Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 3 Nomor 4, 2025
DOI: https://doi.org/10.61104/alz.v3i4.1605

Perlindungan Hukum Data Personel Militer Dalam Era Teknologi Informasi di Lingkungan TNI AD

I Putu Arya Wibawa[1], Rokhmat[2], Nani Tulak[3]
Sekolah Tinggi Hukum Militer (AHM -PTHM)[1,2,3]
Email Korespondensi: aryaputu146@gmail.com, rokhmat@sthm.ac.id, nany_tulak@yahoo.com

Article received: 04 Juni 2025, Review process: 23 Juni 2025
Article Accepted: 25 Juli 2025, Article published: 11 Agustus 2025

ABSTRACT

The rapid development of information technology has increased the risk of threats to military personnel data, including cyber warfare, hacking, and internal data misuse, which may endanger national sovereignty. This study aims to analyze the legal protection of military personnel data within the Indonesian Army, identify weaknesses in the existing legal framework, and formulate strategies to strengthen data protection in the digital era. The research method used is a normative juridical approach with descriptive and prescriptive specifications through the examination of laws, literature, and relevant legal documents. The results indicate that existing regulations, such as Law Number 27 of 2022 and Law Number 19 of 2016, have not fully addressed the specific needs of the military sector, which requires a high level of confidentiality. The implication is the necessity to establish sector-specific regulations, strengthen internal policies, modernize cybersecurity infrastructure, and enhance the human resource capacity of the Indonesian Army to ensure the protection of soldiers' privacy rights and maintain military cyber resilience.

Keywords: *Legal Protection, Military Personnel Data, Indonesian Army, Cybersecurity*

ABSTRAK

Perkembangan teknologi informasi yang pesat telah meningkatkan risiko ancaman terhadap data personel militer, termasuk serangan *cyber war*, peretasan, dan penyalahgunaan data internal, yang berpotensi mengancam kedaulatan negara. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap data personel militer di lingkungan TNI Angkatan Darat, mengidentifikasi kelemahan kerangka hukum yang ada, serta merumuskan strategi penguatan perlindungan data di era digital. Metode yang digunakan adalah yuridis normatif dengan spesifikasi deskriptif dan preskriptif melalui kajian peraturan perundang-undangan, literatur, dan dokumen hukum terkait. Hasil penelitian menunjukkan bahwa regulasi yang ada, seperti Undang-Undang Nomor 27 Tahun 2022 dan Undang-Undang Nomor 19 Tahun 2016, belum sepenuhnya mengakomodasi kebutuhan khusus sektor militer yang memiliki tingkat kerahasiaan tinggi. Implikasinya, diperlukan pembentukan regulasi sektoral yang spesifik, penguatan kebijakan internal, modernisasi infrastruktur keamanan siber, dan peningkatan kapasitas sumber daya manusia TNI AD untuk memastikan perlindungan hak privasi prajurit dan menjaga ketahanan siber militer.

Kata Kunci: *Perlindungan Hukum, Data Personel Militer, TNI AD, Keamanan Sibe*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) pada era digital telah mengubah secara signifikan cara masyarakat mengakses, mengelola, dan menyebarkan informasi. Ketergantungan yang semakin tinggi terhadap TIK membuka peluang bagi peningkatan efisiensi di berbagai sektor, namun juga menghadirkan tantangan serius dalam perlindungan data pribadi. Dalam ranah pertahanan dan keamanan negara, kerahasiaan data personel militer menjadi aspek yang sangat krusial, karena kebocoran atau penyalahgunaannya berpotensi mengancam stabilitas nasional. Data personel militer mencakup informasi yang sangat sensitif, mulai dari identitas, penugasan, hingga rincian strategis yang apabila jatuh ke pihak yang tidak berwenang dapat membahayakan keamanan negara.

