ABSTRAK

Penelitian ini bertujuan untuk menganalisis upaya penanggulangan tindak pidana *cybercrime* yang menyerang industri perbankan di Indonesia berdasarkan perspektif peraturan perundang-undangan. Fokus utama dari penelitian ini ialah mengidentifikasi kelemahan regulasi yang ada serta mendorong formulasi kebijakan hukum yang lebih tepat guna dalam menghadapi ancaman serangan siber yang semakin kompleks. Permasalahan dalam penelitian ini dirumuskan ke dalam dua pokok persoalan, yakni: 1. Bagaimana pengaturan penanggulangan *cybercrime* pada industri perbankan berdasarkan perspektif peraturan perundang-undangan Indonesia? dan 2. Bagaimana kebijakan hukum dalam mereformulasi rumusan Pasal 33 Undang-Undang ITE yang berkaitan dengan penanggulangan *cybercrime* pada industri perbankan? Penelitian ini menggunakan metode yuridis-normatif dengan menggunakan pendekatan perundang-undangan dan pendekatan konseptual.Hasil penelitian menunjukkan bahwa meskipun telah terdapat sejumlah regulasi, seperti Undang-Undang ITE, Undang-Undang Perlindungan Data Pribadi, dan POJK Nomor 22 Tahun 2023, pengaturan yang ada belum sepenuhnya menjawab tantangan *cybercrime* di sektor perbankan. Khususnya, ketidakjelasan rumusan dalam Pasal 33 Undang-Undang ITE yang menimbulkan multitafsir dan kesulitan pembuktian unsur *mens rea* pelaku tindak pidana *cybercrime*. Hal tersebut dapat mengakibatkan timbulnya perbedaan interpretasi dalam penerapan hukum yang dapat mempengaruhi konsistensi dalam proses penegakan hukum. Hasil penelitian ini yaitu *pertama, cybercrime* tidak diatur secara spesifik dalam undang-undang perbankan, namun karena berada di ruang siber maka ketentuan hukum dapat merujuk pada undang-undang ITE khususnya dalam Pasal 33, namun masih menimbulkan multitafsir terhadap norma tersebut. *Kedua,* kebijakan hukum dalam mereformulasi Pasal 33 Undang-Undang ITE meliputi: 1) perluasan definisi; 2) metode dalam pembuktian; 3) penjelasan ulang sanksi pidana dan mekanisme perampasan asset; 4) perlindungan data pribadi korban. Penelitian ini menyarankan kepada Pemerintah dan DPR untuk mereformulasi Pasal 33 Undang-Undang ITE agar dapat membatasi penafsiran frasa “mengganggu sistem elektronik”. Kepada industri perbankan juga direkomendasikan untuk meningkatkan sistem siber dengan bekerja sama dengan penyedia layanan keamanan siber eksternal. Kepada aparat penegak hukum agar dapat meningkatkan kapasitasnya dalam menghadapi *cybercrime* yang semakin kompleks.

Kata Kunci: *Cybercrime; Penanggulangan Tindak Pidana; Perbankan.*

ABSTRACT

This research aims to analyze efforts to overcome cybercrime that attacks the banking industry in Indonesia based on legislation perspective. The main focus of this research is to identify the weaknesses of existing regulations and encourage the formulation of legal policies that are more appropriate in facing the increasingly complex threat of cyber attacks. The problems in this research are: 1. How is the regulation of cybercrime countermeasures in the banking industry based on the perspective of Indonesian legislation? and 2. How is legal policy in reformulating the formulation of Article 33 of the ITE Law relating to cybercrime countermeasures in the banking industry? This research uses a juridical-normative method using a statutory and a conceptual approach. The results show that although there have been a number of regulations, such as the ITE Law, the Personal Data Protection Law, and POJK 22/2023, the existing arrangements have'nt fully answered the challenges of cybercrime in the banking sector. In particular, the vagueness of the formulation in Article 33 ITE Law which creates multiple interpretations and difficulties in proving the mens rea element of the perpetrator of cybercrime. The results of this study are first, cybercrime is not specifically regulated in banking law, but because it is in cyberspace, legal provisions can refer to the ITE law, especially in Article 33, but it still causes multiple interpretations of the norm. Second, legal policies in reformulating Article 33 of the ITE Law include: 1) expansion of definitions; 2) methods of proof; 3) re-explanation of criminal sanctions and asset forfeiture mechanisms; 4) protection of victims' personal data. This research suggests that the Government and Parliament reformulate Article 33 of the ITE Law to limit the interpretation of the phrase "disrupting electronic systems". It is also recommended for the banking industry to improve its cyber system by working with external cybersecurity service providers. To law enforcement officials to increase their capacity in dealing with increasingly complex cybercrime.

Keywords:*Banking; Criminal Countermeasures; Cybercrime.*