreased public trust in the government.

An analysis of the decision of the State Administrative Court reveals the formalistic approach of the judge in rejecting the legal standing of the Indonesian Consumer Community, which is considered to ignore substantive justice and the principle of Public Interest Litigation. In conclusion, data protection requires strengthening regulations, improving security infrastructure, and legal flexibility to support access to justice. This research emphasizes the importance of the state's role in protecting privacy rights and data security to build public trust and support sustainable digital transformation.

1. Pendahuluan

Perkembangan digitalisasi yang semakin pesat, mendorong keamanan data menjadi aspek yang sangat penting untuk melindungi informasi sensitif dari akses yang tidak sah. Keamanan data tidak hanya melibatkan penggunaan teknologi canggih, tetapi juga memerlukan pemahaman yang mendalam tentang berbagai metode perlindungan data, termasuk kriptografi. Sebagai contoh, algoritma *Blowfish* dan *Rail Fence* telah dianalisis untuk meningkatkan keamanan data, terutama dalam konteks pengamanan data pemasok dan informasi sensitif lainnya (Y. Pratama & Sutabri, 2023). Penggunaan teknik kriptografi ini menunjukkan bahwa pendekatan teknis dapat secara signifikan meningkatkan integritas dan keaslian data yang disimpan dan ditransmisikan. Di samping itu, kolaborasi antara jaringan komputer dan basis data juga menjadi vital dalam era digital. Dengan kemajuan teknologi seperti *Internet of Things (IoT)* dan *Big Data*, tantangan terkait keamanan data, privasi, dan keberlanjutan infrastruktur jaringan harus diperhatikan secara serius (Aulia dkk., 2023). Dalam konteks ini, penting bagi organisasi untuk menerapkan sistem manajemen keamanan informasi yang efektif, seperti yang diungkapkan dalam penelitian mengenai Indeks KAMI, yang digunakan untuk mengevaluasi pengelolaan keamanan sistem informasi di berbagai institusi (S dkk., 2023). Hal ini menunjukkan bahwa pengelolaan keamanan informasi yang baik dapat membantu organisasi dalam menghadapi ancaman yang muncul akibat digitalisasi.

Pendidikan dan literasi digital juga memainkan peran penting dalam meningkatkan kesadaran akan keamanan data. Program-program pelatihan yang ditujukan untuk masyarakat, seperti pelatihan dasar keamanan data pribadi, telah terbukti efektif dalam meningkatkan pemahaman masyarakat tentang pentingnya menjaga data pribadi mereka (Baso dkk., 2023). Selain itu, kesadaran akan keamanan siber di kalangan pengguna internet, terutama generasi muda, perlu ditingkatkan untuk mencegah serangan siber yang semakin kompleks (Umam, 2019). Dengan demikian, pendekatan edukatif menjadi salah satu strategi kunci dalam memperkuat keamanan data di era digital. Selanjutnya, tantangan yang dihadapi dalam menjaga keamanan data juga mencakup kebutuhan untuk mematuhi regulasi yang semakin ketat, seperti yang terlihat dalam pengembangan standar ISO 27001:2022 untuk sistem keamanan informasi (R. Sinaga, 2024). Standar ini membantu organisasi dalam mengelola data sensitif dengan lebih baik dan memastikan bahwa mereka memenuhi persyaratan hukum yang berlaku. Selain itu, teknologi baru seperti *blockchain* juga menawarkan solusi inovatif untuk meningkatkan keamanan data melalui enkripsi yang lebih kuat dan transparansi dalam pengelolaan data (Munawar dkk., 2023).

Keamanan data dalam konteks digitalisasi memerlukan pendekatan yang komprehensif, melibatkan teknologi, pendidikan, dan kepatuhan terhadap regulasi. Dengan mengintegrasikan berbagai strategi ini, organisasi dapat lebih baik dalam melindungi data mereka dan membangun kepercayaan dengan pengguna. Sama halnya dengan keamanan data, perlindungan data telah menjadi perhatian penting di era digital, di mana sejumlah besar informasi pribadi dan sensitif dihasilkan, disimpan, dan dikirimkan di berbagai platform. Meningkatnya ketergantungan pada teknologi digital mengharuskan penerapan langkah-langkah perlindungan data yang kuat untuk melindungi privasi individu dan memastikan integritas data. Dengan meningkatnya pelanggaran data dan serangan siber, individu semakin khawatir tentang privasi mereka. Langkah-langkah perlindungan data membantu mengurangi kekhawatiran ini dengan memastikan bahwa informasi pribadi ditangani secara bertanggung jawab dan aman (Genaro & Rifiyanti, 2023).

Keamanan data dan perlindungan data merupakan bagian penting yang tidak terpisahkan dalam mewujudkan ekosistem pengelolaan data yang baik serta pemenuhan hak terkait perlindungan data pribadi. Perlindungan data pribadi tidak hanya berkaitan dengan hak individu atas privasi, tetapi juga mencakup aspek hukum dan regulasi yang diperlukan untuk melindungi data dari penyalahgunaan. Perlindungan data pribadi telah menjadi isu penting di era digital, terutama dengan munculnya teknologi *Big Data* dan pengaturan hukum seperti *General Data Protection Regulation (GDPR)* di Eropa. *GDPR*, yang mulai berlaku pada Mei 2018, bertujuan untuk meningkatkan kontrol individu atas data pribadi mereka dan menyelaraskan undang-undang privasi data di seluruh Eropa (Torre dkk., 2020). Peraturan ini mengamanatkan bahwa organisasi harus menerapkan langkah-langkah yang kuat untuk melindungi data pribadi, dengan demikian memastikan kepatuhan dan menjaga hak privasi individu (Zaman & Hassani, 2020).

Masifnya penggunaan teknologi *Big Data* menjadi tantangan yang signifikan di era digital, teknologi ini sering kali memproses data dalam jumlah besar, yang dapat mencakup informasi yang dapat diidentifikasi secara pribadi atau diistilahkan *personally identifiable information (PII).* Sifat yang melekat pada *Big Data* membuatnya sulit untuk menjamin perlindungan informasi pribadi, terutama ketika data tersebut digunakan untuk analisis dan proses pengambilan keputusan . Para ahli telah mencatat bahwa mekanisme perlindungan data offline bisa lebih mudah, lingkungan perlindungan data yang bersifat online justru menimbulkan tantangan yang lebih kompleks karena sifat penggunaan data yang dinamis dan saling terhubung (Bogdan & Kirillova, 2020). Di Eropa, kompleksitas ini diperketat dengan persyaratan *GDPR*, yang mengharuskan organisasi tidak hanya melindungi data tetapi juga memastikan transparansi dan akuntabilitas dalam aktivitas pemrosesan data mereka (Torre dkk., 2020).

Uni Eropa melalui *General Data Protection Regulation (GDPR)* telah menetapkan standar tinggi untuk perlindungan data pribadi. *GDPR* mengatur berbagai aspek, termasuk persetujuan eksplisit dari individu sebelum data mereka diproses, serta hak untuk mengakses dan menghapus data pribadi (Ziqra dkk., 2021). Indonesia perlu mempertimbangkan pendekatan serupa untuk memperkuat perlindungan data pribadi di dalam negeri, terutama dalam menghadapi tantangan yang muncul akibat revolusi industri 4.0 dan penggunaan teknologi baru seperti kecerdasan buatan (E. M. C. Sinaga & Putri, 2020). Selain itu, pentingnya penerapan prinsip *"privacy by design"* dalam pengembangan sistem informasi juga

ditekankan. Prinsip ini mengharuskan bahwa perlindungan data pribadi harus menjadi bagian integral dari proses desain sistem, bukan hanya sebagai tambahan setelah sistem beroperasi (Wiese Schartum, 2017). Hal ini sejalan dengan kebutuhan untuk menciptakan sistem yang tidak hanya mematuhi regulasi tetapi juga melindungi hak-hak individu secara proaktif. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah diimplementasikan sebagai langkah maju dalam melindungi data pribadi masyarakat. Meskipun demikian, masih terdapat tantangan signifikan dalam penerapannya, termasuk kebutuhan untuk meningkatkan infrastruktur teknologi dan pemahaman masyarakat mengenai pentingnya perlindungan data pribadi (Meher dkk., 2023). Penelitian menunjukkan bahwa meskipun UU PDP memberikan kerangka hukum, implementasi yang efektif masih memerlukan penyesuaian dan peningkatan regulasi yang ada .

Salah satu aspek penting dari perlindungan data pribadi adalah pengakuan bahwa data pribadi merupakan bagian dari hak asasi manusia. Pasal 28G ayat (1) UUD 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, termasuk data pribadi mereka (Niffari, 2020). Namun, perlindungan hukum terhadap data pribadi di Indonesia yang terwujud dalam UU PDP serta beberapa undang-undang lainnya seperti UU ITE masih menemukan kendala dalam pelaksanaan dan penegakan hukumnya. Hal ini menyebabkan banyaknya aktivitas ilegal terhadap data pribadi, seperti kebocoran data *(data leak)* dan peretasan data *(data breach)*, yang berujung pada tindakan-tindakan kriminal seperti jual-beli data dan pemerasan. Peretasan data dan kebocoran data merupakan masalah penting dalam bidang keamanan informasi, yang mempengaruhi organisasi dan individu. Pelanggaran data mengacu pada insiden di mana terjadi akses tidak sah ke data sensitif, yang sering kali mengarah pada pemaparan informasi pribadi. Sebaliknya, kebocoran data biasanya melibatkan pelepasan data yang tidak disengaja, yang mungkin tidak selalu disebabkan oleh niat jahat tetapi masih dapat mengakibatkan pelanggaran privasi yang signifikan dan kerugian finansial (Hughes-Lartey dkk., 2021).