Perlindungan data pribadi merupakan bagian integral dari hak privasi yang diakui dalam hukum, yang memberikan kendali kepada individu untuk menentukan akses dan penggunaan informasi miliknya. Di Indonesia, payung hukum mengenai perlindungan data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta sejumlah regulasi lain seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Meskipun demikian, regulasi tersebut belum secara komprehensif mengatur perlindungan data pada sektor militer, sehingga menciptakan celah hukum yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.

TNI Angkatan Darat (TNI AD) sebagai komponen utama pertahanan negara memiliki tanggung jawab besar untuk menjaga kedaulatan dan melindungi bangsa dari berbagai bentuk ancaman, baik dari luar maupun dalam negeri. Kemajuan teknologi informasi telah meningkatkan risiko serangan siber, termasuk ancaman seperti *malware*, *phishing*, dan perang siber (*cyber war*), yang secara khusus menargetkan data personel militer. Serangan-serangan ini tidak hanya berdampak pada individu prajurit, tetapi juga dapat mengganggu integritas dan efektivitas sistem pertahanan negara. Oleh sebab itu, TNI AD memerlukan strategi komprehensif yang menggabungkan kebijakan, teknologi, dan peningkatan kapasitas sumber daya manusia untuk melindungi data tersebut.

Kebijakan pengamanan data di lingkungan TNI AD perlu mempertimbangkan modernisasi infrastruktur teknologi informasi, peningkatan kesadaran keamanan siber di kalangan personel, serta penguatan regulasi internal yang mengatur tata kelola data. Perlindungan yang efektif tidak cukup hanya mengandalkan aspek teknis, tetapi juga harus didukung oleh kepastian hukum yang jelas. Hal ini penting mengingat ancaman kebocoran data dapat berasal dari faktor eksternal maupun internal, termasuk potensi penyalahgunaan oleh pihak yang memiliki akses terhadap data tersebut.

Urgensi pembahasan ini semakin mengemuka ketika melihat masih terbatasnya aturan khusus yang mengatur perlindungan data personel militer secara detail. Ketiadaan regulasi yang spesifik menimbulkan risiko lemahnya penegakan hukum terhadap pelanggaran yang melibatkan data sensitif militer.

Oleh karena itu, diperlukan upaya sinkronisasi antara regulasi umum dan aturan sektoral militer, sehingga tercipta kerangka hukum yang mampu mengantisipasi perkembangan modus ancaman di era digital.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap data personel militer di lingkungan TNI AD, menelaah kekuatan dan kelemahan kerangka hukum yang ada, serta mengidentifikasi langkah-langkah strategis yang dapat diambil untuk memperkuat kebijakan keamanan data di era teknologi informasi yang terus berkembang.

METODE

Penelitian ini menggunakan pendekatan yuridis normatif dengan spesifikasi deskriptif dan preskriptif, yang berfokus pada analisis ketentuan hukum positif melalui penelaahan peraturan perundang-undangan, literatur, serta dokumen hukum terkait perlindungan data personel militer di lingkungan TNI AD. Data penelitian diperoleh sepenuhnya dari sumber sekunder yang terdiri atas bahan hukum primer, sekunder, dan tersier, mencakup Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Analisis dilakukan secara kualitatif dengan pendekatan deskriptif-analitis untuk menggambarkan fenomena hukum yang ada, serta preskriptif-analitis untuk merumuskan rekomendasi normatif yang aplikatif. Penarikan kesimpulan menggunakan logika deduktif, dimulai dari prinsip hukum yang bersifat umum menuju penerapan yang lebih spesifik pada perlindungan data personel militer dalam konteks keamanan siber dan teknologi informasi di TNI AD.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Tentara Nasional Indonesia Angkatan Darat (TNI AD) adalah organisasi yang dibangun dari personel yang terdiri dari prajurit atau militer dengan berbagai tingkat keterampilan dan pengetahuan. Keseluruhan personel ini secara terus menerus dikelola dan ditata sesuai dengan kualitas atau kualifikasi mereka untuk mewujudkan organisasi yang profesional dan kuat. Sebagai benteng terakhir bangsa Indonesia dalam menghadapi segala bentuk ancaman, TNI AD berperan penting dalam melindungi data personel militer, yang seringkali menjadi sasaran peretasan oleh pihak-pihak yang tidak bertanggung jawab. Keamanan data ini sangat vital karena berkaitan dengan informasi pribadi yang tidak hanya melibatkan aspek militer, tetapi juga aspek ketahanan negara.

