HUKUM DINAMIKA EKSELENSIA

https://journalversa.com/s/index.php/hde Volume 07, No. 4, Desember 2025

PERTANGGUNGJAWABAN HUKUM ATAS PENYALAHGUNAAN DATA BIOMETRIK DALAM LAYANAN E-KTP

Fanny Cathelia Erianto[1]
[1]Universitas Pembangunan Nasional Veteran Jakarta
catheliafanny@gmail.com

***ABSTRACT**; The development of digital technology has become a crucial part of national development because it increases the efficiency and effectiveness of various sectors. However, this progress also poses significant risks to information security, particularly regarding biometric data in e-KTP services. Biometric data, which is unique, permanent, and difficult to counterfeit, requires strict legal protection to ensure the security, authentication, and integrity of citizens' identities. This study aims to analyze the legal protection of citizens' biometric data under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and to examine the government's legal accountability for data leaks and misuse in e-KTP services. The study uses a normative juridical method, with an analytical approach based on laws and regulations, legal doctrine, and scientific literature. The analysis includes provisions of the PDP Law, the Population Administration Law, the ITE Law, as well as academic studies related to cybersecurity and personal data protection. The research results show that the Personal Data Protection Law provides comprehensive rights for data subjects, including the rights to access, consent, deletion, and data portability. Data controllers are obligated to implement technical and administrative measures to protect biometric data. The government, as data administrator, is responsible for administrative, civil, and criminal liability in the event of data leaks or misuse and is required to implement a holistic cybersecurity system. Therefore, legal protection of biometric data in e-KTP services not only emphasizes individual rights and government obligations, but also requires the implementation of integrated procedures, technologies, and policies to minimize the risk of data leaks, maintain public trust, and ensure the safe and responsible use of personal data in the digital age.*
***Keywords:** Biometric Data, E-KTP, Personal Data Protection, Legal Liability.*

ABSTRAK; Perkembangan teknologi digital telah menjadi bagian penting dalam pembangunan nasional karena meningkatkan efisiensi dan efektivitas berbagai sektor. Namun, kemajuan ini juga menimbulkan risiko signifikan terhadap keamanan informasi, khususnya terkait data biometrik dalam

layanan e-KTP. Data biometrik yang bersifat unik, permanen, dan sulit dipalsukan membutuhkan perlindungan hukum yang ketat untuk menjamin keamanan, autentikasi, dan integritas identitas warga negara. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap data biometrik warga negara berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta menelaah pertanggungjawaban hukum pemerintah atas kebocoran dan penyalahgunaan data dalam layanan e-KTP. Penelitian menggunakan metode yuridis normatif, dengan pendekatan analisis terhadap peraturan perundang-undangan, doktrin hukum, dan literatur ilmiah. Analisis mencakup ketentuan UU PDP, UU Administrasi Kependudukan, UU ITE, serta kajian akademik terkait keamanan siber dan perlindungan data pribadi. Hasil penelitian menunjukkan bahwa UU PDP memberikan hak-hak komprehensif bagi subjek data, termasuk hak akses, persetujuan, penghapusan, dan portabilitas data, sementara pengendali data memiliki kewajiban untuk menerapkan langkah-langkah teknis dan administratif demi melindungi data biometrik. Pemerintah sebagai pengelola data bertanggung jawab secara administratif, perdata, maupun pidana apabila terjadi kebocoran atau penyalahgunaan data, dan wajib menerapkan sistem keamanan siber yang holistik. Dengan demikian, perlindungan hukum terhadap data biometrik dalam layanan e-KTP tidak hanya menekankan hak individu dan kewajiban pemerintah, tetapi juga menuntut implementasi prosedur, teknologi, dan kebijakan yang terintegrasi untuk meminimalkan risiko kebocoran data, menjaga kepercayaan publik, dan memastikan pemanfaatan data pribadi yang aman dan bertanggung jawab di era digital.

Kata Kunci: Data Biometrik, E-KTP, Perlindungan Data Pribadi, Pertanggungjawaban Hukum.

PENDAHULUAN

Pemanfaatan teknologi digital kini menjadi fondasi penting dalam agenda pembangunan nasional karena mampu meningkatkan efisiensi dan efektivitas di berbagai sektor. Teknologi tidak hanya berperan sebagai alat bantu, tetapi juga sebagai katalis yang memungkinkan pemerintah dan masyarakat mengatasi tantangan sosial dan ekonomi secara lebih cepat dan tepat. Oleh karena itu, investasi dalam pengembangan teknologi digital menjadi langkah strategis untuk mendukung pencapaian tujuan pembangunan berkelanjutan.

