BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan dan kemajuan teknologi dan komunikasi berupa internet turut membawa dampak buruk berupa penyalahgunaan media internet.[1] Dewasa ini pemanfaatan teknologi informasi dan komunikasi yang kian masif mendorong pemerintah untuk memperkuat sistem hukum terutama yang berkaitan dengan keamanan data pribadi. Pasal 28 D Ayat (1) UUD 1945 mengamanatkan bahwa "Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum."[2]

Saat ini kemajuan teknologi membawa kemudahan sekaligus permasalahan akibat timbulnya kejahatan dunia maya (*cybercrime*). Pemerintah sebagai penyelenggara negara dituntut untuk memberikan jaminan atas perlindungan dan kepastian hukum bagi masyarakat. Sebagaimana yang disampaikan dalam Pasal 26 Huruf (a) Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo PDPSE) yang menyebutkan bahwa "Pemilik Data Pribadi berhak atas kerahasiaan Data Pribadinya."[3]

---

[1] I Gede Arya Utamayasa, *et.al*, "Kriminalisasi Terhadap Perbuatan Memperoleh Data Identitas Diri dengan Menggunakan Teknik *Phising*", Kertha Wicara: Journal Ilmu Hukum Vol. 5, No. 1, Februari 2016, hal. 2.

[2] Pasal 28 D Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

[3] Pasal 26 Huruf (a) Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Maka dari itu, setiap masyarakat tanpa terkecuali mempunyai hak atas keamanan seluruh data dan informasi pribadi sehingga mereka dapat menuntut setiap pihak yang berusaha melanggar privasinya. Selaras dengan perkembangan teknologi, mendorong pemerintah untuk menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Mengingat pentingnya perlindungan data pribadi seiring dengan meningkatanya pemanfaatan teknologi digital, maka konsep privasi digagas untuk melindungi integritas dan martabat pribadi. Adanya perkembangan tekonologi tidak menepis kemungkinan munculnya berbagai pelanggaran dan kejahatan terkait kebocoran data pribadi yang ujungnya bermuara pada aksi penipuan maupun tindakan pornografi. Konsep perlindungan dimaksudkan untuk memberikan batasan bagi setiap individu untuk membagi atau bertukar data pribadi mereka. Sejauh ini perlindungan terhadap data pribadi masih bersifat parsial dan sektoral, sehingga belum dapat memberikan perlindangan secara optimal.[4] Hal inilah yang mendorong pemerintah untuk mengesahkan UU PDP pada 17 Oktober 2022.

Penyalahgunaan data pribadi merupakan bentuk pelanggaran terhadap hak privasi seseorang. Sejauh ini, kejahatan dunia maya terus berkembang di era digitalisasi. Adapun kejahatan dunia maya dapat diartikan secara sempit dan secara luas. Kejahatan dunia maya dalam pengertian sempit merupakan kejahatan terhadap sistem komputer, sedangkan kejahatan dunia maya dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang

[4] Badan Pembinaan Hukum Nasional, "Naskah Akademik RUU Perlindungan Data Pribadi". https://bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf diakses pada 23 Juli 2023, hal. 2-3.

menggunakan sarana komputer.[5] Kejahatan dunia maya tersebut di antaranya *carding*, *skimming*, *hacking*, *cracking*, *phising*, *malware*, *cybersquatting*, pornografi, perjudian *online*, pinjaman *online*, *robot trading*, kejahatan *cryptocurrency*, *transnational crime*, *money laundry, human trafficking*, *underground economy*, dan sebagainya.[6]

Bank menjadi salah satu target utama dalam kejahatan dunia maya (*cybercrime*) dikarenakan lembaga ini berkaitan dengan lalu lintas pembayaran yang memungkinkan adanya arus transaksi setiap harinya. Hal inilah yang menyebabkan lembaga perbankan sangat rentan terhadap kejahatan dunia maya, khususnya dalam kasus penyalahgunaan data pribadi. Ditambah lagi, sistem perbankan mulai beralih dari sistem konvensional ke arah digital. Saat ini, sejumlah bank banyak menawarkan layanan *electronic banking* (*e-banking*) berupa *mobile banking* (*m-banking), internet banking (i-banking), phone banking*, dan sebagainya. Di samping dari kemudahan yang didapatkan nasabah bank, kemajuan teknologi seperti ini semakin meningkatkan peluang terhadap kejahatan dunia maya. Berdasarkan Laporan Bank Umum Terintegrasi periode Mei 2023 yang dilakukan oleh Lembaga Penjamin Simpanan (LPS) terdapat 516,52 juta rekening