Terkait peretasan dan kebocoran data pribadi, hal ini tidak hanya berdampak terhadap individu, terlebih lagi hal ini dapat mempengaruhi kepercayaan publik terhadap institusi pemerintah dan sektor swasta selaku pihak yang dipercaya mengelola data. Kejadian kebocoran data dapat mengakibatkan kerugian finansial, reputasi, dan bahkan ancaman terhadap keamanan nasional (Hidayat dkk., 2023). Oleh karena itu, penting bagi negara untuk memiliki kerangka hukum dan kebijakan yang jelas dalam menangani masalah ini, termasuk dalam konteks putusan hukum, seperti Putusan Nomor: 269/G/TF/2024/PTUN.JKT.

Putusan ini melibatkan gugatan yang diajukan oleh Komunitas Konsumen Indonesia (KKI) terhadap Menteri Komunikasi dan Informatika Republik Indonesia di Pengadilan Tata Usaha Negara Jakarta. Gugatan ini berfokus pada dugaan kelalaian pemerintah dalam meningkatkan keamanan Pusat Data Nasional (PDN) dan menyediakan rekam cadang elektronik, yang dianggap sebagai pelanggaran terhadap standar layanan digital berkualitas. Insiden peretasan ransomware yang terjadi pada PDN menyebabkan gangguan signifikan terhadap berbagai layanan publik, termasuk sistem imigrasi, pendidikan, dan proyek strategis nasional seperti Ibu Kota Nusantara (IKN). KKI mengklaim bahwa tindakan pemerintah tidak hanya melanggar peraturan perundang-undangan, tetapi juga asas-asas umum

pemerintahan yang baik, seperti profesionalitas dan kecermatan. Dalam gugatannya, KKI mendasarkan argumen pada Pasal 40 UU ITE dan Pasal 99 PP 71/2019, yang mengatur kewajiban pemerintah untuk melindungi data strategis melalui langkah-langkah keamanan dan rekam cadang elektronik. Selain itu, KKI menilai bahwa kegagalan pemerintah untuk segera memulihkan layanan PDN menunjukkan kurangnya tanggung jawab dalam melindungi hak-hak konsumen. Gugatan ini juga menyoroti dampak luas dari insiden tersebut, termasuk terganggunya layanan publik di 56 kementerian/lembaga yang terintegrasi dengan PDN.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah yuridis-normatif, yang menekankan pada studi kepustakaan dan analisis terhadap peraturan perundang-undangan, literatur hukum, dan dokumen-dokumen terkait. Penelitian ini bersifat deskriptif, yang bertujuan untuk memberikan gambaran komprehensif dan sistematis mengenai permasalahan yang diteliti tanpa bermaksud menguji hipotesis. Dalam konteks tanggung jawab negara ketika terjadi peretasan data, pendekatan deskriptif ini memungkinkan analisis mendalam terhadap kasus-kasus konkret, termasuk Studi Putusan Nomor: 269/G/TF/2024/PTUN.JKT. Melalui penelitian ini, dapat diidentifikasi pola tanggung jawab negara dalam menghadapi insiden keamanan data, mekanisme perlindungan yang diterapkan, serta implikasi hukum yang timbul akibat peretasan tersebut. Dengan demikian, penelitian ini berkontribusi pada pemahaman yang lebih luas mengenai sejauh mana negara bertanggung jawab terhadap perlindungan data pribadi dan kebijakan yang diambil dalam merespons pelanggaran keamanan.

Pengumpulan data dalam penelitian ini dilakukan melalui metode studi pustaka dan analisis dokumen, yang mencakup peraturan perundang-undangan, putusan pengadilan, serta literatur akademik terkait tanggung jawab negara dalam kasus peretasan data. Khususnya, penelitian ini menelaah secara mendalam Putusan Nomor: 269/G/TF/2024/PTUN.JKT untuk mengidentifikasi argumentasi hukum yang digunakan serta implikasi kebijakan yang ditimbulkan. Selain itu, data sekunder diperoleh dari laporan resmi, artikel ilmiah, dan sumber kredibel lainnya guna memberikan perspektif yang lebih luas mengenai praktik perlindungan data dan respons negara terhadap insiden keamanan siber. Dengan pendekatan ini, penelitian berupaya menyusun gambaran sistematis mengenai kerangka hukum dan kebijakan yang diterapkan dalam menghadapi peretasan data.

Analisis penelitian dilakukan secara kualitatif, dengan menginterpretasi dan mengevaluasi data-data normatif yang terkumpul. Jenis penelitian yang diterapkan adalah studi kasus, yang memfokuskan pada pengkajian mendalam terhadap suatu kasus atau fenomena hukum tertentu secara spesifik. Pendekatan studi kasus dipilih untuk memperoleh pemahaman yang mendalam dan detail terhadap penerapan norma hukum dalam konteks kasus yang diteliti, serta mengidentifikasi implikasi dan tantangan yang mungkin timbul.

3. Hasil dan Pembahasan

3.1 Hasil

Penelitian ini mengidentifikasi bagaimana data yang dihimpun dari masyarakat dikelola dan disimpan oleh Pemerintah. Pemerintah, mengelola dan menyimpan

data dalam suatu sistem yang disebut Pusat Data Nasional (PDN). PDN bertujuan untuk memfasilitasi pengambilan keputusan dan perumusan kebijakan yang tepat di berbagai sektor, termasuk tata kelola pemerintahan, kesehatan, dan pembangunan ekonomi. Inisiatif ini sejalan dengan tujuan yang lebih luas untuk menciptakan ekosistem data terpadu, yang dikenal sebagai "Satu Data Indonesia", yang bertujuan untuk menyediakan data yang kredibel dan dapat dipertanggungjawabkan untuk pembuatan dan pelaksanaan kebijakan (Islami, 2021).

Regulasi mengenai PDN diatur dalam Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), dan Permenkominfo No. 1 Tahun 2023 tentang Interoperabilitas Data. Dalam menjalankan fungsinya PDN bertanggung jawab untuk mengumpulkan, menyimpan, dan mengelola data dalam jumlah besar dari berbagai sumber, memastikan bahwa data tersebut mutakhir dan dapat diandalkan (Susniwati & Zamili, 2022). Selain itu, PDN juga memiliki fungsi dalam peningkatan kualitas data, yang mana inisiatif ini bertujuan untuk meningkatkan kualitas dan standarisasi data di berbagai sektor, mengatasi tantangan yang ada, yaitu ketidakkonsistenan dan fragmentasi data (Islami, 2021).

Terlepas dari perannya yang sangat penting, PDN menghadapi beberapa tantangan seperti fragmentasi data, kapasitas dan keahlian SDM, serta kesadaran publik. Keberadaan berbagai sistem data independen di berbagai lembaga menyebabkan data terfragmentasi, sehingga menyulitkan upaya integrasi (Susniwati & Zamili, 2022). Juga terdapat tantangan akan kebutuhan tenaga terampil dalam pengelolaan dan analisis data untuk memanfaatkan data yang dikumpulkan secara efektif. Di lain sisi, perlunya meningkatkan kesadaran dan keterlibatan publik, hal ini sangat penting untuk memaksimalkan dampak PDN. PDN merupakan bagian integral dari upaya transformasi digital Indonesia. Dengan memfasilitasi tata kelola pemerintahan berbasis data, PDN berkontribusi pada peningkatan pelayanan publik. Manajemen data yang lebih baik akan menghasilkan layanan publik yang lebih efisien, menguntungkan warga negara, dan meningkatkan tata kelola pemerintahan secara keseluruhan (Islami, 2021).

Penelitian ini membahas sejauh mana negara menjamin keamanan data yang mereka kelola. Dalam menjamin keamanan data, Pemerintah Indonesia memiliki kerangka hukum serta regulasi mengenai perlindungan data pribadi dan keamanan siber, dengan UU PDP sebagai dasar utama yang memberikan hak kepada individu untuk mengontrol data pribadinya, mengatur kewajiban pengendali dan prosesor data dalam menjaga keamanan, serta menetapkan sanksi berat bagi pelanggar. UU PDP juga mengadopsi prinsip internasional seperti *General Data Protection Regulation (GDPR)* dan menjunjung asas kepastian hukum, kemanfaatan, dan kerahasiaan. Selain itu, terdapat Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia, yang bertujuan menciptakan tata kelola data terintegrasi antarinstansi pemerintah melalui standarisasi data dan pengelolaan Pusat Data Nasional (PDN). Peraturan Pemerintah Nomor 71 Tahun 2019 memperkuat aspek keamanan sistem elektronik dan mewajibkan lokalisasi data strategis di Indonesia untuk menjamin kedaulatan data. Permenkominfo Nomor 1 Tahun 2023 mendukung SPBE (Sistem Pemerintahan Berbasis Elektronik) dengan memastikan interoperabilitas data antarinstansi untuk meningkatkan efisiensi layanan publik. Di

sisi keamanan siber, Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional menekankan perlindungan infrastruktur vital dan manajemen krisis siber, termasuk keamanan PDN. Sebagai pelengkap, UU ITE berfungsi sebagai dasar hukum penanganan kejahatan siber, dengan ancaman pidana hingga 8 tahun penjara bagi pelaku peretasan sistem elektronik. Regulasi ini bersama-sama bertujuan melindungi data, mendukung transformasi digital, dan menjaga kedaulatan siber nasional. Dari kebijakan perlindungan data yang efektif memiliki implikasi yang signifikan untuk meningkatkan kepercayaan publik, dengan adanya jaminan perlindungan data, masyarakat akan lebih percaya untuk berbagi informasi pribadi mereka, baik dengan pemerintah maupun dengan sektor swasta. Kepercayaan ini penting untuk mendorong partisipasi aktif dalam program-program pemerintah (Utomo dkk., 2020). Perlindungan data yang baik juga dapat mendorong pertumbuhan ekonomi digital dengan menciptakan lingkungan yang aman bagi inovasi dan investasi di sektor teknologi informasi (Mauliza dkk., 2022).

