ABSTRAK

Perkembangan pesat teknologi informasi dan komunikasi telah mendorong transformasi layanan perbankan, terutama melalui mobile banking. Namun, kemudahan ini juga menghadirkan risiko ataupun kerugian, penyadapan data nasabah (sniffing) merupakan salah satu yang dapat mengakibatkan pencurian informasi pribadi dan finansial. Penelitian ini bertujuan untuk menganalisis secara yuridis praktik sniffing yang terjadi pada pengguna mobile banking di Indonesia.

Penelitian ini bertujuan untuk menganalisis secara yuridis praktik penyadapan data nasabah (sniffing) yang terjadi pada pengguna mobile banking di Indonesia.. Metode penelitian yang digunakan adalah pendekatan normatif, yang meliputi analisis peraturan perundang-undangan yang relevan, studi kasus mengenai insiden yang terjadi, serta wawancara dengan praktisi hukum dan ahli di bidang teknologi informasi.

Hasil analisis menunjukkan bahwa meskipun Indonesia memiliki regulasi seperti Undang-Undang Perlindungan Data Pribadi dan ketentuan dari Otoritas Jasa Keuangan (OJK) yang bertujuan untuk melindungi data nasabah, implementasi dan penegakan hukum terhadap praktik sniffing masih mengalami banyak kendala. Praktik ini seringkali sulit untuk dilacak dan diidentifikasi, sehingga nasabah menjadi rentan terhadap pencurian data pribadi dan informasi finansial. Selain itu, kurangnya kesadaran akan pentingnya keamanan siber di kalangan pengguna mobile banking memperparah situasi ini.

Kata kunci: Penyadapan Data, Mobile Banking.

ABSTRACT

The rapid development of information and communication technology has driven the transformation of banking services, particularly through mobile banking. However, this convenience also presents security risks, one of which is data snooping (sniffing) that can lead to the theft of personal and financial information. This study aims to legally analyze the sniffing practices occurring among mobile banking users in Indonesia.

This study aims to legally analyze the data snooping (sniffing) practices occurring among mobile banking users in Indonesia. The research methodology employs a normative approach, which includes the analysis of relevant regulations, case studies of incidents, and interviews with legal practitioners and experts in the field of information technology.

The analysis results indicate that although Indonesia has regulations such as the Personal Data Protection Law and guidelines from the Financial Services Authority (OJK) aimed at protecting customer data, the implementation and enforcement of laws against sniffing practices still face many challenges. These practices are often difficult to trace and identify, leaving customers vulnerable to the theft of personal and financial data. Furthermore, the lack of awareness regarding the importance of cybersecurity among mobile banking users exacerbates this situation.

Keywords : Data Snooping, Mobile Banking.