BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi, merupakan suatu perkembangan dari era globalisasi. Pada era globalisasi ini muncul keinginan masyarakat untuk berkembang, baik perkembangan dalam bidang politik, ekonomi maupun sosial budaya. Perkembangan di dunia teknologi diimbangi juga dengan kasus pencurian data nasabah. Kejahatan perbankan lahir dan tumbuh seiring dengan kemajuan ilmu pengetahuan dan teknologi yang dicapai oleh manusia. Kejahatan tersebut termasuk dalam kategori kejahatan kelas "*elite*". Dikatakan "*elite*", karena tidak semua orang dapat melakukannya. Kejahatan kelas "*elite*" ini tidak membutuhkan tenaga fisik yang banyak. Kemampuan pikir merupakan faktor yang penting untuk mencapai hasil yang berlipat ganda.

Menurut Johanes Gunawan, pertanggungjawaban bank terhadap nasabah selaku konsumen dapat dilakukan pada saat sebelum terjadinya transaksi (*prepurchase*) atau sesudah terjadinya transaksi (*post purchase*)[1]. Misalkan Pada jenis transaksi *card present*, pelaku mendapatkan informasi korbannya dengan teknik *skimming* menggunakan *card skimmer*. *Card skimmer* adalah alat yang mampu merekam data/informasi. Karena ukuran alatnya cukup kecil, biasanya pelaku menyembunyikan alat tersebut dibawah meja kasir. Pelaku mengambil data-data korbannya dengan cara menggesekkan kartu pada *card skimmer* sesaat setelah dilakukan transaksi pada mesin *electronic data capture* (EDC)[2].

[1] Johanes Gunawan, *Hukum Perlindungan Konsumen*, Bandung: Universitas Katolik Parahyangan, 1999, Hlm. 3.

[2] Annisa Aprilia Wd, Paramita Prananingtyas, Budiharto, "Tanggung jawab Bank Penerbit (*Card Issuer*) Terhadap Kerugian Nasabah Kartu Kredit Akibat Pencurian Data (*Carding*) Dalam Kegiatan Transaksi", *Diponegoro Law Journal*, Vol 6. No. 2, 2017, Hlm.9.

Semakin maju dan berkembang peradaban umat manusia, akan semakin mewarnai bentuk dan corak kejahatan yang akan muncul ke permukaan. Oleh karena itu setelah komputer merajelela di berbagai belahan dunia, maka orangpun lalu disibukkan dan direpotkan pula dengan efek samping yang ditimbulkannya yaitu berupa kejahatan komputer (*cybercrime*) salah satunya *phising*. *Phising* adalah kegiatan memancing pada pengguna teknologi dengan sebuah link agar mengisi data diri seperti *username*, kata sandi pada halaman *web,* kejahatan ini hanya memanfaatkan kelemahan dan kebanyakan menyerang pengguna aplikasi *online banking*[3].

Phising ini juga biasanya dilakukan melalui media-media sosial yang terhubung ke jaringan internet seperti melalui *e-mail*/*sms* dan *website*. Modus perbuatannya yang melalui *e-mail*/*sms* mengirimkan pesan seperti: Pertama, saya membutuhkan pertolongan anda sekarang, maksud pesannya adalah seseorang mengaku sebagai salah satu kerabat atau teman dan mengatakan membutuhkan pertolongan karena sedang dalam masalah. Kedua, selamat, Anda menang, maksud pesannya adalah seperti anda telah memenangkan lotre dan harus mengklaimnya, tetapi biasanya selalu ada pancingan didalamnya, seperti memasukkan data pribadi ke sebuah *website* tertentu atau yang sudah biasa digunakan oleh nasabah untuk mendapatkan hadiah tersebut.

Adapun perkara atau kasus yang pernah terjadi dalam *Cyber Crime Phising*, yaitu pencurian *User ID* seseorang dengan berkedok penipuan *link* untuk melakukan kejahatan yang berupa ujaran kebencian dan penyebaran berita palsu atau *hoax*, pelaku melakukan hal tersebut menggunakan *user ID* seseorang untuk memanipulasi publik, dengan begitu publik menyangka hal tersebut adalah tindakan korban, padahal ada seseorang yang merupakan pelaku sebenarnya yang mengontrol *user ID* korban. Dalam hal ini pula menyatakan terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "Dengan sengaja dan tanpa hak mendistribusikan dan membuat dapat diaksesnya Informasi

[3] Sutan Remy Syahdeini, Kejahatan & Tindak Pidana Komputer,Jakarta: Grafiti, 2009, Hlm. 63-64.

