CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol.15 No.11 Tahun 2025
Prefix doi.org/10.3783/causa. v2i9.2461

Tanggung Jawab Kementerian Pertahanan Dalam Mengatasi Terjadinya Kebocoran Data di Lingkup Kementerian Pertahanan

Dwi Julica Sari[1], Lili Sintia[2], Nawfal Sanie Iswandi[3] , Agung Trie Putra[4] , Pipi Susanti[5]

Email: dwijulicasari@gmail.com , lilisintia97@gmail.com , nawfaliswandi@gmail.com , agungbkl2004@gmail.com , pipi@unib.ac.id

Fakultas Hukum Universitas Bengkulu

Abstrack

This article examines the responsibility of the Ministry of Defense in addressing personal data breaches that may disrupt national security. Data leaks within the defense sector not only create administrative losses but also endanger defense strategy confidentiality and undermine state sovereignty. This study employs a normative legal method with statute and case approaches, focusing on Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). The findings reveal that the Ministry of Defense's legal responsibility encompasses three main dimensions: preventive, corrective, and normative. The preventive responsibility involves building robust cybersecurity systems, the corrective dimension covers system recovery and notification to data subjects, while the normative responsibility emphasizes legal certainty and the application of sanctions in cases of negligence. By consistently implementing these responsibilities, the Ministry of Defense can strengthen personal data protection, maintain public

Article History

Received: Agustus 2025

Reviewed: Oktober 2025

Published: Oktober 2025

Copyright: Author

Publish by: CAUSA

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol.15 No.11 Tahun 2025
Prefix doi.org/10.3783/causa. v2i9.2461

trust, and ensure national defense stability.

Keywords*: Personal Data Protection, legal responsibility, Ministry of Defense, data breach, national security.*

Abstrak

Artikel ini membahas tanggung jawab Kementerian Pertahanan dalam menghadapi kasus kebocoran data pribadi yang berpotensi mengganggu keamanan nasional. Kebocoran data di lingkungan pertahanan tidak hanya menimbulkan kerugian administratif, tetapi juga mengancam kerahasiaan strategi pertahanan serta melemahkan kedaulatan negara. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan kasus, khususnya dengan menelaah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Hasil penelitian menunjukkan bahwa tanggung jawab hukum Kementerian Pertahanan meliputi tiga dimensi utama, yaitu preventif, korektif, dan normatif. Preventif berupa kewajiban membangun sistem keamanan siber yang kokoh, korektif mencakup pemulihan sistem dan pemberitahuan kepada subjek data, sedangkan normatif menekankan pemenuhan prinsip kepastian hukum serta penerapan sanksi apabila terjadi kelalaian. Dengan melaksanakan ketiga tanggung jawab tersebut secara konsisten, Kementerian Pertahanan dapat memperkuat perlindungan data pribadi, menjaga kepercayaan publik, serta menjamin stabilitas pertahanan

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol.15 No.11 Tahun 2025
Prefix doi.org/10.3783/causa. v2i9.2461

negara. **Kata Kunci: Perlindungan Data Pribadi, tanggung jawab hukum, Kementerian Pertahanan, kebocoran data, keamanan nasional.**	

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol.15 No.11 Tahun 2025
Prefix doi.org/10.3783/causa. v2i9.2461

PENDAHULUAN

Kementerian Pertahanan Republik Indonesia atau disingkat Kemhan RI adalah kementerian dalam Pemerintah Indonesia yang membidangi urusan pertahanan. Kementerian Pertahanan dipimpin oleh seorang Menteri Pertahanan (Menhan) yang sejak 21 Oktober 2024 dijabat oleh Sjafrie Sjamsoeddin. Kementerian Pertahanan merupakan salah satu dari tiga kementerian (bersama Kementerian Luar Negeri dan Kementerian Dalam Negeri) yang disebutkan secara eksplisit dalam UUD 1945. Kementerian ini tidak dapat diubah atau dibubarkan oleh presiden, karena Menteri Pertahanan secara bersama-sama dengan Menteri Luar Negeri dan Menteri Dalam Negeri bertindak sebagai pelaksana tugas kepresidenan jika Presiden dan Wakil Presiden mangkat, berhenti, diberhentikan, atau tidak dapat melakukan kewajibannya dalam masa jabatannya secara bersamaan.