Penelitian ini juga memberikan komparasi pengelolaan dan penyimpanan data oleh negara dan individu yang berbeda dalam skala, tujuan, tanggung jawab hukum, infrastruktur, dan dampaknya. Negara mengelola data dalam skala besar untuk keperluan pelayanan publik, perencanaan kebijakan, dan keamanan nasional, dengan menggunakan infrastruktur berstandar tinggi seperti Pusat Data Nasional dan tunduk pada regulasi ketat seperti UU PDP. Dampak kebocoran data negara dapat meluas, memengaruhi masyarakat secara masif, seperti penyalahgunaan identitas dan ancaman keamanan nasional. Sementara itu, individu mengelola data berskala kecil, seperti data pribadi atau bisnis, dengan penyimpanan di perangkat pribadi atau layanan cloud komersial. Tanggung jawab individu juga diatur UU PDP, meskipun dengan skala dan konsekuensi yang lebih terbatas, biasanya terkait kerugian lokal seperti privasi pelanggan. Kedua entitas memiliki kewajiban menghormati hak subjek data dalam pengelolaannya.

Konteks internasional, perbedaan ini semakin kompleks. Negara-negara seperti Australia telah mengambil langkah strategis untuk mengatur penggunaan data oleh perusahaan besar seperti Facebook dan Google, menuntut agar mereka membayar untuk konten yang diambil dari sumber lokal (Darmawan dkk., 2023). Ini menunjukkan bahwa negara memiliki kekuatan untuk mengatur dan memanfaatkan data dalam konteks ekonomi, sementara individu tetap berjuang untuk mempertahankan hak-hak mereka atas data pribadi. Namun walaupun sudah jelas perbedaan hak dan kewajiban antara Negara dan Individu dalam hal pengelolaan dan penyimpanan data, namun penelitian menunjukkan bahwa banyak individu tidak sepenuhnya menyadari hak-hak mereka terkait perlindungan data (Rahayu dkk., 2023).

Penelitian ini mengidentifikasi dampak strategis yang diakibatkan kejadian peretasan Pusat Data Nasional yang terjadi pada tanggal 20 Juni 2024. Secara umum, penulis menemukan dampak strategis atas terjadinya peretasan data yaitu Pertama, peretasan data dapat menyebabkan kerugian finansial yang signifikan bagi organisasi dan negara. Penelitian menunjukkan bahwa biaya yang terkait dengan pelanggaran data dapat sangat bervariasi, tergantung pada sifat dan skala pelanggaran tersebut (Dongre dkk., 2019). Kedua, peretasan data dapat merusak kepercayaan publik terhadap institusi pemerintah dan swasta. Ketika data pribadi warga negara terancam, kepercayaan masyarakat terhadap kemampuan pemerintah untuk melindungi informasi sensitif mereka menurun (Molitor dkk.,

2024). Ketiga, peretasan data dapat memiliki implikasi yang lebih luas bagi keamanan nasional. Dalam konteks ini, peretasan yang menargetkan infrastruktur kritis, seperti sistem energi atau transportasi, dapat mengakibatkan gangguan yang serius dan bahkan membahayakan keselamatan publik. Penelitian menunjukkan bahwa serangan siber terhadap infrastruktur kritis dapat menyebabkan kerugian ekonomi yang besar dan mengganggu layanan publik yang vital (Gordon dkk., 2015). Keempat, peretasan data juga dapat memicu perubahan dalam kebijakan dan regulasi terkait keamanan siber. Banyak negara telah mulai memperkuat undang-undang dan regulasi yang mengatur perlindungan data pribadi sebagai respons terhadap meningkatnya jumlah pelanggaran data (Aslam dkk., 2022).

Lebih spesifik lagi, penulis menemukan Peretasan pada Pusat Data Nasional (PDN) Indonesia tahun 2024 menimbulkan dampak multidimensi yang signifikan. Serangan siber yang melumpuhkan 210 instansi pemerintah pusat dan daerah mengganggu layanan kritis seperti administrasi imigrasi dan penyaluran Kartu Indonesia Pintar Kuliah (KIP-K) (Dwi, 2024), dengan 800 ribu data pendaftar KIP-K hilang tanpa cadangan. Kerugian finansial langsung mencapai US$8 juta untuk tebusan ransomware dan biaya migrasi darurat ke AWS sebesar Rp15 ribu dolar AS per bulan (P. Pratama, 2024), sementara kerugian ekonomi tidak langsung diperkirakan CELIOS mencapai Rp6,3 triliun dalam empat hari pertama akibat lumpuhnya transaksi digital di sektor e-commerce, logistik, dan perbankan (Azzahra, 2024). Dampak jangka panjang mencakup ancaman kebocoran 33,7 GB data sensitif militer yang dijual di dark web (P. Pratama, 2024) dan penurunan kepercayaan investor akibat kerentanan sistem keamanan berbasis Windows Defender tanpa cadangan data (Azzahra, 2024). Meski kunci dekripsi akhirnya diberikan cuma-cuma, pemulihan data tidak sepenuhnya menjamin integritas informasi yang hilang (P. Pratama, 2024), sementara kerugian immateriil termasuk terganggunya reputasi internasional Indonesia dan potensi sanksi pelanggaran UU PDP (Azzahra, 2024).

Penelitian ini penulis coba menganalisa putusan PTUN Nomor 269/G/TF/2024/PTUN.JKT terkait kasus peretasan PDN yang diajukan oleh Komunitas Konsumen Indonesia (KKI). Dalam penilaiannya, Pengadilan Tata Usaha Negara (PTUN) menganggap KKI tidak memiliki hubungan hukum yang langsung dengan objek sengketa merupakan suatu pendekatan yang terlalu formalistik, pendekatan seperti ini mengabaikan keadilan substantif serta realitas sosial. Hal ini dapat menghasilkan keputusan yang kaku dan tidak responsif terhadap dinamika masyarakat.. Sebagai Lembaga Perlindungan Konsumen Swadaya Masyarakat (LPKSM), KKI berfungsi untuk memperjuangkan hak-hak konsumen yang lebih luas, dan dalam hal ini, KKI seharusnya diberi fleksibilitas dalam hal legal standing, majelis hakim seharusnya mengerti bahwa gugatan yang diajukan merupakan *Public Interest Litigation (PIL)*. Penolakan legal standing dalam kasus ini dapat dianggap bertentangan dengan prinsip akses terhadap keadilan. Pasal 53 UU PTUN mengatur adanya hubungan hukum langsung, namun dalam konteks ini, fleksibilitas dapat diberikan untuk mendukung prinsip keadilan bagi kepentingan umum.

Tahapan *Dismissal Prosedur* sesuai Pasal 62 UU No. 5 Tahun 1986, disebutkan bahwa panitera memeriksa kelengkapan administrasi gugatan, termasuk memeriksa syarat formal seperti legal standing. Jika ditemukan gugatan yang tidak memenuhi syarat, pengadilan seharusnya mengeluarkan penetapan tidak dapat diterima tanpa melanjutkan ke tahap persidangan. Jika isu legal standing menjadi

alasan utama penolakan gugatan, seharusnya dapat diselesaikan sejak tahap ini. Dan pada Pasal 63 yaitu tahapan Pemeriksaan Persiapan, juga memberikan peluang bagi hakim untuk mengevaluasi aspek-aspek formil gugatan, termasuk keabsahan *legal standing* penggugat. Jika dalam pemeriksaan ini ditemukan cacat formil seperti tidak adanya hubungan langsung antara penggugat dan objek sengketa, hakim dapat mengeluarkan putusan sela untuk menyatakan gugatan tidak dapat diterima. Dalam kasus ini, penolakan legal standing baru diputuskan dalam eksepsi pada tahap persidangan, bukan dalam tahap persiapan. Hal ini dapat dipertanyakan karena memperpanjang proses meskipun masalah formil sudah dapat dikenali lebih awal.

Putusan PTUN yang menyatakan gugatan sebagai *obscuur libel* karena dianggap tidak jelas dalam hubungan hukum antara penggugat dan tergugat, menurut pandangan penulis, tidak sepenuhnya tepat. Gugatan KKI mengajukan dua hal yang sangat spesifik, yaitu kegagalan dalam meningkatkan keamanan PDN dan tidak dilakukannya rekam cadang elektronik. Oleh karena itu, dasar hukum gugatan tersebut (Pasal 40 UU ITE dan Pasal 99 PP 71/2019) sudah jelas dan dapat dipertanggungjawabkan. Secara hukum, pengadilan seharusnya memberi kesempatan untuk memeriksa pokok perkara lebih lanjut, mengingat tidak adanya unsur yang mendasar yang mengarah pada kaburnya gugatan tersebut. Dari sudut pandang hukum administrasi, PTUN seharusnya lebih mendalami pelanggaran asas-asas umum pemerintahan yang baik (AUPB), terutama dalam hal pelayanan yang baik dan kecermatan oleh tergugat. Kegagalan dalam menjaga data strategis PDN yang berdampak pada layanan publik seperti imigrasi dan pendidikan, seharusnya diperiksa lebih mendalam dalam konteks Pasal 10 UU Administrasi Pemerintahan. Pengadilan harusnya mempertimbangkan apakah kelalaian tersebut memenuhi syarat untuk dikategorikan sebagai pelanggaran asas AUPB, yang bertujuan untuk melindungi kepentingan masyarakat dan memastikan layanan publik yang efektif dan efisien.

3.2 Pembahasan

Sentra Pengelolaan dan Penyimpanan Data

Pusat Data Nasional (PDN) berfungsi sebagai kerangka kerja yang sangat penting untuk mengelola dan memanfaatkan data di berbagai sektor di Indonesia. Pembentukan PDN di Indonesia merupakan respons terhadap meningkatnya kebutuhan akan pengelolaan data yang efisien dalam menghadapi transformasi digital yang cepat. Sebagai pusat penyimpanan data nasional, PDN bertujuan untuk memfasilitasi pengambilan keputusan dan perumusan kebijakan yang tepat di berbagai sektor, termasuk tata kelola pemerintahan, kesehatan, dan pembangunan ekonomi. Inisiatif ini sejalan dengan tujuan yang lebih luas untuk menciptakan ekosistem data terpadu, yang dikenal sebagai “Satu Data Indonesia”, yang bertujuan untuk menyediakan data yang kredibel dan dapat dipertanggungjawabkan untuk pembuatan dan pelaksanaan kebijakan (Islami, 2021).