Informasi, yang menjadi media yang sangat menentukan bagi perkembangan ekonomi suatu negara, juga melibatkan data pribadi yang dikelola oleh pemerintah, khususnya data personel militer yang dikelola oleh TNI AD.

Namun, munculnya era digital memberikan ancaman yang lebih besar terhadap privasi individu, khususnya terhadap data personel militer. Kemajuan teknologi mengakibatkan meningkatnya ancaman terhadap privasi, di mana data pribadi atau data personel militer dan keamanan informasi menjadi sangat rentan. Dalam konsep hukum telematika, data merupakan representasi formal suatu konsep atau fakta yang memiliki nilai hukum, namun dalam praktiknya, data sering digunakan tanpa izin yang sah (Assegaf, 2019).

Tujuan utama dari terbentuknya Negara Indonesia adalah untuk memberikan perlindungan bagi seluruh bangsa, termasuk prajurit TNI AD, sebagaimana tercantum dalam Pembukaan Undang-Undang Dasar 1945. Perlindungan terhadap data pribadi, khususnya data personel militer, menjadi salah satu aspek perlindungan negara untuk menciptakan ketahanan nasional melalui jaminan hak asasi manusia bagi setiap orang di Indonesia. Negara bertanggung jawab untuk menjaga, memajukan, dan memenuhi hak asasi manusia bagi setiap warga negara, termasuk prajurit TNI AD yang memiliki hak atas perlindungan data pribadi mereka (Situmorang, 2015).

Jaminan hukum adalah perlindungan terhadap harkat dan martabat serta pengakuan hak asasi manusia sesuai dengan aturan hukum yang berlaku, yang bertujuan untuk melindungi individu dari kesewenang-wenangan. Happy Susanto menyatakan bahwa jaminan hukum dapat bersifat preventif dan represif, baik tertulis maupun tidak tertulis, sesuai dengan aturan hukum yang berlaku untuk menegakkan ketentuan hukum tersebut (Susanto, 2013). Dalam konteks ini, perlindungan hukum data pribadi diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Pasal 26 yang menyatakan bahwa penggunaan seluruh informasi dengan sarana elektronik yang berhubungan dengan data pribadi seseorang harus mendapatkan izin dari pemilik data tersebut. Ini menunjukkan bahwa perlindungan terhadap data pribadi prajurit TNI AD memerlukan pengaturan yang lebih tegas dan jelas.

Namun, meskipun Undang-Undang Nomor 19 Tahun 2016 memberikan dasar hukum mengenai perlindungan data pribadi, undang-undang ini belum cukup sebagai payung hukum yang komprehensif untuk melindungi data pribadi, termasuk data personel militer. Peraturan ini masih memerlukan ketegasan lebih lanjut terkait bagaimana para pelanggar hukum yang menggunakan data pribadi seseorang tanpa izin dapat dijerat hukum. Setiap individu yang haknya dilanggar, seperti yang diatur dalam ayat (1) Pasal 26, memiliki hak untuk mengajukan tuntutan atas kerugian yang timbul akibat pelanggaran tersebut (Suryani, 2017).

Selain itu, perlu ada undang-undang khusus yang mengatur tentang perlindungan data pribadi, termasuk data personel militer. Undang-undang ini harus memuat ketentuan tentang perbuatan yang dilarang, seperti melarang perolehan atau pengumpulan data pribadi yang bukan miliknya demi keuntungan pribadi yang tidak sah (Purnama, 2020). Di antaranya adalah larangan untuk menyebarkan data pribadi tanpa izin, larangan untuk mempergunakan data pribadi secara tidak sah, dan larangan melakukan pemalsuan data pribadi demi kepentingan pribadi atau pihak lain.