Perkembangan teknologi informasi dan komunikasi di era digital telah memberikan dampak yang signifikan terhadap hampir seluruh aspek kehidupan, termasuk di bidang pertahanan dan keamanan negara. Perkembangan digital pada lembaga pemerintahan, khususnya di lingkungan Kementerian Pertahanan Republik Indonesia, membawa peluang sekaligus tantangan yang kompleks. Salah satu tantangan yang paling krusial adalah kerentanan terhadap serangan siber, yang berpotensi mengakibatkan kebocoran data data pribadi dan data rahasia negara. Kasus kebocoran data yang terjadi di instansi strategis seperti Kementerian Pertahanan ini tidak hanya berdampak pada kerugian administratif atau reputasi kelembagaan, melainkan juga berimplikasi langsung terhadap keamanan nasional.

Kasus kebocoran data berkaitan erat dengan tanggung jawab negara dalam melindungi data data strategis yang dimilikinya. Kementerian Pertahanan sebagai institusi yang memiliki otoritas di bidang pertahanan negara memegang data sensitif yang mencakup data pribadi, strategi pertahanan, intelijen, hingga kerja sama internasional. Apabila data-data tersebut jatuh ke tangan pihak yang tidak bertanggung jawab, maka ancaman yang timbul bukan hanya sebatas pelanggaran hukum, tetapi juga potensi ancaman terhadap kedaulatan negara dan stabilitas nasional.[1]

Salah satu kasus kebocoran data yang pernah terjadi yakni pada November 2023 tentang kebocoran Data Pribadi 667 User dan 37 Karyawan di situs web kementerian pertahanan. Undang-

[1] Jimly Asshiddiqie, Hukum Tata Negara dan Pilar-Pilar Demokrasi (Jakarta: Konstitusi Press, 2015), hlm. 218.

Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang memberikan kerangka hukum terkait kewajiban pengendali data dalam menjaga kerahasiaan dan keamanan data yang dikelolanya.[2]

Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.

Secara Praktis tanggung jawab Kementerian Pertahanan dalam menghadapi kasus kebocoran data harus dianalisis melalui beberapa aspek. Pertama, dari aspek regulasi internal kementerian, yaitu sejauh mana Kementerian Pertahanan memiliki mekanisme dan instrumen hukum dalam mengatur keamanan data dan sanksi bagi pihak yang lalai. Kedua, dari aspek regulasi nasional, yakni apakah kebocoran data tersebut dapat dikualifikasikan sebagai pelanggaran hukum menurut Undang-Undang PDP.[3]

Dalam Penelitian terdahulu, penelitian Heru Susetyo, lebih banyak membahas perlindungan data pribadi dalam kerangka hukum nasional, tanpa menyoroti secara spesifik implikasi kebocoran data di institusi pertahanan.[4] Begitu pula, kajian Aidul Fitriciada Azhari menitikberatkan pada kebijakan keamanan nasional, namun belum membahas secara rinci mengenai tanggung jawab hukum kementerian ketika terjadi kebocoran data pribadi.[5] Dengan demikian, masih ada celah penelitian yang perlu diisi mengenai tanggung jawab Kementerian Pertahanan dalam menghadapi kasus kebocoran data pribadi yang terjadi di kementerian pertahanan.

Artikel ini menghadirkan novelty yakni mengkaji secara lebih spesifik bagaimana tanggung jawab Kementerian Pertahanan dalam menghadapi kebocoran data. Maka dari itu penulis akan membahas mengenai Bagaimana tanggung jawab Kementerian Pertahanan dalam menghadapi kasus kebocoran data pribadi yang terjadi di kementerian pertahanan?

---

[2] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 200.
[3] Jimly Asshiddiqie, Pengantar Ilmu Hukum Tata Negara (Jakarta: Rajawali Pers, 2010), hlm. 98.
[4] Ibid.
[5] Aidul Fitriciada Azhari, Hukum dan Kebijakan Keamanan Nasional di Indonesia, hlm. 150.

