ABSTRAK

Penelitian ini bertujuan untuk melihat bagaimana pihak perbankan dapat bertanggungjawab secara pidana akibat tindak kejahatan *sim swap.* Perkembangan teknologi memberikan kemudahan kegiatan dalam sektor perbankan. Sayangnya, kejahatan terbaru pun kian berkembang yang merambah hingga ke tahap kejahatan siber. Penelitian ini juga bertujuan untuk mengkaji apakah peraturan yang berlaku saat ini cukup untuk melindungi nasabah dari kejahatan siber. Berlandaskan UU ITE pada Pasal 15 yang mewajibkan pihak penyelenggara sistem elektronik bertanggung jawab dalam membuat sistem keamanan yang andal. Namun, dalam Pasal tersebut tidak menjelaskan dengan rinci bagaimana standar sistem keamanan elektronik yang baik. Pada penelitian ini penulis menggunakan metode yuridis-normatif dengan pendekatan perundang-undangan dan pendekatan kasus. Hasil menunjukan bahwa kurangnya ketegasan terkait peraturan sistem elektronik oleh penyelenggara sistem elektronik membuat pihak penyelenggara, dalam konteks ini adalah pihak perbankan tidak membuat sistem elektronik yang benar-benar aman. Akibatnya kejahatan-kejahatan siber seperti phishing dan *sim swap* terus berkembang. Tidak adanya sanksi pidana bagi perbankan juga memberikan celah untuk tidak mendorong setiap penyelenggara sistem elektronik serius dalam membuat sistem yang aman. Sehingga berdampak pada kurangnya perlindungan hukum terhadap nasabah. Padahal berdasarkan doktrin-doktrin yang ada, pihak perbankan juga dapat dijatuhi sanksi pidana, seperti dalam kasus *sim swap.* Sayangnya kekurangan regulasi dengan sanksi pidana membuat ketidak jelasan dan ketidak pastian hukum bagi nasabah.

Kata Kunci: *Pertanggungjawaban Pidana, Sim Swap, Perbankan*

ABSTRACT

This research aims to see how banks can be criminally responsible for *sim swap crimes.* Technological developments provide ease of activities in the banking sector. Unfortunately, the latest crimes are also growing which penetrate to the stage of cybercrime. This study also aims to examine whether the current regulations are sufficient to protect customers from cybercrime. Based on the ITE Law in article 15 which requires the electronic system operator to be responsible in creating a reliable security system. However, the article does not explain in detail how a good electronic security system standards are. In this study, the author uses a juridical-normative method with a legislative approach and a case approach. The results show that the lack of firmness regarding electronic system regulations by electronic system operators makes the operators, in this context, the banks do not make electronic systems that are truly safe. As a result, cybercrimes such as phishing and *sim swaps* continue to grow. The absence of criminal sanctions for banks also provides a loophole not to encourage every electronic system operator to be serious about making a safe system. So that it has an impact on the lack of legal protection for customers. In fact, based on existing doctrines, banks can also be subject to criminal sanctions, such as in the case of *sim swaps.* Unfortunately, the lack of regulations with criminal sanctions creates ambiguity and legal uncertainty for customers.

Keywords: *Criminal Liability, Sim Swap, Banking*