Teori perlindungan hukum sangat dibutuhkan dalam konteks ini, karena perlindungan data pribadi, khususnya data personel militer, merupakan hak asasi manusia yang wajib diberikan perlindungan sesuai dengan aturan hukum yang berlaku. Namun, undang-undang yang ada saat ini belum hadir untuk memberikan perlindungan hukum yang maksimal terhadap data personel militer. Oleh karena itu, upaya hukum yang lebih konkret dan pengaturan pasal yang lebih spesifik tentang perlindungan data pribadi prajurit TNI AD harus segera disusun untuk menghindari penyalahgunaan dan pelanggaran yang dapat merugikan negara dan individu terkait.

Pengertian perlindungan dalam ilmu hukum adalah suatu bentuk pelayanan yang wajib dilaksanakan oleh aparat penegak hukum atau aparat keamanan untuk memberikan rasa aman, baik fisik maupun mental, kepada korban dan sanksi terhadap ancaman yang ada. Perlindungan hukum merupakan gambaran dari berjalannya fungsi hukum untuk mewujudkan tujuan hukum, yaitu keadilan, kemanfaatan, dan kepastian hukum. Perlindungan hukum ini dapat bersifat preventif (pencegahan) maupun represif (pemaksaan), yang sesuai dengan aturan hukum yang berlaku (Hadjon, 2014).

Saat ini, regulasi yang digunakan sebagai dasar hukum untuk menangani kejahatan terkait teknologi informasi dan transaksi elektronik (ITE) adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dengan adanya Undang-Undang ITE ini, diharapkan dapat melindungi masyarakat pengguna teknologi informasi di Indonesia, mengingat jumlah pengguna internet yang semakin meningkat dari tahun ke tahun. Walaupun penggunaan internet memberikan kemudahan bagi manusia, hal ini juga membuka peluang bagi pihak-pihak tertentu untuk melakukan tindak pidana melalui media online. Fenomena cybercrime yang berkembang dengan pesat dan tidak mengenal batas teritorial ini harus diwaspadai karena kejahatan ini berbeda dengan kejahatan lainnya (Nugroho, 2019).

Menurut Richard Clark, serangan kejahatan ITE saat ini telah mengalami banyak perubahan dalam hal pola, teknologi, dan strategi yang digunakan. Serangan kejahatan ITE dapat menyerang infrastruktur data personel militer, yang mengimplikasikan bahwa media peperangan telah bergeser dari sistem pertahanan yang dioperasikan oleh manusia menuju sistem yang dapat diakses melalui komputer online yang berhubungan langsung dengan data personel militer (Clark, 2017). Ancaman kejahatan ITE yang ditujukan kepada data personel militer ini telah mengubah konsep doktrin dan strategi militer, yang sebelumnya tidak mengadopsi perang informasi data, menjadi kebutuhan yang sangat mendesak untuk pembentukan cyber defense yang khusus untuk melindungi data personel militer (Aplison, 2020).

Penyesuaian terhadap kemajuan teknologi informasi memerlukan perubahan dalam tiga komponen dasar militer, yaitu strategi, tingkat integrasi, dan pendekatan command and control. Sebagai contoh, Aplison mengusulkan penambahan data center dan perbaikan sistem keamanan data di TNI AD, dengan

penggunaan server virtual untuk memastikan kesiapan data dan menjamin keamanan data personel militer (Aplison, 2020). Hal ini sangat penting mengingat ancaman cyber yang terus berkembang mengikuti kemajuan teknologi global.

Selain itu, *Transfer of Technology* (TOT) menjadi sistem yang sangat diperlukan dalam proses pendelegasian kemampuan, pengetahuan, dan teknologi sistem informasi serta jaringan yang sudah terbangun. Namun, saat ini, proses TOT ke personel TNI AD masih terbatas, dan banyak personel yang belum sepenuhnya terlatih dalam menguasai sistem perangkat aplikasi pengamanan data. Hal ini menyebabkan TNI AD masih bergantung pada pihak luar untuk menangani permasalahan teknis dan pengamanan data, termasuk konfigurasi perangkat data center yang berupa firewall dan hak akses data (Suryadi, 2018).