[5] Mohammad Yusuf D.M., *et.al*, "Kejahatan *Phising* dalam Dunia *Cyber Crime* dan Sistem Hukum di Indonesia", Jurnal Pendidikan dan Konseling Vol. 4 No. 5 (2022), hal. 8019.

[6] Sugeng, *Hukum Telematika Indonesia* (Jakarta: Prenadamedia Group, 2020), hal. 85.

dari total keseluruhan rekening simpanan bank umum dan dari jumlah tersebut, 97,9% merupakan rekening tabungan.[7]

Peralihan pola transaksi ke arah digital semakin berkembang sehingga menyebabkan meningkatnya volume transaksi pada platform digital, salah satunya melalui *m-banking*. Layanan *m-banking*, seperti BRI-mo, Livin *by* Mandiri, Kopra *by* Mandiri, m-BCA, dan layanan *m-banking* lainnya terus mengalami peningkatan jumlah pengguna sepanjang tahun 2023. Menurut laporan yang disampaikan oleh Direktur Digital dan Teknologi Informasi BRI, Arga M. Nugraha tercatat bahwa hingga akhir Maret 2023 BRI-mo berhasil membukukan sebanyak 225 juta transaksi finansial serta menunjukkan peningkatan jumlah pengguna yang kini tembus di angka 26,3 juta pengguna.[8] Di samping itu, Direktur Utama Bank Mandiri Darmawan Junaidi menyampaikan bahwa transaksi digital Bank Mandiri juga terus mengalami peningkatan, dimana Livin *by* Mandiri telah melayani lebih dari 1,64 miliar transaksi finansial dengan total 22 juta pengguna.[9]

Layanan perbankan tidak pernah lepas kaitannya dengan penggunaan data pribadi. Berdasarkan Pasal 1 Angka 1 Surat Edaran Otoritas Jasa Keuangan Nomor

---

[7] Lembaga Penjamin Simpanan, "Distribusi Simpanan Bank Umum Mei 2023". https://lps.go.id/web/guest/data-distribusi-simpanan/-/asset_publisher/eN56/content/data-distribusi-simpanan-mei-2023?_101_INSTANCE_eN56_redirect=https%3A%2F%2Flps.go.id%2Fweb%2Fguest%2Fdata-distribusi-simpanan%3Fp_p_id%3D101_INSTANCE_eN56%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1 diakses pada 20 Juli 2023.

[8] Abdurrahman Faruq, "Transaksi Melonjak 154,63%, BRImo Semakin Menjadi Pilihan Masyarakat". https://bri.co.id/test/-/asset_publisher/G3x3P8wG7JRn/content/transaksi-melonjak-154-63-brimo-semakin-menjadi-pilihan-masyarakat diakses pada 20 Juli 2023.

[9] Mandiri, "Buah Digitalisasi! Keberhasilan Transformasi Bisnis Bank Mandiri Menciptakan *Values* Baru, Mendukung Kinerja 2022 Yang Cemerlang". https://bankmandiri.co.id/web/guest/press-detail?primaryKey=140544139&backUrl=/en/press diakses pada 20 Juli 2023.

14/SEOJK.07/2014 Tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen berbunyi:[10]

> "Data dan/atau informasi pribadi konsumen adalah data dan/atau informasi, yang mencakup sebagai berikut:
> a. perseorangan:
> 1) nama;
> 2) alamat;
> 3) tanggal lahir dan/atau umur;
> 4) nomor telepon; dan/atau
> 5) nama ibu kandung.
> b. korporasi:
> 1) nama;
> 2) alamat;
> 3) nomor telepon;
> 4) susunan direksi dan komisaris termasuk dokumen identitas berupa Kartu Tanda Penduduk/paspor/izin tinggal; dan/atau
> 5) susunan pemegang saham."