Elektronik dan Dokumen Elektronik yang memiliki muatan penghinaan dan pencemaran nama baik", sebagaimana diatur dan diancam pidana dalam Pasal 45 ayat (3)

Kasus *phising* terjadi pada nasabah bank BRI di Padang Provinsi Sumatra Barat. Kasus ini merugikan nasabah Bank BRI mencapai Rp, 1.114 Miliar. Peristiwa tersebut diketahui terjadi pada Rabu 31 Mei 2022 pukul 14.00 WIB. Korban yang sedang berada di rumah mendapatkan pesan *whatsapp* tentang pemberitahuan berupa perubahan biaya *transfer*, kemudian korban dikirimkan berupa formulir dan link oleh pelaku, setelah itu korban klik link dan masuk ke dalam link yang diberikan pelaku tersebut dan mendaftarkan *username*, *password* dan PIN. Setelah mengisi formulir, korban mendapatkan *sms* dari pihak BRI berupa kode OTP dan *link*, kemudian *link* yang diberikan bank BRI disalin dan ditempelkan pada *link* yang diberikan melalui WA sebelumnya. Lanjutnya, korban mendapatkan notifikasi aplikasi BRIMO adanya pembayaran BRIVA atas nama korban senilai Rp300.000 dan adanya *transfer* dari aplikasi BRIMO senilai Rp250.000.000 dan beberapa transaksi lainnya, sehingga korban mengalami kerugian senilai Rp 1,1 miliar lebih.

Kasus lain terjadi di Provinsi Bali yang dialami anggota DPRD Kabupaten Klungkung I Wayan Misna. Dimana Misna terpancing setelah mengklik tautan *link* di *media sosial facebook.* Modus yang dilakukan sedikit berbeda tidak mengisi *form* dari *link*, namun pelaku berpura-pura menjadi *customer service* Bank BPD Bali dan meminta identitas diri dan data *mobile banking* milik korban. Setelah mendapatkan data diri, kemudian pelaku menguras isi rekening korban dengan *mentransfer* sejumlah dana ke rekening tertentu. Kendala yang dihadapi Kepolisian akibat terjaidnya kasus bank *phising* yaitu, Kepolisian kesulitan menghubungi tujuan rekening yang di *transfer*, karena berbeda daerah regional ataupun antar provinsi.

Cybercrime dalam bentuk *phising* saat ini di Indonesia dapat dikenakan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini selain membuat aturan tentang *phising*, Undang-Undang ini juga membuat aturan

terhadap perbuatan-perbuatan kejahatan yang merugikan orang lain yang terjadi didunia maya melalui transaksi elektronik yang dapat diketahui bahwa perkembangan teknologi informasi semakin pesat.

Pemerintah sudah membuat suatu Undang Undang yang mencakup kejahatan di Internet yaitu Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah menjadi Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Sebelum lahirnya UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronika (ITE), maka Polri seharusnya tidak menggunakan pasal-pasal di dalam KUHP. Seperti pasal pencurian, pemalsuan dan penggelapan, hal ini menimbulkan berbagai kesulitan dalam pembuktiannya. Karena karakteristik dari *cybercrime* sebagaimana telah disebutkan di atas yang terjadi secara non fisik.

Apabila dikaitkan kepada perbuatan yang dilarang maka UU ITE sudah melarang perbuatan memperoleh informasi dengan cara apapun sebagaimana yang tertera dalam pasal 30 khususnya pada ayat (2). Ketika pelanggaran itu dilakukan maka dapat dikenakan sanksi pidana berupa pidana penjara maksimal 7 tahun dan denda maksimal Rp 700.000.000,-(tujuh ratus juta rupiah). Hal ini berdasarkan pasal 46 ayat (2) UU ITE yang telah tertulis dengan adanya peraturan ini data pribadi seseorang sudah memiliki payung hukum dan dilindungi oleh hukum. Kewajiban sebagai penyelenggara layanan aplikasi yaitu menjaga kerahasiaan serta keamanan dari informasi elektronik yang dikelolanya. Hal ini sesuai dengan pasal 15 ayat (1) karena apabila penyelenggara aplikasi tidak dapat menjaga data yang dikelolanya dapat dikenakan sanksi administratif sesuai Pasal 84 ayat (1) dan (2) PP No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Penyelenggara layanan aplikasi juga harus mematuhi UU ITE dan juga seluruh perUndang-Undangan terkait yang berlaku di Indonesia hal ini juga dipertegas oleh Surat Edaran dari KOMINFO Nomor 3 Tahun 2016 terkait Penyediaan Layanan Aplikasi dan/atau Konten Melalui Internet.