Mekanisme pengamanan data di data center saat ini belum menjadi fokus utama bagi organisasi TNI AD, terbukti dengan belum adanya organisasi khusus yang menangani masalah cyber secara menyeluruh. Saat ini, pengamanan data hanya mengandalkan peran Pusat Data Sistem Informasi (Pustasisinfo), yang lebih berfokus pada pemeliharaan perangkat data center, bukan pada pengaturan proteksi data yang lebih komprehensif terkait upaya pemblokiran situs atau pengamanan data dari malware (Sutrisno, 2021).

Cyber security, dalam konteks ini, mengacu pada semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan terhadap kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi data personel militer. Elemen-elemen pokok dalam cyber security yang perlu diperhatikan meliputi dokumen security policy, information infrastructure, perimeter defense, network monitoring system, serta human resources dan security awareness (Miller, 2019).

Namun, meskipun ada kemajuan dalam keamanan dunia maya, Hasyim Gautama menyatakan bahwa ada beberapa permasalahan dalam pembangunan cyber security nasional, seperti lemahnya pemahaman penyelenggara negara mengenai ancaman cyber, serta rendahnya kesadaran akan ancaman serangan cyber internasional yang dapat melumpuhkan infrastruktur vital negara (Gautama, 2020). Pada tingkat perlindungan hukum, terdapat dua macam perlindungan hukum yang dapat diterapkan, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya pelanggaran, sedangkan perlindungan hukum represif berfungsi untuk memberikan sanksi setelah terjadinya pelanggaran, seperti denda atau penjara (Hadjon, 2014).

Beberapa kasus pelanggaran data terhadap personel militer yang terjadi menunjukkan bahwa terkoneksi dengan internet secara masif membuka peluang bagi peretasan data penting. Contohnya adalah peretasan data Badan Intelijen Strategis TNI yang dilakukan oleh pihak yang tidak bertanggung jawab, dan data situs Kostrad yang dibobol oleh kelompok yang mengatasnamakan Indian Cyber Mafia. Meskipun situs Kostrad dapat segera ditangani, insiden ini menegaskan pentingnya perlindungan yang lebih ketat terhadap data personel militer (Kurniawan, 2021).

Pembahasan

Perlindungan data pribadi, khususnya data personel militer, menjadi isu yang semakin relevan seiring dengan perkembangan teknologi informasi yang pesat. Dalam konteks ini, dua teori utama yang dapat dikaitkan adalah teori kepastian hukum dan teori perlindungan hukum. Kedua teori ini saling melengkapi dalam memberikan dasar hukum bagi perlindungan data personel militer di Indonesia, khususnya dalam lingkungan TNI AD.

Teori kepastian hukum, menurut Hans Kelsen, menekankan bahwa hukum harus dapat memberikan kepastian kepada semua pihak yang terlibat. Dalam hal ini, hukum harus jelas dan dapat diprediksi dampaknya bagi setiap tindakan hukum yang dilakukan oleh individu atau badan hukum. Dalam konteks perlindungan data pribadi, kepastian hukum sangat dibutuhkan agar setiap individu, termasuk prajurit TNI AD, dapat memahami hak-hak mereka terkait pengelolaan dan penggunaan data pribadi mereka. Kepastian hukum dalam hal ini berfungsi untuk memastikan bahwa setiap pelanggaran terhadap data pribadi akan mendapat konsekuensi hukum yang jelas, dan setiap individu yang menggunakan atau memanipulasi data pribadi tanpa izin dapat dikenakan sanksi yang setimpal. Hal ini sejalan dengan pendapat Hadjon (2014) yang menyatakan bahwa hukum yang baik adalah hukum yang dapat memberikan kepastian kepada masyarakat, dan ini penting untuk menciptakan ketertiban sosial yang teratur.

