

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi dan komunikasi telah mengikuti perkembangan perbankan Indonesia saat ini. *Electronic Banking* adalah sistem layanan yang ditawarkan oleh institusi keuangan seperti bank untuk memungkinkan sejumlah transaksi keuangan dilakukan langsung oleh nasabah melalui perangkat *mobile* seperti ponsel.¹ Dengan adanya *Electronic Banking*, sangat membantu masalah pelayanan. Sebuah bank dapat menyediakan layanan *Electronic Banking*, yang akan membuat layanan menjadi cepat dan efisien, dan dapat diakses di mana pun dan kapan pun. Hal ini sangat memudahkan nasabah serta membuat mereka tidak perlu mengantri di depan teller untuk mengirim uang. Hal ini yang menarik minat pelanggan untuk membuka rekening di bank tersebut. Khususnya bagi para pebisnis berskala besar yang membutuhkan sistem yang hemat biaya, mudah, aman, terintegrasi, dan handal tanpa terkendala dengan ruang dan waktu. Tidak diragukan lagi, *Electronic Banking* ini dapat menjadi alat yang berguna bagi nasabah yang tinggal di kota-kota besar dengan lalu lintas yang padat.²

Bagi nasabah, *Electronic Banking* memberikan kemudahan dan kecepatan dalam melakukan transaksi perbankan. Selain itu, bank dapat menggunakan *Electronic Banking* sebagai alternatif untuk membangun infrastruktur yang lebih mahal daripada membuka ATM (Anjungan Tunai mandiri). Meskipun

¹ Dewi, Ni Made. "Perlindungan Hukum Terhadap Nasabah *Mobile Banking* Dalam Transaksi Perbankan", *Jurnal Komunikasi Hukum (JKH)* Vol. 7, No. 1, (Februari, 2021), hlm. 83.

² *Ibid*, hlm. 84.

menggunakan *internet banking* memiliki banyak keuntungan, masih ada beberapa kelemahan dan risiko yang muncul. Selain itu, *Electronic Banking* juga membuka peluang kejahatan yang terjadi saat menggunakannya.³ Beberapa risiko yang muncul terkait dengan menggunakan layanan ini yaitu risiko strategi, operasional, dan reputasi, serta adanya berbagai risiko kerusakan atau kegagalan sistem internet *banking*.⁴ Selain itu, risiko yang lain yaitu banyaknya pelanggaran hukum yang berkaitan dengan data pribadi di internet dan risiko finansial yang dihadapi oleh nasabah bank sebagai akibat dari tindakan para pelaku kejahatan tersebut. Akibatnya, industri perbankan harus mengembangkan fitur keamanan yang dapat mempertahankan kepercayaan masyarakat.⁵

Salah satu kewajiban bank adalah menjamin kerahasiaan data pribadi nasabah. Namun, seiring munculnya layanan *Electronic Banking* dalam dunia perbankan, semakin sulit untuk menjamin kerahasiaan data pribadi nasabah tersebut. Data pribadi didefinisikan sebagai setiap informasi yang dapat diidentifikasi atau diakses oleh orang lain. Informasi pribadi didefinisikan sebagai setiap informasi yang berhubungan dengan transaksi *online*.⁶

Berikut beberapa kasus penyalahgunaan *Electronic Banking* yang sering terjadi yaitu:

³ Adelia, F., "Peran Otoritas Jasa Keuangan Atas Perlindungan Data Pribadi Konsumen *Fintech Lending*", *Dinamika*, Vol. 27, No. 21, (Januari, 2022), hlm. 4

⁴ Resa, R., 2014, *Aspek Hukum Transaksi Elektronik*, Jakarta, Graha Ilmu, hlm. 65

⁵ Resa Raditio, *Op.Cit*, hlm. 67

⁶ Assafa Endeshaw, 2007, *Hukum E-Commerce dan Internet, Dengan Fokus di Asia Pasifik*, Yogyakarta, Pustaka Pelajar. hlm. 28.