Melihat bahwa data pribadi selalu dibutuhkan dalam layanan perbankan membawa keresahan bagi nasabah bank mengingat banyaknya kasus penyalahgunaan data pribadi yang berujung pada kerugian finansial. Hal ini disebabkan karena tingginya penggunaan platform digital yang tidak diimbangi dengan kesadaran akan keamanan data pribadi. Celah inilah yang dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk memperoleh keuntungan dari informasi yang didapatkan. Tentunya tindakan seperti ini termasuk dalam perbuatan melawan hukum, dimana pelaku berusaha memperoleh keuntungan dengan menimbulkan kerugian bagi pihak lain.

Salah satu kejahatan dunia maya yang sering terjadi adalah kejahatan *phising*. *Phising* adalah modus yang digunakan untuk mendapatkan informasi dan

[10] Pasal 1 Angka 1 Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOJK.07/2014 Tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen.

data seseorang dengan teknik pengelabuan. *Phising* biasanya dilakukan dengan mengelabui korban untuk mengeklik sebuah tautan palsu yang berpotensi pada terbukanya informasi dan data pribadi pengguna, seperti *username*, *password*, detail kartu kredit, dan sebagainya. Umumnya tautan yang dilampirkan dibuat semirip mungkin seperti tautan asli dari sebuah instansi. Tautan tersebut kemudian disisipkan dalam sebuah narasi yang disebarkan melalui email, pesan, atau situs web. Ketika korban mengakses tautan tersebut, *malware* akan diunduh ke perangkat korban untuk menyerang sistem perlindungan data dan terjadilah kebocoran informasi pribadi dan pencurian aset. *Phising* memiliki ciri-ciri khusus, seperti:[11]

1. Perintah untuk mengisi data sensitif. *Phising* merupakan tindakan manipulatif yang mendorong korban untuk memberikan data-data pribadi yang sifatnya sensitif, contohnya kata sandi, PIN, OTP, nomor kartu, dan sebagainya.
2. Menggunakan identitas palsu. Pelaku *phising* atau *phisher* biasanya menggunakan identitas palsu untuk menjebak korbannya, misalnya dengan mengatasnamakan pihak bank atau lembaga resmi lainnya.
3. Memberi tautan atau file palsu. *Phisher* juga selalu menyertakan tautan atau file palsu sehingga pelaku dapat mengakses data pribadi korban yang telah terunduh dalam perangkat korban.

[11] Bank Central Asia, "Awas Modus *Phising* yang Bisa Membahayakan Akun Perbankan". https://www.bca.co.id/id/informasi/awas-modus/2022/03/02/04/12/awas-modus-phisingyang-bisa-membahayakan-akun-perbankan diakses pada 23 Juli 2022.

4. Pesan yang bersifat ajakan bahkan ancaman. Pesan yang disampaikan *phisher* umumnya menuntut korban untuk mengambil keputusan secara cepat sehingga korban dengan spontan mengambil keputusan tersebut.
5. Ditargetkan pada korban tertentu. Pelaku umumnya telah menargetkan korbannya.

Adapun beberapa modus *phising* dalam sektor perbankan dilakukan dengan cara-cara berikut.[12]

1. Informasi perubahan tarif transfer bank yang dilakukan dengan memberikan informasi palsu dan meminta korban untuk mengisi data pribadi, seperti *User ID,* PIN, *One Time Password* (OTP), *Password*, *Card Verification Value* (CVV), *Card Verification Code* (CVC), dan m-Token.
2. Layanan konsumen palsu yang mengatasnamakan bank yang dilakukan dengan mengarahkan korban ke *website* palsu untuk mencuri data dan informasi pribadi.
3. Tawaran menjadi nasabah prioritas yang dilakukan dengan menawarkan promo *upgrade* dengan berbagai hadiah menarik, lalu pelaku meminta data pribadi korban.
4. Tawaran menjadi agen laku pandai, kemudian pelaku meminta korban mentransfer uang untuk mendapatkan mesin *Electronic Data Capture* (EDC).