Namun, kemajuan teknologi juga membawa tantangan serius, salah satunya adalah isu keamanan informasi. Kebocoran data menjadi fenomena yang kerap terjadi,

menunjukkan adanya kelemahan signifikan dalam sistem digital, baik di tingkat individu maupun institusi. Masalah ini semakin kompleks ketika berhadapan dengan tindak kejahatan siber (cyber crime), yang melibatkan berbagai faktor saling terkait, seperti pelaku, korban, respons sosial, dan regulasi hukum.[1]

Penegakan hukum konvensional seringkali kesulitan menanggulangi kejahatan digital karena sifatnya yang cepat berubah dan lintas batas. Regulasi yang ada mudah menjadi usang karena perkembangan teknologi berlangsung lebih cepat dibanding pembaruan hukum. Akibatnya, muncul kekosongan hukum yang menyulitkan penanganan cyber crime secara efektif. Fenomena ini menegaskan pentingnya adaptasi hukum yang responsif terhadap kemajuan teknologi, sekaligus perlunya strategi keamanan digital yang menyeluruh untuk melindungi masyarakat dari risiko siber yang terus berkembang.[2]

Rumusan Masalah

1. Bagaimana bentuk perlindungan hukum terhadap data biometrik warga negara dalam sistem layanan e-KTP berdasarkan Undang-Undang Nomor 27 Tahun 2022 ?
2. Bagaimana pertanggungjawaban hukum pemerintah, atas terjadinya kebocoran dan penyalahgunaan data biometrik dalam penyelenggaraan layanan e-KTP?

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang menekankan pada analisis terhadap peraturan perundang-undangan, doktrin hukum, serta literatur ilmiah yang relevan dengan topik penelitian[3]. Metode ini dilakukan dengan menelaah secara sistematis dan komprehensif aturan hukum yang berlaku, termasuk

[1] Anak Agung Sugiantari et al., "Analisis Sanksi Hukum Atas Pertanggungjawaban Pemerintah Terhadap Insiden Bocornya Data Pribadi Masyarakat Dari Pusat Data Nasional (PDN) Indonesia," Jurnal Hukum Saraswati 6, no. 2 (2024): 728–41, https://e-journal.unmas.ac.id/index.php/JHS/article/view/9979.

[2] Ana Maria F. Pasaribu, "Kejahatan Siber Sebagai Dampak Negatif Dari Perkembangan Teknologi Dan Internet Di Indonesia Berdasarkan Undang-Undang No. 19 Tahun 2016 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Persfektif Hukum Pidana," Jurnal Hukum Departemen Hukum Pidana Fakultas Hukum Universitas Sumatera Utara, 2017, 1–23, https://www.scribd.com/document/545314476/Kejahatan-siber-sebagai-dampak-negatif-dari-perkembanganteknologi-dan-internet-di-indonesia

[3] Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," Gema Keadilan 7, no. 1 (2020): 20–33, https://doi.org/10.14710/gk.2020.7504.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, dan peraturan pelaksanaannya, guna memahami kerangka hukum terkait perlindungan data biometrik dalam layanan e-KTP. Selain itu, penelitian ini juga mengkaji literatur hukum sekunder, seperti buku, jurnal, artikel ilmiah, dan pendapat para ahli hukum, untuk memperkuat argumentasi dan memberikan perspektif kritis. Analisis dilakukan dengan membandingkan ketentuan hukum, menelaah prinsip-prinsip perlindungan data pribadi, serta mengidentifikasi implikasi hukum atas penyalahgunaan data biometrik. Dengan pendekatan yuridis normatif ini, penelitian bertujuan menghasilkan pemahaman yang mendalam mengenai landasan hukum, hak dan kewajiban pihak terkait, serta mekanisme pertanggungjawaban hukum dalam pengelolaan data biometrik warga negara.