Regulasi mengenai PDN di Indonesia terutama diatur melalui Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Perpres 95/2018); Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Perpres 39/2019); Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019); dan Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2023 tentang Interoperabilitas

Data (Permenkominfo 1/2023). Layanan Pusat Data Nasional Sementara (PDNS) mencakup penyediaan layanan Government Cloud Computing oleh Kemkominfo, integrasi dan konsolidasi pusat data Instansi Pemerintah Pusat dan Daerah (IPPD) ke PDN, penyediaan platform proprietary dan Open Source Software untuk mendukung aplikasi umum maupun khusus Sistem Pemerintahan Berbasis Elektronik (SPBE), serta teknologi pendukung big data dan kecerdasan buatan bagi IPPD (Rahmawati, 2022).

PDN memiliki tujuan untuk menyatukan data dari berbagai kementerian dan pemerintah daerah, sehingga mengurangi silo data dan meningkatkan aksesibilitas (Susniwati & Zamili, 2022). Dengan meningkatkan jaringan komunikasi data dan sistem aplikasi, PDN mendukung pengembangan ekonomi digital Indonesia, yang sangat penting bagi pertumbuhan nasional (Dudhat & Agarwal, 2023). Dan melalui inisiatif seperti *Linked Government Data (LGD)*, PDN mendorong keterlibatan dan transparansi publik, sehingga memungkinkan warga negara untuk mengakses dan memanfaatkan data pemerintah secara efektif (Rakhmawati dkk., 2018). Selain itu, PDN memiliki beberapa fungsi penting yaitu bertanggung jawab untuk mengumpulkan, menyimpan, dan mengelola data dalam jumlah besar dari berbagai sumber, memastikan bahwa data tersebut mutakhir dan dapat diandalkan (Susniwati & Zamili, 2022). PDN juga mendorong kolaborasi di antara berbagai lembaga pemerintah, memungkinkan mereka berbagi data dan sumber daya secara efektif, yang sangat penting untuk tata kelola pemerintahan yang terkoordinasi. PDN juga memiliki fungsi dalam peningkatan kualitas data, yang mana inisiatif ini bertujuan untuk meningkatkan kualitas dan standarisasi data di berbagai sektor, mengatasi tantangan yang ada, yaitu ketidakkonsistenan dan fragmentasi data (Islami, 2021).

Penggunaan Pusat Data Nasional (PDN) direkomendasikan sebagai solusi terbaik untuk penyediaan infrastruktur TIK pemerintahan karena dapat meningkatkan efisiensi belanja dengan mengurangi duplikasi, mempercepat konsolidasi data nasional, mendukung integrasi layanan publik secara menyeluruh, serta menjamin keamanan informasi dan kedaulatan data negara maupun data pribadi warga negara Indonesia (Rahmawati, 2022). Pusat Data serta dukungan teknologi merupakan infrastruktur pendukung PDN sangat penting dalam proses pengoperasiannya. Indonesia memiliki sekitar 2.700 pusat data di berbagai kementerian dan lembaga, yang sangat penting untuk penyimpanan dan pemrosesan data (Susniwati & Zamili, 2022). Integrasi teknologi canggih, seperti cloud computing dan langkah-langkah keamanan siber, meningkatkan keamanan dan aksesibilitas data yang dikelola oleh PDN (Dudhat & Agarwal, 2023).

Terlepas dari perannya yang sangat penting, PDN menghadapi beberapa tantangan seperti fragmentasi data, kapasitas dan keahlian SDM, serta kesadaran publik. Keberadaan berbagai sistem data independen di berbagai lembaga menyebabkan data terfragmentasi, sehingga menyulitkan upaya integrasi (Susniwati & Zamili, 2022). Juga terdapat tantangan akan kebutuhan tenaga terampil dalam pengelolaan dan analisis data untuk memanfaatkan data yang dikumpulkan secara efektif. Di lain sisi, perlunya meningkatkan kesadaran dan keterlibatan publik, hal ini sangat penting untuk memaksimalkan dampak PDN (Islami, 2021).

PDN merupakan bagian integral dari upaya transformasi digital Indonesia. Dengan memfasilitasi tata kelola pemerintahan berbasis data, PDN berkontribusi pada peningkatan pelayanan publik. Manajemen data yang lebih baik akan

menghasilkan layanan publik yang lebih efisien, menguntungkan warga negara, dan meningkatkan tata kelola pemerintahan secara keseluruhan (Islami, 2021). Akses ke data yang komprehensif memungkinkan para pembuat kebijakan untuk membuat keputusan berdasarkan informasi yang dapat menjawab tantangan nasional secara efektif. Pemanfaatan data juga dapat mendorong inovasi dan pertumbuhan ekonomi, mendorong ekonomi berbasis data yang sangat penting bagi pembangunan nasional (Dudhat & Agarwal, 2023).

Pusat Data Nasional merupakan landasan bagi upaya Indonesia dalam memanfaatkan data untuk pembangunan nasional. Meskipun menghadapi beberapa tantangan, perannya dalam mendorong integrasi, keamanan, dan pemanfaatan data sangat penting untuk meningkatkan tata kelola pemerintahan dan layanan publik. Seiring dengan perjalanan Indonesia menuju transformasi digital, PDN akan tetap menjadi pemain penting dalam membentuk masa depan pengelolaan data di Indonesia. Penyimpanan data oleh badan usaha swasta merupakan aspek penting dalam pengelolaan informasi di era digital saat ini. Dengan meningkatnya volume data yang dihasilkan, badan usaha swasta berperan dalam menyediakan solusi penyimpanan yang efisien dan aman. Dalam konteks bisnis modern, penyimpanan data yang efektif sangat penting untuk mendukung operasional dan pengambilan keputusan. Badan usaha swasta, baik yang besar maupun kecil, berinvestasi dalam teknologi penyimpanan data untuk memastikan bahwa informasi yang mereka kelola dapat diakses dengan cepat dan aman. Hal ini tidak hanya mencakup penyimpanan fisik tetapi juga penyimpanan berbasis cloud yang semakin populer (Dong dkk., 2017).

Penyimpanan data masyarakat oleh pihak swasta diatur oleh beberapa regulasi penting seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur kewajiban pengendali dan prosesor data pribadi untuk melindungi kerahasiaan, keamanan, serta hak pemilik data pribadi, serta PP 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik: Mengharuskan penyimpanan data strategis dilakukan di dalam negeri, meskipun data lain dapat disimpan pada fasilitas swasta tergantung jenisnya.

Badan usaha swasta menggunakan berbagai metode untuk menyimpan data seperti Cloud, Penyimpanan Lokal, dan Blockchain. Banyak perusahaan beralih ke penyimpanan cloud karena fleksibilitas dan skalabilitas yang ditawarkannya. Penyimpanan cloud memungkinkan perusahaan untuk mengakses data dari mana saja dan kapan saja, serta mengurangi biaya infrastruktur fisik (Dong dkk., 2017). Teknologi ini juga mendukung kolaborasi yang lebih baik antar tim dan departemen. Meskipun penyimpanan cloud semakin populer, banyak perusahaan masih mengandalkan penyimpanan lokal untuk data sensitif yang memerlukan kontrol lebih ketat. Penyimpanan lokal memberikan keamanan tambahan, tetapi memerlukan investasi lebih dalam hal perangkat keras dan pemeliharaan (Kao dkk., 2013).

Teknologi blockchain juga mulai diterapkan dalam penyimpanan data untuk meningkatkan keamanan dan transparansi. Dengan sifat desentralisasi dan transparansi yang dimiliki blockchain, data dapat disimpan dengan aman dan sulit untuk dimanipulasi (Zhu dkk., 2023). Ini sangat relevan untuk industri yang memerlukan audit dan pelacakan data yang ketat. Penyimpanan data yang baik oleh badan usaha swasta memiliki implikasi yang signifikan pada peningkatan efisiensi operasional organisasi. Dengan sistem penyimpanan yang efisien,

perusahaan dapat mengakses dan menganalisis data dengan lebih cepat, yang mendukung pengambilan keputusan yang lebih baik (Dong dkk., 2017).

Penyimpanan data yang efektif juga memungkinkan perusahaan untuk mengumpulkan dan menganalisis data yang diperlukan untuk inovasi produk dan layanan (Ridwan Maksum dkk., 2020). Hal ini penting untuk mempertahankan daya saing di pasar yang semakin kompetitif. Dengan mengelola data secara aman dan transparan, perusahaan dapat membangun kepercayaan dengan pelanggan mereka. Kepercayaan ini penting untuk hubungan jangka panjang dan loyalitas pelanggan (Zhu dkk., 2023). Penyimpanan data oleh badan usaha swasta merupakan komponen penting dalam pengelolaan informasi di era digital. Meskipun tantangan seperti keamanan dan kepatuhan terhadap regulasi ada, manfaat dari penyimpanan data yang baik dapat meningkatkan efisiensi operasional, inovasi, dan kepercayaan pelanggan. Oleh karena itu, penting bagi badan usaha swasta untuk terus berinvestasi dalam teknologi dan praktik terbaik dalam penyimpanan data.

Jaminan Keamanan Data dalam Pengelolaan oleh Negara

Jaminan perlindungan dan keamanan data oleh negara merupakan isu penting dalam era digital saat ini, di mana data pribadi dan informasi sensitif semakin rentan terhadap penyalahgunaan. Negara memiliki tanggung jawab untuk melindungi data warganya melalui regulasi dan kebijakan yang efektif. Negara sebagai entitas yang memiliki otoritas hukum diharapkan dapat memberikan jaminan perlindungan terhadap data warganya. Hal ini penting untuk menjaga privasi individu dan mencegah penyalahgunaan data yang dapat merugikan masyarakat (Andriananda & Maulana, 2023). Negara memiliki tanggung jawab besar dalam memberikan jaminan terhadap data masyarakat yang mereka kelola. Hal ini diatur secara komprehensif melalui UU PDP, yang menjadi tonggak hukum utama dalam melindungi data pribadi di Indonesia.