Tingginya tingkat kejahatan memberikan dampak negatif bagi para nasabah bank. Walaupun sudah diatur dalam undang-undang ITE ini akan tetapi dalam pelaksanaannya undang-undang ini banyak menemui kendala. Kendala

dalam undang-undang ITE ini salah satunya terdapat dalam pembuktian terhadap pelaku, dimana untuk hal pembuktian memerlukan alat bukti informasi dan/atau dokumen elektronik pelaku pencurian di bank melalui bank *phising* biasanya terletak atau disimpan dalam *hard disk*, sehingga pelaku bisa menghapus atau mengganti hardisk komputernya untuk menghilangkan jejak yang dapat menyulitkan proses penindakan. Selain itu, peraturan (*das sein*).

Dalam UU Perlindungan Data Pribadi Juga khususnya di Pasal 20 ayat (1) menjelaskan bahwa pengelola data atau penyelenggara aplikasi wajib mencegah data pribadi yang diakses secara tidak sah. Larangan hal tersebut juga tertera dalam pasal 50 ayat (1) yang berbunyi Setiap Orang dilarang memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian pemilik data pribadi.

Dalam UU ITE belum ada pengaturan yang membahas tentang perlindungan hukum terhadap korban *cybercrime* baik membahas tentang restitusi maupun kompensasi terhadap korban. Pengembalian hak-hak korban hanya diatur dalam undang-undang tentang perlindungan saksi dan korban. Berdasarkan uraian di atas, artikel ini membahas mengenai Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Bank *Phising*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dipaparkan, yang menjadi pokok permasalahan dalam penulisan proposal ini adalah:

1. Bagaimana penindakan hukum pencurian data pribadi nasabah dengan metode bank *phising*?
2. Bagaimana pertanggungjawaban pidana dalam pencurian data nasabah perbankan dengan menggunakan metode bank *phising*?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini terdiri dari tujuan obyektif dan subyektif sebagai berikut:

1. Untuk mengetahui penindakan hukum pencurian data pribadi nasabah dengan metode bank *phising*.

2. Untuk mengetahui pertanggungjawaban pidana dalam pencurian data nasabah perbankan dengan menggunakan metode bank *phising*.

1.4 Kegunaan Penelitian

Adapun kegunaan dalam penelitian ini adalah sebagai berikut:

a. Kegunaan Teoritis

Secara teoritis, penelitian ini mampu memberi kontribusi ilmiah untuk ilmu hukum khususnya dalam pengembangan penegakkan hukum bagi para korban pertanggungjawaban pidana bagi pelaku tindak pidana pencurian data nasabah perbankan dengan metode bank *phising*.

b. Kegunaan Praktis

1) Hasil Penelitian ini diharapkan dapat memberikan manfaat dengan menghasilkan bahan masukan bagi para korban terhadap pengaturan untuk mengurangi ataupun mencegah terjadinya pencurian data nasabah perbankan dalam kasus bank *phising.*
2) Hasil Penelitian ini diharapkan dapat memberikan manfaat dengan menghasilkan bahan masukan pengaturan mengenai penindakan hukum pencurian data pribadi nasabah dengan metode bank *phising*.

1.5 Kerangka Teoritis

1.5.1 Teori Pertanggungjawaban

Menurut Hans Kelsen dalam teorinya tentang tanggung jawab hukum menyatakan bahwa: "seseorang bertanggung jawab secara hukum atas suatu perbuatan tertentu atau bahwa dia memikul tanggung jawab hukum, subyek berarti bahwa dia bertanggung jawab atas suatu sanksi dalam hal perbuatan yang bertentangan. Lebih lanjut Hans Kelsen menyatakan bahwa kegagalan untuk melakukan kehati-hatian yang diharuskan oleh hukum disebut kekhilafan (*negligence*); dan kekhilafan biasanya dipandang sebagai satu jenis lain dari kesalahan (culpa), walaupun tidak sekeras kesalahan yang terpenuhi karena mengantisipasi dan menghendaki, dengan atau tanpa maksud jahat, akibat yang