HASIL DAN PEMBAHASAN

Bentuk Perlindungan Hukum Terhadap Data Biometrik Warga Negara Dalam Sistem Layanan e-KTP Berdasarkan Undang-Undang Nomor 27 Tahun 2022

Data biometrik merupakan informasi yang mencerminkan karakteristik unik dari pemiliknya dan bersifat autentik serta nyata. Menurut Muhammad Thoriq Bahri (2022), data biometrik dapat dipahami sebagai data yang memuat karakteristik fisiologis individu[4]. Pandangan ini kemudian diperluas oleh Departemen Pendidikan Pemerintah Inggris (2022), yang mendefinisikan data biometrik sebagai informasi pribadi yang mampu mengidentifikasi seseorang melalui ciri-ciri fisik, psikologis, maupun perilaku individu.[5]

Keunikan data biometrik inilah yang membedakannya dari jenis data lainnya. Karakteristik yang melekat secara eksklusif pada individu membuat data ini sulit dipalsukan, cenderung permanen, dan memiliki tingkat keandalan tinggi[6]. Karena sifat-sifat tersebut, data biometrik sering dimanfaatkan untuk tujuan keamanan dan autentikasi, seperti verifikasi identitas dalam sistem e-KTP, kontrol akses, dan aplikasi keamanan digital lainnya. Keunikan dan ketahanannya terhadap pemalsuan menjadikan data

[4] Bahri, Mohammad Thoriq. "Immigration Biometric Data Exchange Among Asean Member States: Opportunities And Challenges In Legislations." Jurnal Ilmiah Kebijakan Hukum. Vol. 15. No. 3 (November 2022). Hlm. 443-456.
[5] Departemen Edukasi Inggris. Protection of Biometric Data of Children in Schools and Colleges. London: The Open Government Licence, 2022, Hlm. 7
[6] Fennelly, Lawrence J. Effective Physical Security. Oxford: Elsevier Inc., 2013, hlm. 225

biometrik sebagai salah satu elemen paling penting dalam perlindungan identitas dan integritas sistem digital.

Penggunaan data biometrik telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari masyarakat modern. Diperkirakan pada tahun 2024, sekitar 66% pengguna ponsel di dunia akan memanfaatkan data biometrik untuk keperluan keamanan maupun transaksi pembayaran (Payment Journal, 2020). Data biometrik sendiri memiliki beragam bentuk, mulai dari sidik jari, face print, citra X-Ray, gambar MRI, hingga pola perilaku seperti ritme berjalan dan kecepatan mengetik. Berdasarkan karakteristiknya, data biometrik dibedakan menjadi dua kategori utama: biometrik fisik dan biometrik perilaku[7]. Contoh data fisik termasuk sidik jari dan face print, sedangkan ritme berjalan dan kecepatan mengetik termasuk jenis biometrik perilaku. Pemisahan ini menegaskan bahwa data biometrik tidak hanya bersifat unik dan sulit dipalsukan, tetapi juga dapat digunakan dalam berbagai aplikasi mulai dari autentikasi identitas hingga sistem keamanan digital dan transaksi elektronik.

Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), individu sebagai subjek data diberikan hak-hak yang komprehensif untuk mengontrol informasi pribadi mereka. Hak-hak ini dirancang agar setiap orang memiliki kendali penuh atas data yang dimiliki, termasuk mengetahui bagaimana data dikumpulkan, diproses, disimpan, dan dibagikan. Subjek data juga berhak memberikan persetujuan atau menarik persetujuan tersebut, meminta penghapusan data yang sudah tidak relevan atau diperoleh secara ilegal, serta mengajukan keberatan apabila data mereka diproses di luar tujuan awal. Lebih jauh lagi, UU PDP memberikan hak akses dan portabilitas data, sehingga subjek data dapat menyalin atau memindahkan data pribadi ke penyedia layanan lain. Bagi data sensitif, seperti informasi kesehatan, biometrik, dan data anak, pengelola data diwajibkan menerapkan perlindungan lebih ketat dan memperoleh persetujuan khusus, sehingga tercipta keseimbangan antara hak privasi individu dan kepentingan pengelolaan data di era digital.[8]

Di sisi lain, pihak yang berperan sebagai pengendali data baik itu lembaga pemerintah, perusahaan, maupun individu mempunyai tanggung jawab besar untuk

[7] Fennelly, Lawrence J. Effective Physical Security. Oxford: Elsevier Inc., 2013, hlm, 255
[8] Miyuki Fattah Rizki dan Abdul Salam. 2023. Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris). Lex Patrimonium, Vol. 2, Iss. 2 [2023]

memastikan setiap proses pengelolaan data dilakukan secara sah, terbuka, dan dapat dipertanggungjawabkan. Sebelum data pribadi dikumpulkan atau digunakan, pengendali data wajib memperoleh persetujuan yang sah dan jelas dari pemilik data. Persetujuan ini harus diberikan secara sukarela dengan pemahaman penuh mengenai tujuan pengumpulan, jenis data yang dikumpulkan, serta cara penyimpanan dan penggunaannya.