1) *Pharming*

merupakan jenis serangan siber yang digunakan oleh penjahat dengan cara mengalihkan *website* asli yang akan dikunjungi oleh konsumen menjadi *website* palsu yang telah dibuat oleh penjahat tersebut;

2) *Spoofing*

merupakan salah satu pelanggaran *cyber* yang memanfaatkan berbagai media komunikasi untuk melakukan pencurian identitas hingga penyebaran *malware* atau perangkat lunak yang telah dibuat untuk merusak komputer pengguna internet dengan tujuan untuk menyembunyikan identitas dengan menampilkan alamat *e-mail*, nama, atau nomor telepon palsu di komputer Anda;

3) *Phishing*

merupakan tindakan mengumpulkan informasi pribadi secara ilegal. Dengan tujuan untuk mengakses rekening, melakukan penipuan kartu kredit, atau mengarahkan pelanggan untuk melakukan *transfer* ke rekening tertentu dengan hadiah sebagai pemikatnya;

4) *Keylogger*

merupakan program yang memiliki kemampuan untuk menghafal tombol *keyboard* yang digunakan tanpa diketahui oleh pengguna.

5) *Sniffing*

merupakan pekerjaan menyadap paket data jaringan.⁷

⁷ Han Revanda Putra dan Nurhadi, 2023, *Kenali 5 Modus Kejahatan Mobile Banking dan Cara Menghindarinya*, <https://tekno.tempo.co/read/1726592/kenali-5-modus-kejahatan-mobile-banking-dan-cara-menghindarinya>, (diakses pada 02 Oktober 2023, 01:00)

Dilaporkan oleh Kompas.com bahwa terdapat nasabah yang kehilangan dana di tiga bank besar di Indonesia dikarenakan telah dibobol melalui metode yang menggunakan *Mobile Banking*. Modus kejahatan ini diperkirakan mengakibatkan kerugian sebesar Rp 130 miliar.⁸

Dilansir oleh detiknews.com bahwa terdapat kasus mengenai pembobolan data dengan cara mengirimkan *file* pdf kepada korban sehingga menyebabkan data-data penting korban termasuk *M-Banking* dapat didapatkan dan diketahui dengan mudah oleh pelaku. Kejadian ini terjadi pada salah satu warga Malang bernama Irwan Gema pada tanggal 14 Juli 2023 yang mengaku telah kehilangan uangnya di Bank sebesar 549 juta setelah ia mengunduh dan membuka *file* aplikasi dengan format pdf yang dikirimkan melalui aplikasi WhatsApp.⁹

Selain dengan cara mengirimkan *file* aplikasi dengan format pdf, detik news melaporkan terdapat kasus yang sekarang ramai terjadi adalah pengiriman undangan pernikahan *online* yang dikirimkan oleh nomor yang tidak dikenal. Cara ini digunakan oleh pelaku untuk membobol data pribadi korban termasuk *M-Banking*. Hal ini terjadi pada salah seorang pengusaha di Malang yang bernama Silvia Yap pada tanggal 7 Juli 2023. Akibat dari kejadian ini, Silvia mengalami kehilangan uang di rekening bank sebesar 1,4 miliar rupiah.¹⁰

⁸ Kompas.com, 2015, *Ini Modus Pembobolan Rekening Nasabah Melalui "e-Banking"*, <https://money.kompas.com/read/2015/04/15/113500326/Ini.Modus.Pembobolan.%20Rekening.Nasabah.Melalui.e-Banking>, (diakses pada 01 Oktober 2023, 21:00)

⁹ Muhammad Aminudin, 2023, *Duit Warga Malang Raib Rp 549 Juta Usai Klik-Buka APK Berkedok PDF di WA*, <https://news.detik.com/berita/d-6823573/duit-warga-malang-raib-rp-549-juta-usai-klik-buka-apk-berkedok-pdf-di-wa>, (diakses pada tanggal 01 Oktober 2023, 21:05)

¹⁰ Tim Detik Jatim, 2023, *Unduh File 'Undangan' di WA, Nasabah Kehilangan Duit Tabungan Rp 1,4 M*, <https://www.detik.com/jateng/berita/d-6810966/unduh-file-undangan-di-wa-nasabah-kehilangan-duit-tabungan-rp-14-m>, (diakses pada 01 Oktober 2023, 21:10)

Berdasarkan kasus-kasus di atas, terbukti bahwa tidak hanya satu orang yang pernah mengalami kejadian pembobolan data dengan cara *Phishing* atau pengelabuan melalui *link* atau aplikasi. Selain itu juga sudah jelas bahwa sistem perbankan nasional belum memperhatikan perlindungan nasabah perbankan dengan baik. Namun, karena pihak nasabah sangat penting dalam dunia perbankan, kehidupan dunia perbankan sangat bergantung pada masyarakat atau nasabah. Namun, belum ada kejelasan yang jelas mengenai perlindungan hukum yang diberikan kepada nasabah bank saat melakukan transaksi *e-banking*.