membahayakan[4]. Hans Kelsen selanjutnya membagi mengenai tanggung jawab terdiri dari:

a. Pertanggungjawaban individu yaitu seorang individu bertanggung jawab terhadap pelanggaran yang dilakukannya sendiri;
b. Pertanggungjawaban kolektif berarti bahwa seorang individu bertanggung jawab atas suatu pelanggaran yang dilakukan oleh orang lain;
c. Pertanggungjawaban berdasarkan kesalahan yang berarti bahwa seorang individu bertanggung jawab atas pelanggaran yang dilakukannya karena sengaja dan diperkirakan dengan tujuan menimbulkan kerugian;
d. Pertanggungjawaban mutlak yang berarti bahwa seorang individu bertanggung jawab atas pelanggaran yang dilakukannya karena tidak sengaja dan tidak diperkirakan [5].

1.5.2 Pengertian Data Pribadi

Menurut Kamus Besar Bahasa Indonesia pengertian data adalah keterangan yang benar dan nyata yang dapat dijadikan dasar kajian.[6] Sedangkan pribadi sendiri memiliki arti manusia sebagai perseorangan (diri manusia atau diri sendiri), dapat disimpulkan bahwa data pribadi merupakan keterangan yang benar dan nyata yang dimiliki oleh manusia sebagai perseorangan. UU ITE tidak memberikan definisi hukum yang jelas tentang data pribadi. Akan tetapi, dilihat dari prespektif penafsiran resmi tentang hak pribadi (*pivacy right*) dalam Pasal 26 ayat (1), maka data pribadi meliputi urusan kehidupan pribadi termasuk (riwayat) komunikasi seseorang dan data tentang seseorang.[7]

---

[4] Hans Kelsen, "*General Theory Of Law And State*" , Teori Umum Hukum Dan Negara, Dasar-Dasar Ilmu Hukum Normatif Sebagai Ilmu Hukum Deskriptif Empirik, Bee Media Indonesia, 2007. Jakarta, Hlm. 81

[5] Ibid

[6] Kbbi. "Pengertian Data". Https://Kbbi.Web.Id/Data Diakses Pada 5 Februari 2023 Pukul 16.00

[7] Daniar Supriyadi, "Data Pribadi Dan Dua Dasar Legalitas Pemanfaatannya". https://www.hukumonline.com/berita/a/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-lt59cb4b3feba88. Diakses 5 Juni 2023

Dalam PP No. 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik, mendefinisikan data pribadi yaitu "data perseorangan tertentu yang disimpan, dirawat, dijaga kebenaran serta dilindungi kerahasiaannya" (Pasal 1 ayat 27). Menurut penjelasan Pasal 1 ayat 1 Data *Protection Act* Inggris tahun 1998 menentukan bahwa:[8]

> "Data adalah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses. Data juga termasuk informasi yang merupakan bagian tertentu dari catatan-catatan kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan."

Peraturan ini menyebutkan bahwa data pribadi dimaksudkan sebagai identitas seseorang yang terang dan jelas yang merupakan penetapan bukti diri terhadapnya yang dipelihara, dijaga kebenarannya dan ditempatkan dengan aman kerahasiannya. Secara umum, definisi data pribadi menurut hukum positif di Indonesia memiliki kesamaan, yaitu data yang melekat pada pribadi seseorang sebagai identitas dan ciri khusus orang tersebut.

Dalam praktiknya istilah data privasi dan data pribadi dipersepsikan sama karena objeknya sama-sama data yang melekat pada pribadi seseorang. Dalam hukum positif di Indonesia yang ada saat ini juga menggunakan istilah data pribadi. Istilah perlindungan data pribadi pertama kali digunakan di Jerman dan Swedia pada tahun 1970-an yang mengatur perlindungan data pribadi melalui Undang-Undang. Alasan dibuatnya perlindungan karena pada waktu itu mulai dipergunakan komputer sebagai alat untuk menyimpan data penduduk, terutama untuk keperluan sensus penduduk. Ternyata dalam prakteknya, telah terjadi banyak pelanggaran yang dilakukan baik oleh Pemerintah maupun pihak

[8] Pasal 1 Ayat (1). Data Protection Act Inggris Tahun 1998

Swasta. Berdasarkan hal itu agar penggunaan data pribadi tidak disalahgunakan maka diperlukan pengaturan.[9]

Definisi mengenai data pribadi telah dimuat di beberapa hukum positif di Indonesia, diantaranya yaitu:

1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan adalah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi dimana data pribadi yang dimaksud yaitu data tentang perorangan yang teridentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik ataupun non elektronik.
2) Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya.
3) Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Menurut PP ini, data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik.
4) Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Dari beberapa penjelasan diatas maka Undang-Undang ini berfungsi untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi. Undang-undang ini diharapkan menjadi payung hukum yang kuat bagi tata kelola dan

[9] S. D. Rosadi, "Perlindungan Pivasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia," *Yustitia* 4, No. 1 (2018). Hlm.89

perlindungan data personal warga Negara dan para penyelenggara Pemerintahan.[10]

Undang-Undang Administrasi Kependudukan mengatur data pribadi digabungkan dengan urusan kependudukan, yang menyebutkan data pribadi penduduk terdiri atas: nomor KK, NIK, tanggal/bulan/tahun lahir, keterangan tentang kecacatan fisik dan/atau mental, NIK ibu kandung, NIK ayah, dan beberapa isi catatan peristiwa penting.

Sedangkan sebelumnya menurut UU Perlindungan Data Pribadi yang merupakan hukum yang dicita-citakan (*Ius Constituendum*), data pribadi sendiri dibagi menjadi dua jenis. pertama, data pribadi yang bersifat umum, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Kedua, data pribadi yang bersifat spesifik, meliputi data dan informasi kesehatan, data biometrik, data genetika, kehidupan/orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan peraturan perUndang-Undangan.

Diterangkan juga dalam Data *Protection Act* Inggris tahun 1998 bahwa data pribadi adalah data yang berhubungan dengan seseorang individu yang hidup yang dapat diidentifikasikan dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh data *controller*. Selain itu data prbadi juga dapat dikaitkan dengan ciri responden contohnya jenis kelamin, umur, nama dan lain-lain.

Menurut Peraturan Menteri Kominfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik menjelaskan, data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Secara umum data pribadi terdiri atas fakta-fakta yang berkaitan dengan individu yang merupakan informasi sangat pribadi bagi semua orang yang bersangkutan ingin menyimpan untuk dirinya sendiri dan/atau membatasi orang lain untuk menyebarkannya kepada pihak lain maupun menyalahgunakannya.

[10] Yuking, "Urgensi Peraturan Perlindungan Data Pribadi Dalam Era Bisnis Fintech." *Jurnal Somasi: Sosial Humaniora Komunikasi.* Vol. 2, No.1 (2021). Hlm. 32

Secara khusus, data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karakteristik masing-masing individu.

Menurut Pasal 1 Ayat (1) Undang-Undang Perlindungan data pribadi memberikan definisi tentang data pribadi yaitu :

> "Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupuntidak langsung melalui sistem elektronik dan/atau nonelektronik"

Data bersifat umum meliputi: nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Data yang bersifat spesifik meliputi :

1) data dan informasi kesehatan;
2) data biometrik;
3) data genetika;
4) kehidupan/orientasi seksual;
5) pandangan politik;
6) catatan kejahatan;
7) data anak;
8) data keuangan pribadi; dan/atau
9) data lainnya sesuai dengan ketentuan peraturan perUndang-Undangan.

Data pribadi menjadi data privasi seseorang yang harus dilindungi dan tidak boleh disalahgunakan. Penyalahgunaan data pribadi merupakan suatu perbuatan melawan hukum. Belakangan ini banyak ditemukan kasus pencurian data pribadi yang kemudian disalahgunakan, seperti kasus yang terjadi pada aplikasi *online shop* Tokopedia, BPJS, Bhineka dan lainnya. Data pribadi pada sistem elektronik diatas dicuri oleh orang yang tidak bertanggung jawab, kemudian diperjualbelikan di *online market place*/ pasar *online*.

1.5.3 Dasar Hukum Perlindungan Data Pribadi

Apabila membahas persoalan dasar hukum perlindungan data pribadi bahwasannya secara umum perlindungan data pribadi sudah terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian diubah menjadi Undang-Undang Nomor 19 Tahun 2016.

Selain itu terdapat juga dalam Undang-Undang Perlindungan Data Pribadi yang saat ini telah resmi disahkan. Perlindungan hukum itu sendiri adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban, perlindungan hukum korban kejahatan sebagai bagian dari perlindungan masyarakat, dapat diwujudkan dalam berbagai bentuk, seperti melalui pemberian restitusi, kompensasi, pelayanan medis, dan bantuan hukum.