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol.15 No.11 Tahun 2025
Prefix doi.org/10.3783/causa. v2i9.2461

METODE PENELITIAN

Artikel ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan kasus (case approach). Penelitian ini bersifat deskriptif-analitis dengan menelaah peraturan perundang-undangan yang mengatur tentang keamanan dan perlindungan data, seperti UUD NRI 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, sekaligus mengkaji kasus kebocoran data di lingkungan Kementerian Pertahanan sebagai studi kasus. Bahan hukum yang digunakan terdiri dari bahan hukum primer berupa peraturan perundang-undangan dan dokumen resmi kebijakan pertahanan, bahan hukum sekunder berupa buku, jurnal, dan artikel ilmiah yang relevan, serta bahan hukum tersier berupa kamus dan ensiklopedia hukum. Analisis dilakukan dengan menghubungkan norma hukum yang berlaku dengan realitas kebocoran data pertahanan guna menilai bentuk tanggung jawab Kementerian Pertahanan.

ANALISIS DAN PEMBAHASAN

Kementerian Pertahanan (Kemenhan) sebagai institusi strategis negara memiliki kewajiban hukum yang sangat kuat dalam mengelola dan melindungi data yang ada. Kasus kebocoran data yang pernah menimpa sistem informasi internal Kemenhan menjadi bukti nyata bahwa pertahanan siber belum sepenuhnya kokoh. Dalam konteks regulasi, kewajiban ini telah ditegaskan dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). [6] Oleh karena itu, jika terjadi kebocoran, Kemenhan memiliki tanggung jawab untuk melakukan pencegahan, penanganan, hingga pemulihan sistem.[7] Dari sisi tanggung jawab preventif, Kemenhan dituntut untuk menerapkan standar keamanan siber berlapis, antara lain melalui klasifikasi data strategis, enkripsi, serta pengelolaan akses yang ketat. Selain itu, Kemenhan perlu memiliki Computer Security Incident Response Team (CSIRT) internal yang bertugas melakukan deteksi dini, monitoring, serta penanganan insiden kebocoran data secara cepat.[8] Langkah ini sejalan dengan Peraturan Presiden No. 47 Tahun 2023

[6] Fachrudin Sembiring & Figo M. Pattihahuan, Peran BSSN dalam Kasus Serangan Siber Kebocoran Data, Gloria Justitia (2025)
[7] Imanuel Toding Bua & Nur I. Idris, Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional 2024, Desentralisasi (2025).
[8] Farlin H. Sigiro dkk., Collaborative Sharing Intelijen Ancaman pada Komunitas CSIRT, Syntax Literate (2024).

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol.15 No.11 Tahun 2025
Prefix doi.org/10.3783/causa. v2i9.2461

tentang Strategi Keamanan Siber Nasional, yang menekankan pentingnya kesiapsiagaan siber pada lembaga strategis negara.[9] Dengan membangun mekanisme pencegahan yang kuat, Kemenhan dapat meminimalisir potensi kebocoran yang bersumber dari serangan siber eksternal maupun kelalaian internal.[10] Namun, tanggung jawab tersebut tidak berhenti pada aspek pencegahan. Jika kebocoran data terjadi, Kemenhan memiliki kewajiban korektif berupa pemulihan sistem, investigasi penyebab kebocoran, serta penyampaian informasi kepada publik sesuai amanat UU PDP.[11] Keterbukaan informasi ini menjadi penting untuk menjaga kepercayaan masyarakat sekaligus menunjukkan akuntabilitas negara. Dalam praktiknya, respons terhadap insiden kebocoran data sering kali bersifat reaktif dan kurang transparan, sehingga memperburuk citra institusi.[12] Oleh karena itu, Kemenhan harus memperkuat manajemen krisis dengan SOP yang jelas, penyediaan cadangan data (backup), serta peningkatan koordinasi dengan Badan Siber dan Sandi Negara (BSSN).[13] Selain tanggung jawab preventif dan korektif, terdapat pula tanggung jawab normatif yang harus dipenuhi. Sebagai lembaga negara, Kemenhan wajib tunduk pada prinsip kepastian hukum, kemanfaatan, dan keadilan dalam pengelolaan data strategis. Apabila terbukti lalai dalam menjalankan kewajiban hukum, sanksi administratif maupun disiplin dapat dijatuhkan sesuai dengan ketentuan UU PDP dan PP 71/2019.[14] Meski demikian, praktik penegakan hukum terhadap lembaga pemerintahan sering kali belum konsisten, sehingga akuntabilitas kelembagaan masih dipertanyakan. Oleh karena itu, internalisasi aturan melalui peraturan menteri pertahanan atau kebijakan khusus mengenai keamanan siber menjadi penting untuk memastikan penerapan hukum berjalan efektif di lingkup Kemenhan.[15] Dengan demikian, bentuk tanggung jawab hukum Kemenhan dalam menghadapi kasus kebocoran data dapat dipetakan ke dalam tiga dimensi: preventif, yakni kewajiban