UU PDP memberikan landasan hukum yang kuat untuk memastikan perlindungan data masyarakat, termasuk Hak Subjek Data dimana masyarakat memiliki hak untuk mengakses, memperbarui, atau menghapus data pribadinya, serta mendapatkan pemberitahuan jika terjadi kebocoran data; Kewajiban Pengendali Data yaitu Pemerintah sebagai pengendali data wajib menjaga kerahasiaan, keamanan, dan integritas data pribadi; serta Sanksi, yang mana UU PDP mengatur sanksi administratif hingga pidana bagi pihak yang lalai atau melanggar ketentuan perlindungan data pribadi, termasuk denda hingga Rp6 miliar atau hukuman penjara hingga 6 tahun.

Negara telah membangun dan mengembangkan infrastruktur untuk mendukung keamanan data, yaitu PDN. PDN dirancang untuk menyimpan data masyarakat secara terpusat dengan standar keamanan tinggi guna mencegah kebocoran. Dalam mendukunhg keamanan data, BSSN juga memiliki tugas untuk meningkatkan keamanan siber dengan melakukan audit sistem informasi pemerintah dan menangani insiden kebocoran data. Sesuai dengan UU PDP, jika terjadi kebocoran data, pemerintah diwajibkan untuk memberikan pemberitahuan tertulis kepada subjek data dalam waktu maksimal 3x24 jam setelah insiden teridentifikasi dan melakukan investigasi menyeluruh untuk menemukan penyebab kebocoran dan mengambil langkah pemulihan. Meskipun telah ada regulasi khusus yang mengatur tentang perlindungan data pribadi, namun masih terdapat tantangan

yang dihadapi dalam implementasinya. Banyak organisasi, baik publik maupun swasta, yang belum sepenuhnya mematuhi regulasi perlindungan data. Hal ini dapat disebabkan oleh kurangnya pemahaman tentang regulasi atau sumber daya yang terbatas untuk menerapkan kebijakan tersebut (Utomo dkk., 2020).

Banyak negara, termasuk Indonesia, masih menghadapi keterbatasan dalam hal sumber daya manusia dan teknologi untuk menerapkan kebijakan perlindungan data secara efektif (Rosmita dkk., 2022). Dengan meningkatnya serangan siber, perlindungan data menjadi semakin kompleks. Negara harus berinvestasi dalam teknologi dan infrastruktur untuk melindungi data dari ancaman ini (Mauliza dkk., 2022). Indonesia menghadapi banyak serangan siber setiap tahun, dengan lebih dari 700 juta serangan tercatat pada tahun 2022 saja ("RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan," 2022). Beberapa instansi pemerintah belum sepenuhnya mematuhi standar perlindungan data pribadi yang diatur dalam UU PDP, serta belum ada lembaga independen khusus yang bertugas mengawasi pelaksanaan UU PDP secara efektif.

Meningkatkan jaminan terhadap data masyarakat, langkah-langkah yang perlu dilakukan yaitu peningkatan Literasi Digital dimana asyarakat perlu dididik mengenai pentingnya perlindungan data pribadi dan cara melindunginya; penguatan Infrastruktur Keamanan, yaitu Pemerintah harus terus memperbarui sistem keamanan untuk menghadapi ancaman siber yang semakin kompleks; serta pembentukan Lembaga Independen yang bertanggung jawab langsung kepada presiden untuk mengawasi pelaksanaan UU PDP secara netral dan efektif. Dari kebijakan perlindungan data yang efektif memiliki implikasi yang signifikan untuk meningkatkan kepercayaan publik, dengan adanya jaminan perlindungan data, masyarakat akan lebih percaya untuk berbagi informasi pribadi mereka, baik dengan pemerintah maupun dengan sektor swasta. Kepercayaan ini penting untuk mendorong partisipasi aktif dalam program-program pemerintah (Utomo dkk., 2020). Perlindungan data yang baik juga dapat mendorong pertumbuhan ekonomi digital dengan menciptakan lingkungan yang aman bagi inovasi dan investasi di sektor teknologi informasi (Mauliza dkk., 2022). Perlindungan data juga berkaitan erat dengan hak asasi manusia. maka secara langsung, negara yang melindungi data pribadi warganya menunjukkan komitmen terhadap penghormatan hak asasi manusia (Nurmalasari, 2021).

Regulasi yang jelas, infrastruktur pendukung, dan langkah-langkah mitigasi risiko yang tepat, negara dapat memberikan jaminan lebih baik terhadap perlindungan data masyarakat. Namun, keberhasilan ini sangat bergantung pada implementasi regulasi secara konsisten dan peningkatan kapasitas pengendalian risiko keamanan siber.

Perbedaan Tanggung Jawab Pengelolaan Data: Negara vs Individu

Perbedaan antara negara dan individu dalam hal pengelolaan dan penyimpanan data dapat dilihat berdasarkan skala, tujuan, tanggung jawab hukum, serta dampak dari pengelolaan data tersebut.

Berdasarkan skala pengelolaan dan penyimpanan data

Negara mengelola dan menyimpan data dalam skala besar yang mencakup seluruh populasi, seperti data kependudukan (e-KTP), pajak (NPWP), kesehatan (BPJS), pendidikan, dan keamanan. Data ini sering kali disimpan dalam Pusat

Data Nasional (PDN) atau fasilitas pemerintah lainnya yang memiliki standar keamanan tinggi (Birokrasi, 2024). Sedangkan, Individu mengelola data dalam lingkup kecil, biasanya terbatas pada data pribadi atau data milik orang lain dalam konteks tertentu, seperti pelanggan bisnis kecil. Penyimpanan sering kali dilakukan di perangkat pribadi (komputer, ponsel) atau layanan cloud komersial.

Berdasarkan tujuan pengelolaan datanya

Tujuan pengelolaan data oleh negara adalah untuk pelayanan publik, perencanaan kebijakan, penegakan hukum, dan keamanan nasional (Birokrasi, 2024). Contohnya adalah penggunaan data kependudukan untuk pemilu atau distribusi bantuan sosial. Sedangkan Individu mengelola data untuk keperluan pribadi atau bisnis kecil, seperti menyimpan kontak pelanggan, dokumen pekerjaan, atau informasi keluarga.

Berdasarkan tanggung jawab hukumnya

Negara mengatur secara ketat melalui regulasi seperti UU PDP. Negara bertindak sebagai pengendali data yang wajib menjaga kerahasiaan dan keamanan data masyarakat. Jika terjadi pelanggaran (misalnya kebocoran data), negara wajib memberikan pemberitahuan kepada subjek data dalam waktu 3x24 jam dan dapat dikenai sanksi administratif atau gugatan hukum. Sedangkan tanggung jawab individu lebih terbatas tetapi tetap diatur oleh UU PDP jika mereka bertindak sebagai pengendali atau prosesor data (misalnya dalam bisnis kecil). Pelanggaran oleh individu dapat dikenai sanksi pidana atau perdata jika terbukti lalai melindungi data pribadi orang lain.

Berdasarkan infrastruktur penyimpanannya

Negara menggunakan infrastruktur skala besar seperti PDN yang dirancang dengan standar keamanan tinggi, serta sistem terintegrasi antarinstansi pemerintah (Birokrasi, 2024). Penyimpanan dilakukan secara domestik sesuai dengan PP No. 71 Tahun 2019, yang mewajibkan data strategis disimpan di dalam negeri. Sedangkan Individu biasanya menggunakan perangkat pribadi atau layanan cloud komersial seperti Google Drive, Dropbox, atau layanan lokal lainnya. Infrastruktur ini tidak selalu memenuhi standar keamanan tinggi.

Berdasarkan dampak kebocoran datanya

Kebocoran data yang dikelola negara dapat berdampak luas pada masyarakat, seperti penyalahgunaan identitas massal, gangguan pelayanan publik, hingga ancaman terhadap keamanan nasional (Annapolis dkk., t.t.). Contoh: Kebocoran data e-KTP atau BPJS Kesehatan yang berpotensi merugikan jutaan orang. Dan pada Individu dampaknya lebih terbatas pada lingkup kecil, seperti kerugian finansial bagi pelanggan atau gangguan privasi individu tertentu.

Berdasarkan hak subjek data

Negara wajib memastikan hak subjek data atas akses, pembaruan, penghapusan, dan pembatasan pemrosesan datanya sesuai UU PDP. Dan jika individu mengelola data orang lain (misalnya pelanggan), mereka juga harus menghormati hak-hak tersebut meskipun dalam skala lebih kecil. Negara memiliki tanggung jawab yang jauh lebih besar dibandingkan individu karena skala pengelolaan data yang luas dan dampaknya terhadap masyarakat secara keseluruhan. Namun demikian, baik negara maupun individu wajib mematuhi

prinsip-prinsip perlindungan data pribadi sesuai dengan UU PDP untuk menjaga privasi dan keamanan informasi yang dikelola. Dilain sisi, perbedaan antara negara dan individu dalam pengelolaan dan penyimpanan data sangat mencolok, terutama dalam konteks regulasi, tanggung jawab, dan hak privasi. Negara, sebagai entitas yang memiliki kekuasaan hukum dan administratif, bertanggung jawab untuk mengatur dan melindungi data pribadi warganya. Di sisi lain, individu memiliki hak atas data pribadi mereka dan bertanggung jawab untuk melindungi informasi tersebut dari penyalahgunaan.

