ABSTRAK

PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA NASABAH BANK MANDIRI DARI KEJAHATAN *PHISING* (Studi Pada PT Bank Mandiri (Persero) Tbk. Jakarta Selatan)

Oleh
FITRIA WULANDARI

Phising adalah kejahatan siber yang dilakukan dengan cara menyamar sebagai pihak resmi bank melalui email, SMS, situs web palsu, atau aplikasi palsu untuk mencuri data pribadi nasabah seperti *username*, *password*, PIN, dan informasi kartu kredit. Sebagai salah satu bank terbesar di Indonesia, Bank Mandiri memiliki tanggung jawab fundamental melindungi keamanan data nasabah dari kejahatan *phising*. Permasalahan dalam penelitian ini mencakup bagaimanakah peran Bank Mandiri dalam melindungi keamanan data nasabah dari kejahatan *phising* dan bagaimanakah perlindungan hukum yang diberikan terhadap keamanan data nasabah Bank Mandiri dari kejahatan *phising* berdasarkan peraturan perundang-undangan yang berlaku di Indonesia.

Jenis penelitian yang digunakan adalah penelitian normatif-empiris dengan tipe penelitian hukum deskriptif. Pendekatan masalah penelitian adalah pendekatan normatif-empiris. Sumber data yaitu data primer dan sekunder. Metode pengumpulan data dilakukan dengan cara studi pustaka dan wawancara. Penulis mengambil penelitian dengan mewawancarai dua narasumber dari Bank Mandiri, diantaranya *IT Security Lead-Subsidiary IT Security* dan *First Senior Manager-UIUX Designer*. Metode pengolahan data yaitu pemeriksaan data, penandaan data, dan sistematika data. Analisis data yang digunakan adalah kualitatif.

Hasil penelitian menunjukkan Bank Mandiri memiliki tanggung jawab melindungi data nasabah dari *phising* melalui tiga peran: peran normatif berdasarkan kepatuhan regulasi perbankan dan perlindungan data pribadi; peran ideal dengan menerapkan teknologi keamanan seperti *firewall*, sistem deteksi dan pencegahan intrusi (IDS/IPS), SSL/TLS, MFA, AI/*machine learning*, dan Token atau OTP; serta peran faktual melalui koordinasi aktif dengan aparat berbagai lembaga serta penetapan kebijakan internal seperti SOP deteksi dan respons insiden *phising*, kebijakan keamanan informasi, prosedur verifikasi berlapis, pembentukan unit CSIRT, pelatihan berkala bagi karyawan, program edukasi, kampanye literasi digital, evaluasi risiko berkala, pembentukan tim khusus kepatuhan data. Perlindungan hukum dilakukan secara preventif melalui implementasi teknologi keamanan dan program edukasi nasabah sesuai UU Perbankan, UU Perlindungan Konsumen, UU PDP, serta secara represif melalui pelaporan, investigasi, penuntutan pelaku, dan pemulihan hak korban dengan koordinasi OJK, BSSN, dan Direktorat Siber berdasarkan UU ITE dan KUHP.

Kata Kunci: Bank Mandiri, Keamanan Data Nasabah, Perlindungan Hukum, *Phising*.

ABSTRACT

LEGAL PROTECTION FOR THE SECURITY OF BANK MANDIRI CUSTOMERS DATA FROM PHISING CRIMES
(Study at PT Bank Mandiri (Persero) Tbk. South Jakarta)

By
FITRIA WULANDARI

Phishing is a cybercrime committed by impersonating an official bank through email, SMS, fake websites, or fake applications to steal customers' personal data such as usernames, passwords, PINs, and credit card information. As one of the largest banks in Indonesia, PT Bank Mandiri has a fundamental responsibility to protect customer data security from phishing crimes. The issues addressed in this study include the role of Bank Mandiri in protecting customer data security from phishing crimes and the legal protections provided for the security of Bank Mandiri customers' data against phishing crimes based on applicable laws and regulations in Indonesia.

The type of research used is normative-empirical research with a descriptive legal research type. The research problem approach is a normative-empirical approach. The data source is secondary data. The data collection method was conducted through literature study and interviews. The data processing methods were data examination, data marking, and data systematics. The author conducted the study by interviewing two sources from Bank Mandiri, including the IT Security Lead-Subsidiary IT Security and the First Senior Manager-UI/UX Design. The data processing methods included data examination, data coding, and data organization. The data analysis employed was qualitative.

The study finds that Bank Mandiri has a responsibility to protect customer data from phishing through three roles: a normative role based on compliance with banking regulations and personal data protection; an ideal role by implementing security technologies such as firewalls, intrusion detection and prevention systems (IDS/IPS), SSL/TLS, MFA, AI/machine learning, and tokens or OTP; and a factual role through active coordination with officials from various agencies and the establishment of internal policies such as SOPs for phishing incident detection and response, information security policies, multi-layered verification procedures, the formation of a CSIRT unit, periodic employee training, educational programs, digital literacy campaigns, periodic risk assessments, and the formation of a dedicated data compliance team. Legal protection is carried out preventively through the implementation of security technologies and customer education programs in accordance with the Banking Law, Consumer Protection Law, and PDP Law, , as well as repressively through reporting, investigation, prosecution of perpetrators, and restoration of victims' rights in coordination with the OJK, BSSN, and the Cyber Directorate based on the ITE Law and the Criminal Code.

Keywords: Bank Mandiri, Customer Data Security, Legal Protection, Phising.