[9] Balqis F. Bintang Semesta, Keamanan Siber: Respon Strategis Indonesia terhadap Ancaman Digital, Triwikrama (2025).
[10] Syarifa Tommy & M.I.P. Nasution, Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah, JMEB (2024)
[11] Ghalib Y.W., Analisis Perkembangan Keamanan Siber Dampak Kebocoran Data PDNS 2 Surabaya, JISCO (2025)
[12] Annisa Erikha & Z.A. Hoesein, Strategi Pencegahan Kebocoran Data Pribadi melalui Peran Kominfo dan Gerakan Siberkreasi, Retentum (2025)
[13] Hani P. Sari dkk., Efektivitas Hukum Perlindungan Data Pribadi terhadap Kejahatan Siber di Indonesia, Jurnal Media Akademik (2023)
[14] M.I. Hilmy & R.H.N. Azmi, Konstruksi Pertahanan dan Keamanan Negara terhadap Perlindungan Data dalam Cyberspace, Jurnal Lemhannas RI (2021).
[15] Elfirda Putri dkk., Keamanan Nasional dalam Menghadapi Perubahan Cyber Warfare, Mercatoria (2023)

membangun sistem keamanan siber yang kokoh; korektif, yaitu kewajiban pemulihan, investigasi, dan transparansi pasca insiden; serta normatif, berupa pemenuhan prinsip hukum dan akuntabilitas kelembagaan. Implementasi yang konsisten dari ketiga dimensi ini akan menentukan sejauh mana Kemenhan mampu melindungi data strategis pertahanan sekaligus memperkuat kepercayaan publik terhadap ketahanan siber nasional.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) turut memberikan landasan normatif atas tanggung jawab kementerian dan lembaga negara dalam menjaga kerahasiaan data pribadi, meskipun dalam kasus pertahanan negara cakupannya lebih luas karena menyangkut data strategis dan bukan hanya data pribadi masyarakat. Pasal 35 UU PDP menegaskan bahwa pengendali data wajib mencegah terjadinya akses ilegal, pengungkapan tidak sah, serta perusakan data.[16] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan regulasi khusus yang mengatur pelindungan data pribadi dan menjadi lex specialis terhadap aturan mengenai data pribadi. Undang-Undang ini terdiri atas 78 Pasal dan 18 Bab yang didalamnya mengatur mengenai subjek data pribadi, pengelolaan data pribadi, transfer data pribadi, sanksi administratif, kelembagaan, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara, larangan dalam penggunaan data pribadi, ketentuan pidana, hingga ketentuan peralihan dan penutup.[17]

Kementerian Pertahanan memiliki tanggung jawab penuh dalam menghadapi kasus kebocoran data, sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Berdasarkan UU PDP, kementerian sebagai pengendali data pribadi wajib menjamin keamanan data, mencegah akses ilegal, serta segera memberitahukan kepada pemilik data dan otoritas terkait jika terjadi kebocoran. Tanggung jawab ini mencakup langkah penanganan insiden, perbaikan sistem keamanan, evaluasi internal, serta kerja sama dengan lembaga seperti BSSN. Kegagalan dalam memenuhi kewajiban ini dapat menimbulkan sanksi

[16] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Tahun 2022 Nomor 183.
[17] Rosa Aqilah, Deli Waryenti, Pipi Susanti, Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Jurnal Ilmiah Kutei, Vol. 23, No 2, September 2024, https://doi.org/10.33369/jik.v23i2.34476

administratif dan menurunkan kepercayaan publik, karena kebocoran data di sektor pertahanan bukan hanya pelanggaran hukum, tetapi juga ancaman terhadap keamanan nasional.