Pengaturan *Electronic Banking* tentu saja tidak terlepas dari Undang-Undang Perbankan Nomor 7 tahun 1992 beserta Undang-Undang perubahannya yakni Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, Peraturan Bank Indonesia Nomor: 9/15/PBL/2007 Tentang Penerapan Manajemen Resiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum dan juga Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Pada pasal 2 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen menetapkan bahwa perlindungan konsumen harus memenuhi asas keamanan, manfaat, keadilan, keseimbangan, dan keselamatan konsumen. Tujuan dari asas kepastian hukum ini adalah untuk menjamin bahwa barang dan jasa yang dikonsumsi atau digunakan akan aman, menguntungkan, dan adil. Sangat penting bahwa peraturan dibuat untuk melindungi konsumen dari penyimpangan teknologi yang dapat merugikan pengguna teknologi internet. Penyimpangan ini dapat terjadi

karena kelemahan dalam sisi perlindungan karena kemajuan teknologi cenderung lebih cepat dan tidak ada jaminan dari sisi kepastian hukum.

Selain diatur oleh Peraturan Perundang-Undangan diatas, *Electronic banking* diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum, menurut Peraturan Otoritas Jasa Keuangan tersebut, "layanan perbankan digital adalah layanan perbankan elektronik yang dikembangkan dengan mengoptimalkan pemanfaatan data nasabah dalam rangka melayani nasabah secara lebih cepat, mudah dan sesuai dengan kebutuhan serta dapat dilakukan secara mandiri sepenuhnya oleh nasabah, dengan memperhatikan aspek pengamanan."

Otoritas Jasa Keuangan merupakan salah satu lembaga yang melindungi nasabah karena memiliki peran sebagai pengawas dalam sektor perbankan, seperti yang dijelaskan dalam Peraturan Otoritas Jasa Keuangan Nomor: 6/POJK.07/2022 tentang Perlindungan Konsumen Sektor Jasa Keuangan. Dengan adanya PJOK tersebut, diharapkan masyarakat sebagai nasabah bank dapat merasa aman dalam menggunakan jasa dari perbankan di Indonesia ini.

Berdasarkan uraian diatas, dengan ini penulis ingin menelaah lebih dalam mengenai **“PENGAWASAN OTORITAS JASA KEUANGAN TERHADAP PENGAMANAN DATA PRIBADI NASABAH DALAM LAYANAN *DIGITAL BANK*”**.

B. Rumusan Masalah

Berdasarkan Latar Belakang Masalah, maka rumusan masalah adalah:

1. Bagaimana mekanisme pengawasan Otoritas Jasa Keuangan terhadap perlindungan data pribadi nasabah dalam transaksi *Electronic Banking*?
2. Apa upaya yang dapat ditempuh nasabah yang terkena pembobolan data pribadi melalui *phishing*?

C. Tujuan Penelitian

1. Untuk mengetahui bagaimana mekanisme pengawasan yang dilakukan oleh Otoritas Jasa Keuangan dalam hal melindungi data pribadi nasabah dalam transaksi *Electronic Banking*.
2. Untuk mengetahui upaya hukum yang dapat ditempuh oleh nasabah yang terkena pembobolan data pribadi melalui *phishing*.

D. Manfaat Penelitian

1. Manfaat Teoritis

Dalam pembahasan, diharapkan memberikan manfaat sebagai bahan kajian mahasiswa ke arah pengembangan atau kemajuan dibidang ilmu hukum dagang pada umumnya dan khususnya terkait pengawasan OJK terhadap pengamanan data pribadi nasabah dalam layanan digital bank khususnya *Electronic Banking*.

2. Manfaat Praktis

a. Untuk Mahasiswa

Diharapkan hasil penelitian ini dapat memberikan manfaat untuk mahasiswa sebagai bahan untuk pembelajaran dan pencegahan agar tidak terkena pembobolan data dengan cara *phishing*!

b. Untuk Masyarakat

Diharapkan hasil penelitian ini dapat memberikan manfaat untuk masyarakat sebagai bahan edukasi agar terlindungi dari modus kejahatan transaksi *online* berupa *phishing*.

c. Untuk Otoritas Jasa Keuangan

Diharapkan hasil penelitian ini dapat memberikan manfaat untuk pihak Otoritas Jasa Keuangan sebagai pengawas terhadap bank agar memperketat peraturan bagi sistem IT (*Information Technology*) bank dan sebagai bahan evaluasi agar tidak terjadi pembobolan data berupa *phishing* terhadap nasabah bank tersebut.