Lebih dari itu, pengendali data harus menjamin keamanan informasi melalui penerapan standar perlindungan yang kuat, baik secara teknis maupun administratif. Upaya tersebut dapat berupa penggunaan sistem enkripsi, penerapan keamanan berlapis, dan pembatasan akses hanya untuk pihak yang berwenang. Apabila terjadi kebocoran data, mereka berkewajiban untuk segera melaporkan insiden tersebut kepada pihak terkait, termasuk subjek data dan lembaga pengawas, dalam waktu paling lambat 3 x 24 jam agar dampak yang timbul dapat segera diminimalkan. [9]

Selanjutnya, pengendali data harus menyediakan saluran pengaduan yang mudah diakses, sehingga masyarakat dapat mengajukan pertanyaan, keberatan, atau permintaan penghapusan data pribadi dengan cepat dan transparan. Untuk instansi yang mengelola data dalam jumlah besar atau bersifat sensitif, Undang-Undang Perlindungan Data Pribadi (UU PDP) menganjurkan penunjukan Data Protection Officer (DPO). Petugas ini berperan penting dalam memastikan kepatuhan terhadap regulasi, memberi saran kebijakan internal, serta menjadi penghubung resmi dengan otoritas pengawas. Selain itu, setiap pengendali data wajib menyimpan catatan pemrosesan data dan bukti persetujuan dari subjek data sebagai dokumen hukum jika terjadi sengketa.

Tanggung jawab ini tetap melekat bahkan ketika pengendali data bekerja sama dengan pihak ketiga atau penyedia jasa pengolahan data. Oleh karena itu, perlu dibuat perjanjian tertulis yang secara tegas mengatur standar keamanan dan batas tanggung jawab masing-masing pihak. Untuk memastikan kepatuhan, UU PDP juga menetapkan sanksi yang tegas mulai dari denda administratif hingga 2% dari pendapatan tahunan perusahaan, hingga sanksi pidana bagi pelanggaran berat seperti penjualan data pribadi secara ilegal.

[9] Muhammad Yudistira and Ramadani Ramadani, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh KOMINFO," Jurnal Unnes Law Review 5, no. 4 (2023): 3917–29, https://doi.org/10.31933/unesrev.v5i4.698.

Melalui pengaturan yang komprehensif ini, UU PDP tidak hanya melindungi hak-hak pemilik data pribadi, tetapi juga mendorong terciptanya budaya pengelolaan data yang transparan, aman, dan beretika, sehingga kepercayaan masyarakat terhadap sistem digital dapat terus terjaga di tengah pesatnya perkembangan teknologi.[10]

Pertanggungjawaban Hukum Pemerintah, Atas Terjadinya Kebocoran Dan Penyalahgunaan Data Biometrik Dalam Penyelenggaraan Layanan e-KTP

Pertanggungjawaban hukum pemerintah atas kebocoran dan penyalahgunaan data biometrik dalam penyelenggaraan layanan e-KTP diatur melalui berbagai mekanisme hukum. Secara hukum, pemerintah wajib melindungi data pribadi warga negara, termasuk data biometrik, berdasarkan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Jika terjadi kebocoran atau penyalahgunaan data, pemerintah dapat dikenai pertanggungjawaban administratif berupa peringatan, pembatasan pemrosesan data, atau kewajiban memperbaiki sistem keamanan. Selain itu, pertanggungjawaban perdata dapat muncul jika warga yang menjadi korban menuntut ganti rugi akibat kerugian material maupun immaterial akibat kebocoran data, terutama jika terbukti adanya kelalaian pemerintah dalam pengelolaan data. Di sisi pidana, pihak yang sengaja atau lalai menyebarluaskan atau memanfaatkan data biometrik secara ilegal dapat dijerat sesuai ketentuan UU PDP, UU ITE, dan KUHP. Selain tanggung jawab hukum formal, pemerintah juga memiliki tanggung jawab moral untuk memberi perlindungan maksimal, memberitahukan jika terjadi kebocoran, dan menyediakan mekanisme pemulihan bagi korban. Upaya pencegahan, seperti penerapan sistem keamanan siber yang ketat, audit rutin, dan edukasi publik, menjadi bagian penting untuk meminimalkan risiko kebocoran dan menjaga kepercayaan masyarakat terhadap layanan e-KTP.