KESIMPULAN

Tanggung jawab Kementerian Pertahanan dalam menghadapi kasus kebocoran data berlandaskan pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sebagai pengendali data, Kementerian Pertahanan memiliki kewajiban hukum untuk memastikan keamanan data pribadi melalui langkah-langkah preventif, korektif, dan normatif. Secara preventif, Kementerian Pertahanan wajib membangun sistem keamanan siber yang kuat dengan menerapkan enkripsi, klasifikasi data, pembatasan akses, serta membentuk tim khusus yang mampu mendeteksi dan menangani potensi kebocoran sejak dini. Secara korektif, Kementerian Pertahanan berkewajiban melakukan pemulihan sistem, menelusuri penyebab kebocoran, dan memberikan pemberitahuan kepada subjek data maupun otoritas terkait sebagai bentuk akuntabilitas. Sementara secara normatif, Kementerian Pertahanan harus mematuhi prinsip kepastian hukum, perlindungan hak subjek data, serta menerima sanksi administratif apabila terbukti lalai dalam menjalankan kewajibannya. Dengan pelaksanaan tanggung jawab tersebut secara konsisten, Kementerian Pertahanan tidak hanya memenuhi amanat UU PDP, tetapi juga memperkuat perlindungan data pribadi, menjaga kepercayaan publik, dan memastikan stabilitas pertahanan serta kedaulatan negara tetap terjamin.

REFERENSI

Jimly Asshiddiqie, Hukum Tata Negara dan Pilar-Pilar Demokrasi (Jakarta: Konstitusi Press, 2015), hlm. 218.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 200.

Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Aidul Fitriciada Azhari, Hukum dan Kebijakan Keamanan Nasional di Indonesia (Yogyakarta: FH UII Press, 2019), hlm. 144.

Jimly Asshiddiqie, Pengantar Ilmu Hukum Tata Negara (Jakarta: Rajawali Pers, 2010), hlm. 98.

Heru Susetyo, "Keamanan Siber dan Perlindungan Data dalam Perspektif Hukum Nasional," Jurnal Hukum dan Pembangunan, Vol. 50, No. 2 (2020), hlm. 356–370.

Aidul Fitriciada Azhari, Hukum dan Kebijakan Keamanan Nasional di Indonesia, hlm. 150.

Syamsul Ma'arif, "Tanggung Jawab Administrasi Negara dalam Pelayanan Publik Digital," Jurnal Ilmu Hukum Administrasi Negara, Vol. 6, No. 1 (2021), hlm. 55–72.

Rosa Aqilah, Deli Waryenti, Pipi Susanti, Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Jurnal Ilmiah Kutei, Vol. 23, No 2, September 2024, https://doi.org/10.33369/jik.v23i2.34476

Jimly Asshiddiqie, Hukum Tata Negara Darurat, (Jakarta: Rajawali Pers, 2007), hlm. 45.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Tahun 2008 Nomor 58.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Tahun 2022 Nomor 183.

Dedi Rianto Rahadi, "Keamanan Siber dalam Perspektif Nasional," Jurnal Keamanan Nasional, Vol. 5 No. 2, 2019, hlm. 122.

U.S. Department of Defense, Cyber Strategy 2018, Washington D.C.: Pentagon Press, 2018, hlm. 11.

David Leigh dan Luke Harding, WikiLeaks: Inside Julian Assange's War on Secrecy, (London: Guardian Books, 2010), hlm. 75.

Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Lemhannas RI, Ketahanan Nasional: Konsep dan Implementasi, (Jakarta: Lemhannas, 2015), hlm. 87.

Philipus M. Hadjon, Pengantar Hukum Administrasi Indonesia, (Yogyakarta: Gadjah Mada University Press, 2016), hlm. 112.

Bivitri Susanti, "Kekosongan Regulasi Keamanan Siber di Indonesia," Jurnal Konstitusi, Vol. 17 No. 4, 2020, hlm. 890.

Rachmaditya H. A. Pratama, "Tantangan SDM Keamanan Siber di Indonesia," Jurnal Teknologi dan Keamanan Informasi, Vol. 8 No. 1, 2021, hlm. 14.