Kepastian hukum juga mengacu pada adanya aturan yang tegas dan terstruktur dalam mengatur perlindungan data pribadi, baik melalui Undang-Undang Perlindungan Data Pribadi maupun peraturan lainnya. Dalam hal ini, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, meskipun sudah memberikan dasar hukum bagi perlindungan data pribadi, masih memiliki kelemahan dalam hal penegakan hukum terhadap pelanggaran yang melibatkan data personel militer. Kepastian hukum yang lebih mendalam dan khusus terkait dengan data personel militer sangat dibutuhkan agar regulasi yang ada dapat diimplementasikan dengan lebih efektif, memberikan rasa aman kepada prajurit TNI AD, dan menjaga kerahasiaan serta integritas data mereka (Hadjon, 2014).

Teori perlindungan hukum, di sisi lain, berfokus pada upaya melindungi hak-hak individu atau kelompok dari pelanggaran yang dilakukan oleh pihak lain, baik oleh negara maupun individu lain. Perlindungan hukum dalam konteks ini dapat bersifat preventif maupun represif. Teori ini menekankan pentingnya memberikan perlindungan terhadap hak-hak asasi manusia, termasuk hak atas data pribadi, yang dapat menjadi sasaran tindak pidana siber (cybercrime). Dalam konteks TNI AD, teori perlindungan hukum dapat diartikan sebagai upaya untuk melindungi data personel militer yang sangat sensitif. Data tersebut memiliki nilai strategis yang tinggi dan merupakan bagian dari hak privasi setiap individu, yang wajib dilindungi oleh negara.

Perlindungan hukum dalam bentuk preventif berfungsi untuk mencegah penyalahgunaan atau kebocoran data, misalnya dengan membatasi akses terhadap data pribadi hanya kepada pihak yang berwenang dan dengan menggunakan sistem

pengamanan yang ketat. Sedangkan perlindungan hukum represif akan mengatur pemberian sanksi terhadap pelaku yang melanggar hak privasi dan menyalahgunakan data pribadi personel militer. Seperti yang dijelaskan oleh Hadjon (2014), perlindungan hukum berfungsi untuk memberikan rasa aman kepada individu dengan memberikan pengakuan dan perlindungan terhadap hak-hak mereka sesuai dengan peraturan yang berlaku.

Teori perlindungan hukum ini menjadi sangat penting dalam konteks perkembangan ancaman kejahatan siber, yang semakin canggih dan dapat menyasar data-data sensitif milik personel militer. Oleh karena itu, perlindungan hukum yang efektif harus mencakup langkah-langkah preventif, seperti pembuatan kebijakan keamanan data yang lebih ketat, serta langkah-langkah represif yang memberikan sanksi yang tegas bagi pelanggar. Hal ini sesuai dengan prinsip dasar perlindungan hukum yang dijelaskan oleh Philipus M. Hadjon, yaitu bahwa perlindungan hukum berfungsi untuk memberikan rasa aman kepada individu dengan memberikan pengakuan dan perlindungan terhadap hak-hak mereka sesuai dengan peraturan yang berlaku (Hadjon, 2014).

Dalam kaitannya dengan perlindungan data personel militer di TNI AD, penerapan kedua teori ini sangat relevan. Kepastian hukum menjadi dasar bagi prajurit TNI AD untuk mengetahui hak mereka terkait pengelolaan data pribadi mereka dan untuk merasa aman bahwa data mereka tidak akan disalahgunakan. Perlindungan hukum berfungsi sebagai mekanisme yang menjamin hak privasi prajurit TNI AD untuk dilindungi dari ancaman peretasan atau penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab.

Namun, dalam praktiknya, masih terdapat celah dalam sistem hukum yang mengatur perlindungan data pribadi prajurit TNI AD, terutama terkait dengan ketidakjelasan atau ketidaklengkapan dalam peraturan yang ada. Sebagai contoh, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik memang memberikan dasar hukum untuk perlindungan data pribadi, namun belum sepenuhnya mencakup perlindungan data sensitif, seperti data personel militer, yang memiliki tingkat kerahasiaan yang sangat tinggi. Oleh karena itu, diperlukan penguatan dalam bentuk regulasi yang lebih spesifik yang dapat memberikan kepastian hukum dan perlindungan hukum yang lebih baik bagi data personel militer di TNI AD.