Dalam kerangka hukum Indonesia, perlindungan terhadap data pribadi, termasuk data biometrik dalam layanan e-KTP, memiliki landasan yang jelas dan sanksi yang tegas. Misalnya, Pasal 31 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menegaskan bahwa setiap orang yang dengan sengaja dan melawan hukum

[10] Rosa Aqilah, Deli Waryenti, and Pipi Susanti, "Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," Jurnal Ilmiah Kutei 23, no. 2 (2024): 158–72, https://doi.org/10.33369/jik.v23i2.34476.

melakukan penyadapan elektronik terhadap informasi atau dokumen elektronik yang bersifat pribadi, baik menimbulkan perubahan atau tidak, dapat dijerat sanksi pidana sesuai Pasal 47 UU ITE, yaitu penjara maksimal sepuluh tahun dan/atau denda hingga delapan ratus juta rupiah. Sementara itu, Pasal 33 UU ITE menekankan bahwa setiap tindakan yang secara sengaja dan tanpa hak mengganggu atau menyebabkan sistem elektronik tidak bekerja, diatur dalam Pasal 49 UU ITE dengan ancaman pidana maksimal sepuluh tahun dan/atau denda hingga sepuluh miliar rupiah.

Selain itu, Undang-Undang Perlindungan Data Pribadi (UU PDP) menuntut agar pengelola data, baik pemerintah, badan usaha, maupun individu, menjalankan tahapan keamanan yang memadai untuk menjaga kerahasiaan dan integritas informasi pribadi. Keamanan siber tidak sekadar soal teknologi, tetapi juga proses dan kebijakan yang mendukung pemanfaatan teknologi tersebut. Sebagaimana diungkapkan dalam studi Cate, pendekatan keamanan siber yang efektif harus bersifat holistik, mencakup aspek teknologi, manusia, dan prosedur operasional untuk meminimalkan risiko kebocoran data maupun serangan siber.

Setiap pengelola sistem elektronik memiliki kewajiban melindungi data pribadi yang dikelolanya, mulai dari tahap perolehan, pengumpulan, pengolahan, analisis, penyimpanan, perbaikan, pembaruan, hingga penampilan, pengumuman, transfer, penyebarluasan, dan penghapusan data. Proses pengelolaan ini harus selalu didasarkan pada persetujuan sah dari pemilik data, dengan tujuan yang jelas dan telah disampaikan sebelumnya. Dengan demikian, pengaturan ini menegaskan bahwa tanggung jawab atas keamanan data pribadi tidak hanya bersifat teknis, tetapi juga mencakup aspek hukum, etika, dan prosedural, untuk menjamin hak warga negara tetap terlindungi dalam era digital.

Keamanan data pribadi menjadi perhatian utama, khususnya ketika lembaga pemerintah bertindak sebagai pengendali data yang paling berperan dalam pengelolaan informasi warga negara. Dalam hal terjadinya kebocoran data pribadi di pusat data nasional, pemerintah tidak dapat mengabaikan tanggung jawabnya. Pasal 47 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan bahwa pengendali data memiliki tanggung jawab penuh atas pemrosesan data pribadi serta wajib mematuhi prinsip-prinsip perlindungan data.

Selain itu, Pasal 12 UU PDP memberikan perlindungan hukum bagi subjek data, yakni hak untuk menuntut dan memperoleh ganti rugi apabila terjadi pelanggaran dalam pengelolaan data pribadi yang dilakukan oleh pengendali data. Dengan demikian, setiap kelalaian pemerintah dalam menjaga keamanan data dapat menimbulkan konsekuensi hukum, baik administratif maupun perdata, sesuai mekanisme yang telah diatur.[11]

Dari analisis ini, dapat ditarik kesimpulan bahwa dalam penyelenggaraan pusat data nasional, pemerintah memikul kewajiban hukum yang jelas untuk memastikan keamanan data pribadi, bertindak transparan dalam pemrosesan data, serta menyediakan mekanisme pertanggungjawaban yang efektif apabila terjadi kebocoran atau penyalahgunaan informasi warga negara. Tanggung jawab ini tidak hanya bersifat formal, tetapi juga mencerminkan komitmen moral pemerintah untuk melindungi hak privasi masyarakat dalam era digital.