Perlindungan hukum yang diberikan kepada subyek hukum ke dalam bentuk perangkat baik yang bersifat preventif maupun yang bersifat represif, baik yang lisan maupun yang tertulis. Dengan kata lain dapat dikatakan bahwa perlindungan hukum sebagai suatu gambaran tersendiri dari fungsi hukum itu sendiri, yang memiliki konsep bahwa hukum memberikan suatu keadilan, ketertiban, kepastian, kemanfaatan dan kedamaian.

Perlindungan Hukum adalah Sebagai kumpulan peraturan atau kaidah yang akan dapat melindungi suatu hal dari hal lainnya. Berkaitan dengan konsumen, berarti hukum memberikan perlindungan terhadap hak-hak pelanggan dari sesuatu yang mengakibatkan tidak terpenuhinya hak-hak tersebut [11].

Dalam beberapa pasal yang termuat di Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik sudah memberikan perlindungan hukum terkait data pribadi seperti pada pasal 26 contohnya. Dalam pasal tersebut telah ditegaskan bahwa penggunaan informasi elektronik apapun di media harus dengan persetujuan pemilik data tersebut. Apabila dikaitkan kepada perbuatan yang dilarang maka UU

[11] Philipus M. Hadjon. Perlindungan Hukum Bagi Rakyat Indonesia. Bina Ilmu ,Surabaya, 1987, Hlm.25

ITE sudah melarang perbuatan memperoleh informasi dengan cara apapun sebagaimana yang tertera dalam pasal 30 khususnya pada ayat (2). Ketika pelanggaran itu dilakukan maka dapat dikenakan sanksi pidana berupa pidana penjara maksimal 7 tahun dan denda maksimal Rp 700.000.000,- (tujuh ratus juta rupiah).

Hal ini berdasarkan pasal 46 ayat (2) UU ITE yang telah tertulis dengan adanya peraturan ini data pribadi seseorang sudah memiliki payung hukum dan dilindungi oleh hukum. Kewajiban sebagai penyelenggara layanan aplikasi yaitu menjaga kerahasiaan serta keamanan dari informasi elektronik yang dikelolanya. Hal ini sesuai dengan pasal 15 ayat (1) karena apabila penyelenggara aplikasi tidak dapat menjaga data yang dikelolanya dapat dikenakan sanksi administratif sesuai Pasal 84 ayat (1) dan (2) PP No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Penyelenggara layanan aplikasi juga harus mematuhi UU ITE dan juga seluruh perUndang-Undangan terkait yang berlaku di Indonesia hal ini juga dipertegas oleh Surat Edaran dari KOMINFO Nomor 3 Tahun 2016 terkait Penyediaan Layanan Aplikasi dan/atau Konten Melalui Internet.

Dalam UU Perlindungan Data Pribadi Juga khususnya di Pasal 20 ayat (1) menjelaskan bahwa pengelola data atau penyelenggara aplikasi wajib mencegah data pribadi yang diakses secara tidak sah. Larangan hal tersebut juga tertera dalam pasal 50 ayat (1) yang berbunyi : “Setiap Orang dilarang memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian pemilik data pribadi.”

1.5.4 Perlindungan Data pribadi

Konsep perlindungan hak pribadi merupakan salah satu ciri khas konsep hukum Amerika. Kecuali di Prancis dan di Negara-Negara besar lainnya, konsep hukum ini hingga sekarang belum ada. Di Inggris, misalnya, yang memberi tempat bagi gugatan pencemaran nama baik (*libel*) dan penghinaan (*slander*), konsep hukum demikian pun tidak

ditemukan. Hal ini tidaklah mengherankan sebab di Negara Indonesia, pemberitaan yang menyangkut kehidupan pribadi dari perorangan ternyata lebih disukai daripada yang lainnya.

Sejarah perlindungan privasi berawal dari perlindungan atas tempat kediaman seseorang (rumah) dan lalu berlanjut pada perlindungan atas informasi dan komunikasi melalui surat menyurat. Pengaturan perlindungan hak atas privasi awalnya memang lebih dikenal di Eropa dan Amerika. Pada saat itu hukum, meski secara terbatas, telah memberikan perlindungan terhadap kegiatan "menguping" pembicaraan di dalam rumah dan juga melindungi rumah seorang laki – laki dari kegiatan lain yang tidak sah.

