

ABSTRAK

Pusat Data Nasional Kementerian Komunikasi dan Digital mengalami peretasan data pada tahun 2024 yang menyebabkan kebocoran data, hal ini berdampak pada keamanan data dan informasi publik di Indonesia. Kejadian ini merupakan peringatan bagi pemerintah untuk dapat memitigasi hal serupa agar tidak terjadi dikemudian hari. Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap data dan informasi di Pusat data Nasional serta mengkaji strategi kelembagaan di Indonesia dalam perlindungan data nasional di masa mendatang. Pendekatan yang digunakan dalam penelitian pendekatan peraturan perundang-undangan, guna pendekatan konseptual dan pendekatan kasus.

Peraturan perundang-undangan di Indonesia sudah mengatur mengenai perlindungan data, tercantum pada Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pemerintah sendiri telah mengeluarkan kebijakan terkait perlindungan data di Indonesia yang tertuang pada Peraturan Presiden Nomor 39 Tahun 2019 Tentang Satu Data Indonesia serta membentuk Badan Siber dan Sandi Negara sebagai lembaga yang mengoordinasikan kemana siber di Indonesia. Selain dari peraturan perundang-undangan tersebut, peneliti melihat bahwa adanya kelemahan pada fasilitas dan sumber daya manusia, seperti standar keamanan yang belum optimal dan masih ditemukan serangan-serangan siber yang berasal dari luar.

Hasil penelitian menunjukkan bahwa, strategi pemerintah Indonesia dalam perlindungan data nasional untuk membentuk lembaga pengawas yang bertugas untuk mengawasi pengelolaan data dan informasi nasional sesuai dengan yang diamanatkan oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi salah satu langkah untuk memitigasi dan meminimalisir adanya serangan siber yang masuk ke Indonesia. Maka, diperlukan kolaborasi antar kelembagaan dan diadakannya lembaga pengawas perlindungan data untuk mengisi kelemahan diatas agar pengelolaan keamanan data dapat lebih optimal dan berkelanjutan.

Kata Kunci: Keamanan Siber, Peretasan Data, Perlindungan Hukum, Pusat Data Nasional.

ABSTRACT

The Ministry of Communication and Digital's National Data Center experienced a data breach in 2024, resulting in a data leak. This impacted the security of public data and information in Indonesia. This incident served as a warning to the government to mitigate similar incidents to prevent future recurrences. This study aims to analyze the legal protection of data and information at the National Data Center and examine Indonesia's institutional strategies for national data protection in the future. The approach used in this research is a legislative approach, using both a conceptual and case-based approach.

Indonesian laws and regulations already regulate data protection, as outlined in Law Number 1 of 2024 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection. The government has issued policies related to data protection in Indonesia, outlined in Presidential Regulation Number 39 of 2019 concerning One Data Indonesia, and established the National Cyber and Crypto Agency as an agency to coordinate cyber security in Indonesia. In addition to these laws and regulations, researchers observed weaknesses in facilities and human resources, such as suboptimal security standards and the continued presence of cyberattacks originating from abroad.

The research findings indicate that the Indonesian government's national data protection strategy, which involves establishing a supervisory agency tasked with overseeing the management of national data and information, as mandated by Law Number 27 of 2022 concerning Personal Data Protection, is one step in mitigating and minimizing cyberattacks entering Indonesia. Therefore, inter-institutional collaboration and the establishment of a data protection supervisory agency are needed to address these weaknesses, ensuring more optimal and sustainable data security management.

Keywords: *Cyber Security, Data Hacking, Legal Protection, National Data Center.*