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa perlindungan hukum terhadap data biometrik warga negara dalam layanan e-KTP diatur secara komprehensif melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. UU ini memberikan hak penuh kepada individu untuk mengontrol data pribadinya, termasuk hak akses, persetujuan, penghapusan, keberatan, dan portabilitas data. Pengendali data, baik instansi pemerintah maupun pihak swasta, memiliki kewajiban untuk menjamin keamanan, transparansi, dan akuntabilitas dalam pengolahan data, termasuk penerapan mekanisme teknis seperti enkripsi, pembatasan akses, serta penunjukan Data Protection Officer untuk pengawasan.

Selain itu, pertanggungjawaban hukum pemerintah atas kebocoran dan penyalahgunaan data biometrik mencakup dimensi administratif, perdata, dan pidana. Pemerintah berkewajiban melindungi data warga, memperbaiki sistem keamanan bila terjadi pelanggaran, serta menyediakan mekanisme pemulihan bagi korban. Sanksi tegas dari UU PDP dan UU ITE menegaskan pentingnya tanggung jawab hukum formal, sementara tanggung jawab moral menekankan perlindungan maksimal dan transparansi terhadap masyarakat.

[11] Hezkiel Bram Setiawan and Fatma Ulfatun Najicha, "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data," Jurnal Kewarganegaraan 6, no. 1 (2022): 976–82, https://doi.org/10.31316/jk.v6i1.2657.

Dengan demikian, pengelolaan data biometrik dalam layanan e-KTP menuntut keseimbangan antara inovasi digital, perlindungan hak individu, dan penerapan regulasi yang adaptif. Pendekatan hukum yang holistik, mencakup aspek teknis, prosedural, dan etis, menjadi kunci untuk menjamin keamanan data, mencegah penyalahgunaan, serta membangun kepercayaan publik terhadap sistem digital nasional.

DAFTAR PUSTAKA

Anak Agung Sugiantari et al., "Analisis Sanksi Hukum Atas Pertanggungjawaban Pemerintah Terhadap Insiden Bocornya Data Pribadi Masyarakat Dari Pusat Data Nasional (PDN) Indonesia," Jurnal Hukum Saraswati 6, no. 2 (2024): 728–41, https://e-journal.unmas.ac.id/index.php/JHS/article/view/9979.

Ana Maria F. Pasaribu, "Kejahatan Siber Sebagai Dampak Negatif Dari Perkembangan Teknologi Dan Internet Di Indonesia Berdasarkan Undang-Undang No. 19 Tahun 2016 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Persfektif Hukum Pidana," Jurnal Hukum Departemen Hukum Pidana Fakultas Hukum Universitas Sumatera Utara, 2017, 1–23, https://www.scribd.com/document/545314476/Kejahatan-siber-sebagai-dampak-negatif-dari-perkembanganteknologi-dan-internet-di-indonesia

Bahri, Mohammad Thoriq. "Immigration Biometric Data Exchange Among Asean Member States: Opportunities And Challenges In Legislations." Jurnal Ilmiah Kebijakan Hukum. Vol. 15. No. 3 (November 2022). Hlm. 443-456.

Departemen Edukasi Inggris. Protection of Biometric Data of Children in Schools and Colleges. London: The Open Government Licence, 2022, Hlm. 7

Fennelly, Lawrence J. Effective Physical Security. Oxford: Elsevier Inc., 2013, hlm. 225

Hezkiel Bram Setiawan and Fatma Ulfatun Najicha, "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data," Jurnal Kewarganegaraan 6, no. 1 (2022): 976–82, https://doi.org/10.31316/jk.v6i1.2657.

Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," Gema Keadilan 7, no. 1 (2020): 20–33, https://doi.org/10.14710/gk.2020.7504.

Miyuki Fattah Rizki dan Abdul Salam. 2023. Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data

(Studi Kasus Clearview AI Inc. di Yunani dan Inggris). Lex Patrimonium, Vol. 2, Iss. 2.

Muhammad Yudistira and Ramadani Ramadani, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh KOMINFO," Jurnal Unnes Law Review 5, no. 4 (2023): 3917–29, https://doi.org/10.31933/unesrev.v5i4.698.

Rosa Aqilah, Deli Waryenti, and Pipi Susanti, "Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," Jurnal Ilmiah Kutei 23, no. 2 (2024): 158–72, https://doi.org/10.33369/jik.v23i2.34476.