Di Amerika Serikat sendiri perlindungan hak atas privasi dimulai dengan disahkannya *Bill of Rights* dari Konstitusi Amerika Serikat. Amandemen Ketiga Konstitusi Amerika Serikat mencegah Pemerintah untuk memerintahkan tentara menetap di rumah-rumah rakyat. Amandemen Keempat Konstitusi Amerika Serikat mencegah Pemerintah untuk melakukan penggeledahan dan penyitaan yang tidak sah. Pejabat Pemerintah diwajibkan mendapatkan persetujuan dari Pengadilan untuk melakukan penggeledahan melalui surat penggeledahan yang didukung oleh bukti permulaan yang cukup. Amandemen Kelima Konstitusi Amerika Serikat menjamin setiap orang untuk tidak dapat dipaksa memberikan keterangan yang memberatkan dirinya sendiri.

Sejarah moderen mengenai privasi dimulai dari hadirnya Belanda di Indonesia. Keputusan Raja Belanda No. 36 yang dikeluarkan pada 25 Juli 1893, bisa dianggap peraturan tertua mengenai perlindungan privasi komunikasi di Indonesia. Sejak 15 Oktober 1915 melalui *Koninklijk Besluit* No 33 (Stbl.1915 No.732) pengaturan perlindungan privasi mulai muncul di dalam Kitab Undang–Undang Hukum Pidana. Meski pengaturan perlindungan hak atas privasi sudah cukup lama di Indonesia, namun perlindungan hak atas privasi baru menjadi perlindungan konstitusional sejak disahkannya Amandemen Kedua UUD 1945 melalui Pasal 28 G ayat (1) dan Pasal 28 H ayat (4).

Namun peraturan legislasi mengenai perlindungan hak atas privasi masih terjadi dan yang berakibat lemahnya perlindungan warga Negara dari peretasan perlindungan hak atas privasi.[12] Persoalannya bukan sekedar perlindungan terhadap hak kehidupan pribadi seseorang belaka, namun juga sampai sejauh mana hak pribadi tersebut. Terlebih lagi bagi seseorang yang mempunyai kedudukan tertentu dalam masyarakat. Apakah dia masih mempunyai hak-hak pribadi tersebut ataukah dia sudah menjadi milik masyarakat, segala sesuatu tindakannya bukan lagi sebagai pribadinya, melainkan sudah menjadi milik masyarakat. Batasan untuk ini pun sulit ditentukan. Apakah jika seseorang telah mempunyai fungsi tertentu dalam masyarakat, dengan demikian sudah tidak mempunyai lagi hak pribadi, semua tingkah lakunya juga diawasi.

Konsep perlindungan data mengisyaratkan bahwa individu memiliki hak untuk menentukan apakah mereka akan membagi atau bertukar data pribadi mereka atau tidak. Selain itu, individu juga memiliki hak untuk menentukan syarat-syarat pelaksanaan pemindahan data pribadi tersebut. Lebih jauh, perlindungan data juga berhubungan dengan konsep hak privasi. Hak privasi telah berkembang dapat digunakan untuk merumuskan hak untuk melindungi data pribadi.

Hak privasi melalui perlindungan data merupakan elemen kunci bagi kebebasan dan harga diri individu. Perlindungan data menjadi pendorong bagi terwujudnya kebebasan politik, spiritual, keagamaan bahkan kegiatan seksual. Hak untuk menentukan nasib sendiri, kebebasan berekspresi dan privasi adalah hak-hak yang penting untuk menjadikan kita sebagai manusia.

Pengumpulan dan penyebarluasan data pribadi merupakan pelanggaran terhadap privasi seseorang karena hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi. Data pribadi merupakan suatu aset atau komoditi bernilai ekonomi tinggi.

Selain itu, terdapat suatu hubungan korelatif antara tingkat kepercayaan dengan perlindungan atas data tertentu dari kehidupan

[12] Daniel J Solove, "Chapter 1 A Brief History Of Norwood," *Care And Conflict* (Washngton University, 2016).

pribadi. Sayangnya, perlindungan terhadap data pribadi saat ini belum diatur dalam Undang-Undang tersendiri melainkan masih tersebar di berbagai peraturan perUndang-Undangan, misalnya Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, dan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Perbankan mengatur data pribadi mengenai nasabah penyimpan dan simpanannya. Ketentuan hukum terkait perlindungan data pribadi masih bersifat parsial dan sektoral, tampaknya belum bisa memberikan perlindungan yang optimal dan efektif terhadap data pribadi sebagai bagian dari privasi. Potensi pelanggaran hak privasi atas data pribadi tidak saja ada dalam kegiatan *online* tetapi juga kegiatan *offline*. Potensi pelanggaran privasi atas data pribadi secara *online* misalnya terjadi dalam kegiatan pengumpulan data pribadi secara masal (*digital dossier*), pemasaran langsung (*direct selling*), media sosial, pelaksanaan program e-KTP, pelaksanaan program *e-health* dan kegiatan komputasi awan (*cloud computing*). Selanjutnya potensi pelanggaran hak privasi dalam berbagai kegiatan di atas akan diuraikan satu per satu.