[12] Lilis Ekayani dan Hardianto Djanggih, "Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (*Phising*) Di Lingkungan Perbankan", Journal of Lex Philosophy Vol. 4, No. 1, Juni 2023, hal. 25.

*Indonesia Anti-Phising Data Exchang*e (IDADX) menyebutkan setidaknya terdapat 26.675 kasus *phising* yang terjadi pada kuartal I 2023. Kasus ini meningkat secara signifikan dibandingkan tahun sebelumnya yang tercatat sebanyak 6.106 kasus.[13] Adapun berdasarkan data yang diperoleh IDADX, media sosial mencatat 45% dari total kasus, disusul dengan lembaga keuangan sebesar 31%, *e-commerce* atau retail sebesar 20%, *spam* sebesar 2%, ISP sebesar 1%, dan aset kripto sebesar 1%. Laporan tersebut menunjukkan bahwa lembaga keuangan termasuk sebagai sasaran utama kejahatan *phising*.

Kejahatan *phising* dapat mengancam keamanan data pribadi dan hak privasi setiap individu. Salah satu faktor penyebab tingginya kasus kejahatan *phising* adalah karena minimnya pengetahuan dan kesadaran masyarakat akan dampak yang ditimbulkan dari kebocoran data (*data breach*). Seperti halnya satu adagium yang menyebutkan *crime is product of society itself*, artinya masyarakat sendirilah yang menghasilkan kejahatan.[14] Seiring dengan tingginya intelektualitas manusia, maka akan menghasilkan kejahatan yang semakin canggih pula. Oleh karena itu, kesadaran terhadap keamanan data perlu dibangun sebagai landasan bahwa setiap orang berhak memperoleh perlindungan hukum sebagaimana yang telah diundang-undangkan.

1.2 Rumusan Masalah

1. Bagaimana pengaturan mengenai modus kejahatan *phising* di Indonesia?

---

[13] *Indonesia Anti-Phishing Data Exchange*, Laporan Aktivitas *Phising Domain*.ID Periode Q1 2023". https://idadx.id/files/Q1_2023.pdf diakses pada 23 Juli 2023, hal. 2.

[14] Kabib Nawawi, *et.al*, "*Cyber Crime* dalam Bentuk *Phising* Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik", Journal of Criminal Law Vol. 1, No. 2 (2020), hal. 72.

2. Bagaimana bentuk perlindungan hukum bagi nasabah bank yang menjadi korban kejahatan *phising*?

1.3 Tujuan Penelitian

1. Untuk menganalisis pengaturan mengenai modus kejahatan *phising* di Indonesia.
2. Untuk menganalisis bentuk perlindungan hukum bagi nasabah bank yang menjadi korban kejahatan *phising*.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Manfaat teoritis dari penelitian ini adalah dapat menjadi tambahan sumbangan pemikiran terkait perlindungan hukum bagi nasabah bank terhadap ancaman penyalahgunaan data pribadi dalam modus kejahatan *phising*.

1.4.2 Manfaat Praktis

Manfaat praktis dari penelitian ini adalah diharapkan dapat menjadi tambahan acuan bagi masyarakat yang berpotensi menjadi korban kejahatan *phising*.

1.5 Sistematika Penulisan

Sistematika penulisan proposal dibagi dalam beberapa bab, yakni sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan landasan teori berupa pengertian dan definisi dari para ahli yang dikutip melalui sumber-sumber yang berkaitan dengan topik penelitian serta landasan konseptual berupa penjelasan mengenai berbagai regulasi yang berkaitan dengan topik penelitian.

BAB III METODE PENELITIAN

Bab ini berisikan jenis penelitian, jenis data, cara perolehan data, jenis pendekatan, dan analisis data.

BAB IV HASIL PENELITIAN DAN ANALISIS

Bab ini berisikan deskripsi dan pembahasan terkait data yang diperoleh dengan menggunakan metode penelitian yang telah ditentukan untuk memperoleh jawaban atas pertanyaan-pertanyaan penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dan saran atas pembahasan yang telah diuraikan pada bab-bab sebelumnya.