Pertama, negara memiliki kewenangan untuk menetapkan regulasi yang mengatur pengelolaan data. Misalnya, di Indonesia, terdapat Undang-Undang Nomor 19 Tahun 2016 yang mengatur tentang informasi dan transaksi elektronik, yang mencakup perlindungan data pribadi (Razaq, 2023). Namun, meskipun ada regulasi, implementasi dan penegakan hukum sering kali menjadi tantangan. Penelitian menunjukkan bahwa banyak individu masih tidak mendapatkan perlindungan yang memadai terhadap penyalahgunaan data pribadi, baik oleh pemerintah maupun pihak swasta (Dewi, 2016). Hal ini menunjukkan bahwa meskipun negara memiliki kewenangan untuk mengatur, efektivitas regulasi tersebut sering kali dipertanyakan. Kedua, individu memiliki hak untuk mengontrol data pribadi mereka. Namun, penelitian menunjukkan bahwa banyak individu tidak sepenuhnya menyadari hak- hak mereka terkait perlindungan data (Rahayu dkk., 2023). Misalnya, dalam konteks penggunaan kartu prabayar, individu diwajibkan untuk mendaftar menggunakan data pribadi mereka, tetapi sering kali tidak ada sanksi yang jelas bagi penyalahguna data tersebut (Hadita, 2018). Hal ini menciptakan ketidakpastian dan risiko bagi individu, yang seharusnya dilindungi oleh negara. Ketiga, perbedaan dalam pendekatan terhadap data juga terlihat dalam konteks keamanan. Negara sering kali menggunakan data untuk kepentingan keamanan publik, seperti dalam penerapan teknologi pengenalan wajah. Meskipun teknologi ini dapat meningkatkan keamanan, ada kekhawatiran yang signifikan mengenai privasi individu dan persetujuan yang diperlukan untuk penggunaan data biometrik (Razaq, 2023). Di sisi lain, individu mungkin merasa terancam oleh pengawasan yang berlebihan dan kurangnya transparansi dalam bagaimana data mereka digunakan.

Konteks internasional, perbedaan ini semakin kompleks. Negara-negara seperti Australia telah mengambil langkah strategis untuk mengatur penggunaan data oleh perusahaan besar seperti Facebook dan Google, menuntut agar mereka membayar untuk konten yang diambil dari sumber lokal (Darmawan dkk., 2023). Ini menunjukkan bahwa negara memiliki kekuatan untuk mengatur dan memanfaatkan data dalam konteks ekonomi, sementara individu tetap berjuang untuk mempertahankan hak-hak mereka atas data pribadi. Secara keseluruhan, perbedaan antara negara dan individu dalam pengelolaan dan penyimpanan data mencerminkan ketegangan antara kekuasaan regulasi negara dan hak privasi individu. Negara memiliki tanggung jawab untuk melindungi data pribadi, tetapi sering kali gagal dalam implementasi dan penegakan hukum. Individu, di sisi lain, harus lebih sadar akan hak-hak mereka dan berusaha untuk melindungi data pribadi mereka dari penyalahgunaan.

Dampak dan Kerugian Strategis Peretasan Pusat Data Nasional

Peretasan data dapat berdampak pada terjadinya perubahan dalam berbagai sektor serta menimbulkan kerugian yang cukup besar, baik bagi pihak swasta

maupun pemerintah. Peretasan data tidak hanya mengancam privasi individu, tetapi juga dapat memiliki konsekuensi yang luas bagi keamanan nasional, ekonomi, dan reputasi institusi.

Pertama, peretasan data dapat menyebabkan kerugian finansial yang signifikan bagi organisasi dan negara. Penelitian menunjukkan bahwa biaya yang terkait dengan pelanggaran data dapat sangat bervariasi, tergantung pada sifat dan skala pelanggaran tersebut (Dongre dkk., 2019). Misalnya, perusahaan yang mengalami pelanggaran data sering kali mengalami penurunan nilai pasar yang substansial, dengan penurunan rata-rata mencapai 5,6% setelah pengumuman pelanggaran (Curtis dkk., 2018). Hal ini menunjukkan bahwa dampak finansial dari peretasan tidak hanya dirasakan oleh perusahaan itu sendiri, tetapi juga dapat mempengaruhi investor dan pemangku kepentingan lainnya.

Kedua, peretasan data dapat merusak kepercayaan publik terhadap institusi pemerintah dan swasta. Ketika data pribadi warga negara terancam, kepercayaan masyarakat terhadap kemampuan pemerintah untuk melindungi informasi sensitif mereka menurun (Molitor dkk., 2024). Penelitian menunjukkan bahwa kepercayaan konsumen terhadap perusahaan yang mengalami pelanggaran data dapat berkurang secara signifikan, yang pada gilirannya dapat mempengaruhi keputusan pembelian dan loyalitas pelanggan (Curtis dkk., 2018). Oleh karena itu, penting bagi organisasi untuk tidak hanya fokus pada pemulihan setelah pelanggaran, tetapi juga pada upaya untuk membangun kembali kepercayaan publik.

Ketiga, peretasan data dapat memiliki implikasi yang lebih luas bagi keamanan nasional. Dalam konteks ini, peretasan yang menargetkan infrastruktur kritis, seperti sistem energi atau transportasi, dapat mengakibatkan gangguan yang serius dan bahkan membahayakan keselamatan publik. Penelitian menunjukkan bahwa serangan siber terhadap infrastruktur kritis dapat menyebabkan kerugian ekonomi yang besar dan mengganggu layanan publik yang vital (Gordon dkk., 2015). Oleh karena itu, perlindungan terhadap infrastruktur ini harus menjadi prioritas utama bagi pemerintah dan lembaga terkait.

Keempat, peretasan data juga dapat memicu perubahan dalam kebijakan dan regulasi terkait keamanan siber. Banyak negara telah mulai memperkuat undang-undang dan regulasi yang mengatur perlindungan data pribadi sebagai respons terhadap meningkatnya jumlah pelanggaran data (Aslam dkk., 2022). Misalnya, pengenalan regulasi yang lebih ketat mengenai pelaporan pelanggaran data dan tanggung jawab perusahaan dalam melindungi informasi pelanggan dapat membantu mengurangi risiko pelanggaran di masa depan (D'Arcy dkk., 2022). Secara keseluruhan, dampak peretasan data nasional sangat kompleks dan melibatkan berbagai aspek, mulai dari kerugian finansial hingga implikasi terhadap kepercayaan publik dan keamanan nasional. Oleh karena itu, penting bagi semua pemangku kepentingan untuk bekerja sama dalam mengembangkan strategi yang efektif untuk melindungi data dan meminimalkan risiko pelanggaran di masa depan.

Peretasan PDN Indonesia menimbulkan kerugian multidimensi, mulai dari finansial langsung hingga gangguan sistemik. Serangan siber yang menargetkan PDNS 2 pada Juni 2024 mengakibatkan 210 instansi pemerintah pusat dan daerah lumpuh, termasuk layanan kritis seperti imigrasi dan Kartu Indonesia Pintar Kuliah (KIP-K) (Dwi, 2024). Kerugian finansial langsung mencakup tuntutan tebusan sebesar US$8 juta (Rp131 miliar) oleh peretas Brain Cipher, serta biaya migrasi

darurat layanan imigrasi ke Amazon Web Service (AWS) yang menghabiskan Rp15 ribu dolar AS per bulan (P. Pratama, 2024). Di sektor pendidikan, hilangnya data 800 ribu pendaftar KIP-Kuliah tanpa cadangan mengancam kelangsungan studi calon mahasiswa dan menghambat proses akademik (Dwi, 2024). Secara ekonomi, analisis Center of Economic and Law Studies (CELIOS) memperkirakan kerugian inefisiensi mencapai Rp1 triliun per hari akibat lumpuhnya layanan publik, dengan total kerugian empat hari pertama mencapai Rp6,3 triliun (Azzahra, 2024). Sektor bisnis seperti e-commerce, logistik, dan perbankan terdampak gangguan transaksi digital, sementara industri travel menanggung kerugian akibat penundaan penerbangan (Alwi, 2024). Studi Gartner (2014) menyebut kerugian downtime jaringan mencapai Rp132,2 miliar per hari, yang dalam kasus PDN berpotensi melesat hingga Rp1,2 triliun setelah delapan hari (Azzahra, 2024).

Dampak jangka panjang meliputi penurunan kepercayaan investor akibat kerentanan sistem keamanan data, serta risiko kebocoran 33,7 GB data sensitif BAIS TNI dan Inafis yang dijual di dark web (P. Pratama, 2024). Pakar ICT Institute menyoroti absennya pusat data cadangan dan lemahnya sistem keamanan berbasis Windows Defender sebagai akar masalah (Azzahra, 2024). Meski kunci dekripsi akhirnya diberikan cuma-cuma oleh peretas, pemulihan data tidak sepenuhnya menjamin integritas informasi yang hilang atau termanipulasi (P. Pratama, 2024). Kerugian immateriil seperti terganggunya reputasi negara dalam kerjasama internasional dan potensi sanksi akibat pelanggaran UU PDP turut menjadi beban tambahan (Azzahra, 2024).

Analisis Putusan PTUN Nomor 269/G/TF/2024/PTUN.JKT

Analisis ini didasarkan pada peraturan perundang-undangan yang berlaku di Indonesia serta kaidah dan doktrin hukum yang relevan. Fokus utama analisis adalah pada kedudukan hukum penggugat *(legal standing)*, optimalisasi penanganan *legal standing* pada Tahap *Dismissal* dan Pemeriksaan Persiapan, gugatan kabur *(obscuur libel)*, penerapan asas-asas umum pemerintahan yang baik (AUPB), serta tanggung jawab tergugat dalam pengelolaan Pusat Data Nasional (PDN).

