ABSTRAK

Perkembangan teknologi digital yang pesat telah meningkatkan potensi terjadinya kejahatan siber, khususnya dalam bentuk kebocoran data elektronik yang berdampak luas terhadap keamanan dan privasi masyarakat. Salah satu kasus yang menonjol adalah kebocoran data Pusat Data Nasional (PDN) Kominfo pada tahun 2024 yang disebabkan oleh serangan ransomware dan mengganggu berbagai layanan publik. Penelitian ini bertujuan untuk menganalisis pola kejahatan siber dalam kasus tersebut, mengkaji bentuk pertanggungjawaban pidana terhadap pelaku, serta mengevaluasi efektivitas penerapan sanksi pidana dan sistem pengawasan pemerintah terhadap keamanan digital nasional. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan deskriptif-analitis yang menggunakan data sekunder berupa peraturan perundang-undangan, literatur hukum, dan hasil penelitian terdahulu. Hasil penelitian menunjukkan bahwa pola kejahatan siber dalam kasus PDN 2024 bersifat terstruktur dan sistematis, dengan memanfaatkan kelemahan sistem, kesalahan konfigurasi, serta faktor kelalaian sumber daya manusia. Pertanggungjawaban pidana terhadap pelaku secara normatif telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta Kitab Undang-Undang Hukum Pidana (KUHP), baik terhadap individu maupun korporasi. Namun, implementasinya masih menghadapi berbagai kendala, seperti kompleksitas pembuktian digital, karakter kejahatan lintas negara, serta belum optimalnya pengaturan mengenai tanggung jawab pidana korporasi. Selain itu, efektivitas penerapan sanksi pidana dan sistem pengawasan pemerintah terhadap sistem digital nasional dinilai belum maksimal. Kelemahan terlihat pada aspek koordinasi antar lembaga, keterbatasan sumber daya dan teknologi, serta pendekatan pengawasan yang masih bersifat reaktif. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas aparat penegak hukum, serta pengembangan sistem pengawasan yang lebih komprehensif dan preventif guna meningkatkan keamanan siber nasional.

Kata kunci: kejahatan siber, kebocoran data, pertanggungjawaban pidana, Pusat Data Nasional, keamanan siber

ABSTRACT

The rapid development of digital technology has increased the potential for cybercrime, particularly in the form of electronic data breaches that have significant impacts on public security and privacy. One prominent case is the 2024 data breach of Indonesia's National Data Center (Pusat Data Nasional/PDN), which was caused by a ransomware attack and disrupted various public services. This study aims to analyze the patterns of cybercrime in the case, examine the forms of criminal liability imposed on the perpetrators, and evaluate the effectiveness of criminal sanctions and government supervision systems over national digital security. This research employs a normative legal method with a descriptive-analytical approach, utilizing secondary data such as statutory regulations, legal literature, and previous research findings. The results indicate that the cybercrime pattern in the 2024 PDN case was structured and systematic, involving the exploitation of system vulnerabilities, configuration errors, and human negligence. Criminal liability for the perpetrators is normatively regulated under the Law on Electronic Information and Transactions (EIT Law), the Personal Data Protection Law (PDP Law), and the Indonesian Criminal Code (KUHP), applicable to both individuals and corporations. However, its implementation faces several challenges, including the complexity of digital evidence, the transnational nature of cybercrime, and the lack of clarity regarding corporate criminal liability. Furthermore, the effectiveness of criminal sanctions and government supervision of national digital systems remains suboptimal. Weaknesses are evident in inter-agency coordination, limited technical resources, and a predominantly reactive oversight approach. Therefore, strengthening regulations, enhancing the capacity of law enforcement agencies, and developing more comprehensive and preventive supervisory mechanisms are necessary to improve national cybersecurity.

Keywords: cybercrime, data breach, criminal liability, National Data Center, cybersecurity