Kepastian hukum dan perlindungan hukum memainkan peran yang sangat penting dalam mengatur dan melindungi data pribadi, khususnya data personel militer di TNI AD. Dalam menghadapi ancaman kejahatan ITE yang semakin canggih, penerapan kedua teori ini harus diimplementasikan dalam kebijakan yang lebih jelas dan tegas. Kepastian hukum akan memberikan dasar yang kuat untuk penegakan hak privasi prajurit, sementara perlindungan hukum akan memberikan upaya yang komprehensif untuk melindungi data pribadi mereka dari ancaman cybercrime. Oleh karena itu, untuk memastikan keberhasilan perlindungan data personel militer, penting bagi TNI AD dan pemerintah untuk mengembangkan sistem hukum yang lebih terstruktur dan adaptif terhadap perkembangan teknologi.

SIMPULAN

Perlindungan data personel militer di lingkungan TNI AD merupakan aspek strategis yang menuntut sinergi antara kepastian hukum, perlindungan hukum, dan modernisasi sistem keamanan siber guna mengantisipasi ancaman di era digital. Meskipun Indonesia telah memiliki regulasi umum seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, kerangka hukum yang berlaku belum sepenuhnya mengakomodasi kebutuhan khusus sektor militer yang memiliki tingkat kerahasiaan dan sensitivitas tinggi. Celah regulasi ini berdampak pada belum optimalnya penegakan hukum, khususnya dalam menghadapi modus kejahatan siber yang semakin kompleks seperti *cyber war*, peretasan, dan penyalahgunaan data internal. Oleh karena itu, diperlukan pembentukan regulasi sektoral yang spesifik, penguatan kebijakan internal, serta peningkatan kapasitas sumber daya manusia TNI AD dalam pengelolaan dan pengamanan data. Implementasi langkah-langkah tersebut akan memastikan perlindungan hak privasi prajurit, memperkuat ketahanan siber militer, serta menjaga kedaulatan dan keamanan negara di tengah dinamika ancaman teknologi informasi yang terus berkembang.

DAFTAR RUJUKAN

Arikunto, S. (2013). *Prosedur Penelitian: Suatu Pendekatan Praktik*. Rineka Cipta.

Assegaf, N. (2019). *Hukum Perlindungan Data Pribadi di Era Digital*. Pustaka Pelajar.

Ciptaningrum, P. (2011). *Metode Penelitian Hukum*. Refika Aditama.

Hadjon, P. M. (2014). *Perlindungan Hukum bagi Rakyat di Indonesia*. Gramedia.

Indonesia. (1999). *Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi*.

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

Marzuki, P. M. (2008). *Penelitian Hukum*. Prenada Media.

Mertokusumo, S. (2009). *Penelitian Hukum*. Penerbit Liberty.

Peraturan Kepala Staf Angkatan Darat Nomor 596/IX/2021 tentang Petunjuk Teknis Prosedur Keamanan Teknologi Informasi.

Purnama, S. (2020). *Hukum Teknologi dan Perlindungan Data Pribadi*. RajaGrafindo Persada.

Salim, H. (2014). *Perlindungan Hukum Terhadap Data Pribadi*. Rajawali Pers.

Situmorang, R. (2015). *Perlindungan Hak Asasi Manusia di Indonesia*. Rajawali Pers.

Sudikno, M. (2010). *Metode Penelitian Hukum*. RajaGrafindo Persada.

Suryani, R. (2017). *Penerapan Hukum Perlindungan Data Pribadi di Indonesia*. Laksbang Mediatama.

Susanto, H. (2013). *Jaminan Hukum Perlindungan Data Pribadi*. Refika Aditama.

Sutrisno, E. (2010). *Metode Penelitian Hukum dan Peraturan Perundang-undangan*. Pustaka Pelajar.