Kedudukan Hukum *(Legal Standing)* Penggugat

PTUN menilai bahwa penggugat, Komunitas Konsumen Indonesia (KKI), tidak memiliki hubungan hukum langsung, nyata, dan pribadi dengan objek sengketa. Pendekatan ini dapat dianggap terlalu formalistik, mengingat KKI adalah Lembaga Perlindungan Konsumen Swadaya Masyarakat (LPKSM) yang bertugas memperjuangkan hak-hak konsumen serta sebagai entitas advokasi kepentingan publik, hal ini sebagaimana diatur dalam Pasal 1 Ayat (9) UU Perlindungan Konsumen. Walaupun pendekatan formalistik menjadi salah satu metode yang penting dalam upaya menjaga stabilitas dan konsistensi sistem hukum. Namun hal ini rentan mengabaikan keadilan substantif atau realitas sosial, seperti dalam kasus tersebut. Pendekatan ini juga menghasilkan keputusan yang kaku dan tidak responsif terhadap dinamika masyarakat. Fleksibilitas lega standing dapat memberikan ruang bagi perlindungan kepentingan umum, mengatasi situasi di mana korban langsung tidak mampu atau enggan menggugat, serta memastikan akuntabilitas terhadap pelanggaran yang berdampak luas. Terkait hal tersebut, PTUN perlu memutuskan bahwa pengajuan gugatan oleh pihak yang tidak secara langsung terdampak diperlukan untuk memastikan suatu masalah hukum dapat

diselesaikan dan keadilan ditegakkan, hal ini akan menjadi yurisprudensi dan sebagai landasan untuk mengambil keputusan dalam perkara yang sama dikemudian hari. Namun perlu digarisbawahi, kondisi seperti ini perlu dilandasi dengan kondisi seperti Public Interest Litigation (PIL). Gugatan yang diajukan dalam konteks PIL harus berfokus pada isu yang berkaitan dengan hak-hak publik atau kelompok tertentu, bukan kepentingan pribadi atau individu. Penggugat, meskipun tidak langsung terdampak oleh permasalahan tersebut, harus dapat menunjukkan bahwa mereka bertindak untuk kepentingan umum, mewakili kelompok yang lebih luas atau masyarakat yang terkena dampak. Selain itu, hasil dari gugatan tersebut harus memiliki potensi untuk memberikan manfaat yang lebih besar atau perlindungan yang lebih luas kepada masyarakat secara keseluruhan, bukan hanya untuk kepentingan pribadi penggugat.

Pasal 53 UU PTUN mensyaratkan adanya hubungan hukum langsung antara penggugat dan objek sengketa. Namun, dalam konteks advokasi publik, fleksibilitas seharusnya diberikan kepada LPKSM dalam melindungi hak konsumen. Teori Perlindungan Hukum seharusnya mendorong pengadilan untuk melihat bahwa KKI bertindak sebagai perwakilan kelompok konsumen yang dirugikan akibat kelalaian Tergugat dalam mengelola Pusat Data Nasional (PDN). Dengan menolak gugatan atas dasar formalitas, PTUN tidak memberikan perlindungan hukum yang memadai kepada masyarakat yang diwakili penggugat.

Penerapan Asas-Asas Umum Pemerintahan yang Baik (AUPB)

Gugatan KKI menyoroti pelanggaran asas pelayanan yang baik dan asas kecermatan oleh tergugat. Namun, PTUN tidak melakukan pemeriksaan mendalam terhadap hal ini. Tergugat dianggap gagal melindungi data strategis yang berimbas pada terganggunya layanan publik, seperti layanan imigrasi dan pendidikan. Dampak tersebut relevan untuk diuji berdasarkan Pasal 10 UU Administrasi Pemerintahan. Pemeriksaan atas pelanggaran AUPB penting dilakukan, terutama jika kelalaian tergugat menyebabkan kerugian luas pada masyarakat. Dengan tidak dievaluasinya substansi ini, putusan dapat dianggap mengabaikan aspek esensial dari gugatan.

Gugatan menyoroti bahwa Tergugat gagal menjaga keamanan Pusat Data Nasional (PDN), yang berpotensi melanggar hak atas privasi warga negara. Insiden ini menyebabkan terganggunya layanan publik yang bergantung pada data konsumen, seperti layanan imigrasi dan pendidikan. PTUN tidak secara substansial mengevaluasi apakah kelalaian Tergugat melanggar hak atas privasi masyarakat yang datanya berada di bawah pengelolaan PDN. Fokus pada aspek formalitas mengabaikan pentingnya melindungi hak asasi individu terkait privasi data. Penolakan gugatan dengan alasan formalitas mencerminkan ketidaksungguhan dalam melindungi hak atas privasi. Padahal, teori hak atas privasi menempatkan kewajiban negara untuk memastikan keamanan data sebagai elemen mendasar dari perlindungan warga negara.

Mitigasi dan Tanggung Jawab Tergugat

PTUN menerima argumen tergugat bahwa tanggung jawab rekam cadang elektronik adalah kewajiban IPPD (Instansi Pemerintah Pusat dan Daerah). Namun, ini mengabaikan tanggung jawab tergugat sebagai pengelola utama PDN, sebagaimana diatur dalam Pasal 40 Ayat (3)-(5) UU ITE. Langkah mitigasi yang dilakukan oleh tergugat setelah insiden tidak dievaluasi terhadap kewajiban hukum

dan standar internasional keamanan data. Pasal 99 PP 71/2019 mengatur bahwa pemerintah wajib membuat dokumen elektronik strategis dan rekam cadang elektronik. Argumen tanggung jawab bersama (shared responsibility) tidak membebaskan tergugat dari tanggung jawab utama.

4. Kesimpulan

Penelitian ini menyoroti pentingnya Pusat Data Nasional (PDN) dalam mengelola dan menyimpan data masyarakat sebagai bagian dari inisiatif "Satu Data Indonesia." Dengan landasan hukum yang kuat, seperti UU PDP dan Perpres tentang SPBE, PDN bertujuan menciptakan ekosistem data yang terpadu untuk mendukung pengambilan keputusan yang tepat di berbagai sektor. Meskipun demikian, penelitian ini juga mengidentifikasi tantangan besar, termasuk fragmentasi data, kurangnya tenaga terampil, dan minimnya kesadaran publik, yang perlu segera diatasi untuk meningkatkan efektivitas dan dampak PDN.

Keamanan data menjadi salah satu fokus utama penelitian ini, dengan menyoroti peran kerangka regulasi seperti UU PDP dan PP 71/2019 dalam melindungi data pribadi dan strategis. Penelitian ini menemukan bahwa pengelolaan data yang aman tidak hanya meningkatkan kepercayaan publik terhadap pemerintah tetapi juga mendorong pertumbuhan ekonomi digital melalui perlindungan inovasi dan investasi. Kebijakan perlindungan data yang efektif memberikan jaminan kepada masyarakat untuk berbagi informasi pribadi, yang penting bagi pelaksanaan program-program pemerintah berbasis digital.

Penelitian ini juga menggarisbawahi dampak strategis peretasan PDN yang terjadi pada Juni 2024, yang menyebabkan kerugian ekonomi besar hingga Rp6,3 triliun dan gangguan layanan publik di berbagai sektor. Insiden ini tidak hanya merusak kepercayaan masyarakat terhadap layanan digital pemerintah, tetapi juga memengaruhi investasi asing dan mengungkap kerentanan dalam keamanan siber nasional. Dampak ini mendorong urgensi untuk memperkuat regulasi keamanan data dan implementasi teknologi yang lebih andal. Dalam konteks hukum, penelitian ini mengkritisi putusan PTUN dalam kasus peretasan PDN yang diajukan oleh KKI. Pendekatan formalistik hakim dalam menolak legal standing KKI dinilai mengabaikan aspek keadilan substantif dan dinamika sosial, padahal gugatan ini dapat dikategorikan sebagai Public Interest Litigation (PIL). Keputusan tersebut menunjukkan perlunya fleksibilitas dalam penerapan legal standing untuk mendukung akses terhadap keadilan dan perlindungan kepentingan umum, terutama dalam isu- isu yang memiliki dampak luas terhadap masyarakat

Daftar Pustaka

Alwi, M. (2024, Juni 30). Dampak Domino Peretasan PDN: Ekonomi Tertegun, Masyarakat Panik? *Kumparan*. https://kumparan.com/muhammad-alwi-1718415649986400166/dampak-domino-peretasan-pdn-ekonomi-tertegun-masyarakat-panik-2329I5MFuBK

Andriananda, S. R., & Maulana, D. A. (2023). Kajian Metode Entry Age Normal dan Projected Unit Credit untuk Menghitung Kewajiban Aktuaria Pegawai Pemerintah dengan Perjanjian Kerja. *MATHunesa: Jurnal Ilmiah Matematika*, *11*(3), 443–457. https://doi.org/10.26740/mathunesa.v11n3.p443-457

Annapolis, A. S. A. S. writes on technology trends from, Md., IT, with a focus on government, military, & Technologies, F.-R. (t.t.). *Data Governance: What It Is and How It Enhances Data Management*. Technology Solutions That Drive Government. Diambil 1 Februari 2025, dari https://statetechmagazine.com/article/2023/11/data-governance-what-it-and-how-it-enhances-data-management-perfcon

Aslam, M., Khan Abbasi, M. A., Khalid, T., Shan, R. U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D. A., & Ahmad, R. (2022). Getting Smarter about Smart Cities: Improving Data Security and Privacy through Compliance. *Sensors*, *22*(23), 9338. https://doi.org/10.3390/s22239338

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO | Jurnal Sistem Informasi dan Teknologi Informasi*, *1*(1), 9–20. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253

Azzahra, Q. (2024, Juli 1). Menghitung Potensi Kerugian Ekonomi Negara akibat Peretasan PDN. *tirto.id*. https://tirto.id/menghitung-potensi-kerugian-ekonomi-negara-akibat-peretasan-pdn-gZ7o.

