

ABSTRAK

Kejahatan siber menjadi isu global yang memerlukan perhatian serius dalam konteks hukum internasional. Studi ini menganalisis kasus peretasan Pusat Data Nasional (PDN) di Indonesia untuk merumuskan dua masalah utama: apakah peretasan tersebut dapat dikategorikan sebagai kejahatan internasional dan bagaimana proses penuntutannya, serta siapa yang dapat digugat jika terjadi pelanggaran. Melalui pendekatan analisis hukum, penelitian ini mengkaji kerangka regulasi internasional, termasuk Konvensi Budapest tentang Kejahatan Siber, serta praktik penegakan hukum di tingkat nasional. Hasil penelitian menunjukkan bahwa peretasan PDN dapat diklasifikasikan sebagai kejahatan lintas batas bukan termasuk dalam kejahatan internasional karena tidak memenuhi unsur Pasal 5 Statuta Roma 1998. Selain itu, proses penuntutan dapat melibatkan berbagai pihak, termasuk negara yang terkena dampak, penyedia layanan, dan pelaku kejahatan itu sendiri. Penelitian ini merekomendasikan perlunya penguatan kerjasama internasional dalam penegakan hukum dan penyusunan regulasi yang lebih efektif untuk menangani kejahatan siber di era digital.

Kata kunci: hukum internasional, kejahatan siber , peretasan, Pusat Data Nasional.

ABSTRACT

Cybercrime is a global issue that requires serious attention in the context of international law. This study analyzes the case of the hacking of the National Data Center (PDN) in Indonesia to formulate two main issues: whether the hacking can be categorized as an international crime and how it can be prosecuted, as well as who can be sued in the event of a violation. Through a legal analysis approach, this research examines the international regulatory framework, including the Budapest Convention on Cybercrime, as well as law enforcement practices at the national level. The results show that hacking of NDPs can be classified as a cross-border crime rather than an international crime as it does not fulfill the elements of Article 5 of the Rome Statute 1998. In addition, the prosecution process can involve various parties, including the affected country, the service provider, and the perpetrator of the crime itself. This study recommends the need for strengthening international cooperation in law enforcement and drafting more effective regulations to deal with cybercrime in the digital era.

Keywords: *cybercrime, hacking, international law, National Data Center.*