Baso, F., Isma, A., Fadhilah, N., Fajar B, M., & Surianto, D. F. (2023). Langkah-Langkah Bijak di Era Digital: Pelatihan Dasar Keamanan Data Pribadi bagi Masyarakat. *Jurnal Kemitraan Responsif untuk Aksi Inovatif dan Pengabdian Masyarakat*, 73–79. https://doi.org/10.61220/kreativa.v1i1.202310

Birokrasi, H. S. (2024, Oktober 24). Mengenal Pusat Data Nasional dan Pentingnya dalam E-Government. *Seputar Birokrasi*. https://seputarbirokrasi.com/mengenal-pusat-data-nasional-dan-pentingnya-dalam-e-government/

Bogdan, V., & Kirillova, E. (2020). Problems of personal data protection when using Big Data technologies. *Journal of Applied Engineering Science*, *18*(3), 438-442. https://doi.org/10.5937/jaes18-27927

Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, *33*(4), 425–435. https://doi.org/10.1108/MAJ-11-2017-1692

D'Arcy, J., University of Delaware, Basoglu, A., & University of Delaware. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. *Journal of the Association for Information Systems*, *23*(3), 779–805. https://doi.org/10.17705/1jais.00740

Darmawan, A. B., Saadah, K., & Utama, I. P. A. A. (2023). Kedaulatan Negara dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook dan Google. *Jurnal Hubungan Internasional*, *16*(1), 211–228. https://doi.org/10.20473/jhi.v16i1.38971

Dewi, S. (2016). KONSEP PERLINDUNGAN HUKUM ATAS PRIVASI DAN DATA PRIBADI DIKAITKAN DENGAN PENGGUNAAN CLOUD COMPUTING DI INDONESIA. *Yustisia Jurnal Hukum*, *5*(1). https://doi.org/10.20961/yustisia.v5i1.8712

Dong, F., Zhou, P., Liu, Z., Shen, D., Xu, Z., & Luo, J. (2017). Towards a fast and secure design for enterprise-oriented cloud storage systems. *Concurrency and Computation: Practice and Experience*, *29*(19), e4177. https://doi.org/10.1002/cpe.4177

Dongre, S., Mishra, S., Romanowski, C., & Buddhadev, M. (2019). Quantifying the Costs of Data Breaches. Dalam J. Staggs & S. Shenoi (Ed.), *Critical Infrastructure Protection XIII* (Vol. 570, hlm. 3–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-34647-8_1

Dudhat, A., & Agarwal, V. (2023). Indonesia's Digital Economy's Development. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *4*(2), 109–118. https://doi.org/10.34306/itsdi.v4i2.580

Dwi, A. (2024, Januari 7). 6 Dampak Serangan Ransomware ke Server PDNS. *Tempo*. https://www.tempo.co/digital/6-dampak-serangan-ransomware-ke-server-pdns-44346

Genaro, S., & Rifiyanti, H. (2023). Analyzing the Applications and Implications of Current Emerging Technologies on Digital Trends. *International Journal Education and Computer Studies (IJECS)*, *3*(3), 67–71. https://doi.org/10.35870/ijecs.v3i3.1452

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, *06*(01), 24–30. https://doi.org/10.4236/jis.2015.61003

Hadita, C. (2018). Registrasi Data Pribadi melalui Kartu Prabayar dalam Perspektif Hak Asasi Manusia. *Jurnal HAM*, *9*(2), 191. https://doi.org/10.30641/ham.2018.9.191-204

Hidayat, T., A. Ch. Likadja, J., & E. Derozari, P. (2023). Perlindungan Hukum Data Pribadi Konsumen Dalam Perdagangan Elektronik. *Journal of Comprehensive Science (JCS)*, *2*(5), 1087–1103. https://doi.org/10.59188/jcs.v2i5.323

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Islami, M. J. (2021). Implementasi Satu Data Indonesia: Tantangan dan Critical Success Factors (CSFs). *Jurnal Komunika: Jurnal Komunikasi, Media dan Informatika*, *10*(1), 13. https://doi.org/10.31504/komunika.v10i1.3750

Kao, Y., Huang, K., Gu, H., & Yuan, S. (2013). uCloud: A user-centric key management scheme for cloud data protection. *IET Information Security*, *7*(2), 144–154. https://doi.org/10.1049/iet-ifs.2012.0198

Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). PENGARUH PERLINDUNGAN DATA DAN CYBER SECURITY TERHADAP TINGKAT KEPERCAYAAN MENGGUNAKAN FINTECH MASYARAKAT DI

SURABAYA. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan*, *1*(11), 2497–2516. https://doi.org/10.54443/sibatik.v1i11.395

Meher, C., Sidi, R., & Risdawati, I. (2023). Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum dan Kebijakan di Indonesia. *Jurnal Ners*, *7*(2), 864–870. https://doi.org/10.31004/jn.v7i2.16088

Molitor, D., Saharia, A., Raghupathi, V., & Raghupathi, W. (2024). Exploring the Characteristics of Data Breaches: A Descriptive Analytic Study. *Journal of Information Security*, *15*(02), 168–195. https://doi.org/10.4236/jis.2024.152011

Munawar, Z., Indah Putri, N., Iswanto, I., & Widhiantoro, D. (2023). ANALISIS KEAMANAN PADA TEKNOLOGI BLOCKCHAIN. *Infotronik : Jurnal Teknologi Informasi dan Elektronika*, *8*(2), 67. https://doi.org/10.32897/infotronik.2023.8.2.2062

Niffari, H. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. *Jurnal Hukum dan Bisnis (Selisik)*, *6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Nurmalasari, N. (2021). Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum. *Syntax Idea*, *3*(8), 1947. https://doi.org/10.36418/syntax-idea.v6i8.1414

Pratama, P. (2024, Oktober 7). Daftar Panjang Kerugian Serangan Ransomware di Indonesia. *katadata.co.id*. https://katadata.co.id/analisisdata/668cf48a48836/daftar-panjang-kerugian-serangan-ransomware-di-indonesia

Pratama, Y., & Sutabri, T. (2023). Analisis Kriptografi Algoritma Blowfish pada Keamanan Data menggunakan Dart. *Jurnal Informatika Terpadu*, *9*(2), 126–135. https://doi.org/10.54914/jit.v9i2.975

Rahayu, I. L., Syarifa, R., Akmalia, L. R., Samosir, M. S., Hanggrita, E. P., Muflikhati, I., & Simanjuntak, M. (2023). WILLINGNESS TO SHARE DATA PRIBADI DAN KAITANNYA DENGAN PENYALAHGUNAAN DATA KONSUMEN E- COMMERCE DI INDONESIA: PENDEKATAN MIXED METHODS: Willingness to Share Personal Data and Its Relationship with E-

Commerce Consumer Data Misuse in Indonesia: A Mixed Methods Approach. *Jurnal Ilmu Keluarga dan Konsumen*, *16*(3), 274–287. https://doi.org/10.24156/jikk.2023.16.3.274

Rahmawati, F. (2022, Juli 15). Pusat Data Nasional (PDN). *Ditjen Aptika*. https://aptika.kominfo.go.id/2022/07/pusat-data-nasional-pdn/

Rakhmawati, N. A., Harits, S., Hermansyah, D., & Furqon, M. A. (2018). A Survey of Web Technologies Used in Indonesia Local Governments. *Sisfo*, *07*(03). https://doi.org/10.24089/j.sisfo.2018.05.003

Razaq, M. L. (2023). Penggunaan Teknologi Pengenalan Wajah Dalam Keamanan Publik. *JERUMI: Journal of Education Religion Humanities and Multidiciplinary*, *1*(2), 482–486. https://doi.org/10.57235/jerumi.v1i2.1403

RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan. (2022, Januari 7). *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan

Ridwan Maksum, I., Yayuk Sri Rahayu, A., & Kusumawardhani, D. (2020). A Social Enterprise Approach to Empowering Micro, Small and Medium Enterprises (SMEs) in Indonesia. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(3), 50. https://doi.org/10.3390/joitmc6030050

Rosmita, Herman, H., & Kartius. (2022). PEMBERDAYAAN MASYARAKAT MELALUI CORPORATE SOCIAL RESPONSIBILITY PADA UMKM DI KELUARAHAN BATU BERSURAT KECAMATAN XIII KOTO KAMPAR KABUPATEN KAMPAR. *PATIKALA: Jurnal Pengabdian Kepada Masyarakat*, *2*(2), 639–647. https://doi.org/10.51574/patikala.v2i2.637

S, M. R. B., Andriani Mahadewi, M., Azzahra Imani, S., & Permatasari, R. (2023). ANALISIS KEMATANGAN PENGELOLAAN KEAMANAN INFORMASI BERBASIS INDEKS KAMI DI PT. BPR JAWA TIMUR. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, *3*(1), 78–86 https://doi.org/10.33005/sitasi.v3i1.546

Sinaga, E. M. C., & Putri, M. C. (2020). FORMULASI LEGISLASI PERLINDUNGAN DATA PRIBADI DALAM REVOLUSI INDUSTRI 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 237. https://doi.org/10.33331/rechtsvinding.v9i2.428

Sinaga, R. (2024). Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022. *Jurnal Teknik Informatika dan Sistem Informasi*, *9*(3). https://doi.org/10.28932/jutisi.v9i3.6850

Susniwati, S., & Zamili, Moh. (2022). Acceleration of One Indonesian Data through Collaborative Governance in Indonesia. *Publik (Jurnal Ilmu Administrasi)*, *11*(2), 166. https://doi.org/10.31314/pjia.11.2.166-177.2022

Torre, D., Alferez, M., Soltana, G., Sabetzadeh, M., & Briand, L. (2020). *Model Driven Engineering for Data Protection and Privacy: Application and Experience with GDPR* (Versi 1). arXiv. https://doi.org/10.48550/ARXIV.2007.12046

Umam, M. S. (2019). Orientasi Etika dan Cyber Security Awareness (Studi Kasus pada UMKM di Bantul). *Akmenika: Jurnal Akuntansi dan Manajemen*, *13*(2). https://doi.org/10.31316/akmenika.v16i2.394

Utomo, H. P., Gultom, E., & Afriana, A. (2020). URGENSI PERLINDUNGAN HUKUM DATA PRIBADI PASIEN DALAM PELAYANAN KESEHATAN BERBASIS TEKNOLOGI DI INDONESIA. *Jurnal Ilmiah Galuh Justisi*, *8*(2), 168. https://doi.org/10.25157/justisi.v8i2.3479

Wiese Schartum, D. (2017). Intelligible Data Protection Legislation: A Procedural Approach. *Oslo Law Review*, *4*(1), 48–59. https://doi.org/10.18261/issn.2387-3299-2017-01-03

Zaman, R., & Hassani, M. (2020). On Enabling GDPR Compliance in Business Processes Through Data-Driven Solutions. *SN Computer Science*, *1*(4), 210. https://doi.org/10.1007/s42979-020-00215-x

Zhu, R., Wang, M., Zhang, X., & Peng, X. (2023). *Investigation of Personal Data Protection Mechanism Based on Blockchain Technology*. In Review. https://doi.org/10.21203/rs.3.rs-2988552/v1

Ziqra, Y., Sunarmi, Siregar, M., & Leviza, J. (2021). Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online. *Iuris Studia: Jurnal Kajian Hukum*. https://doi.org/10.55357/is.v2i2.146