1.6 Kerangka Konseptual

1.6.1 Perlindungan Hukum Terhadap Nasabah

Menurut Undang - Undang Nomor 10 Tahun 1998 Tentang Perbankan, Bank adalah badan usaha yang menghimpun dana dari masyarakat. Karena bank adalah lembaga keuangan yang mengumpulkan dana dari masyarakat, maka sangat penting untuk melindungi nasabah secara hukum dari berbagai macam kemungkinan kerugian yang akan dialami nasabah.

Hubungan hukum antara nasabah dan bank didasarkan atas suatu perjanjian. Maka wajar bila kepentingan nasabah mendapatkan perlindungan hukum. Perlindungan hukum bagi nasabah sangat penting, inti dari perlindungan hukum tersebut adalah untuk melindungi kepentingan simpanan nasabah yang disimpan di bank dari risiko

kerugian. Perlindungan hukum ini juga merupakan upaya untuk mendapatkan dan menjaga kepercayaan nasabah, sehingga sudah selayaknya bank memberikan perlindungan hukum[13].

1.6.2 Korban Tindak Pidana

Menurut kamus *crime dictionary* yang dikutip seorang ahli bahwa *victim* atau yang disebut dengan korban adalah "orang yang telah mendapat penderitaan fisik atau penderitaan mental, kerugian harta benda atau mengakibatkan mati atas perbuatan atau usaha pelanggaran ringan dilakukan oleh pelaku tindak pidana dan lainnya[14].

Tindak pidana pada dasarnya cenderung melihat pada perilaku atau perbuatan (yang mengakibatkan) yang dilarang oleh undang-undang.Tindak pidana khusus lebih pada persoalan-persoalan legalitas atau yang diatur dalam undang-undang. Tindak pidana khusus mengandung acuan kepada norma hukum semata atau *legal norm*, hal-hal yang diatur Perundang-undangan tidak termasuk dalam pembahasan.Tindak pidana khusus ini diatur dalam undang-undang di luar hukum pidana umum[15].

Selanjutnya secara yuridis pengertian korban termaktub dalam Undang-Undang Republik Indonesia Nomor 31 Tahun 2014 perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, yang dinyatakan bahwa korban adalah orang yang mengalami penderitaan fisik, mental, dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana.

1.6.3 Pencurian Data Nasabah

Kata pencurian dalam bahasa Indonesia, berasal dari kata dasar "curi" yang memperoleh imbuhan "pe" diberi akhiran "an" sehingga membentuk kata "pencurian". Kata pencurian tersebut memiliki arti

[13] Hermansyah. 2008. *Hukum Perbankan Nasional Indonesia*. Jakarta : Cetakan Keempat Kencana. Hlm. 134.

[14] Bambang Waluyo, Viktimologi Perlindungan Korban Dan Saksi, Sinar Grafika, Jakarta, 2011, Hlm 9

[15] Nandang Alamsah D Dan Sigit Suseno, Modul 1 Pengertian Dan Ruang Lingkup Tindak Pidana Khusus, Hlm. 7.

proses, perbuatan cara mencuri dilaksanakan.[16] Pencurian adalah suatu perbuatan yang sangat merugikan orang lain dan juga orang banyak, terutama masyarakat sekitar kita. Maka dari itu kita harus mencegah terjadinya pencurian yang sering terjadi dalam kehidupan sehari-hari, karena terkadang pencurian terjadi karena banyak kesempatan.

Dalam Kamus Besar Bahasa Indonesia, disebutkan bahwa mencuri adalah suatu perbuatan yang mengambil barang milik orang lain dengan jalan yang tidak sah. Untuk mendapat batasan yang jelas tentang pencurian,maka dapat dilihat dari Pasal 362 KUH Pidana yang berbunyi sebagai berikut:

"Barang siapa mengambil sesuatu barang yang mana sekali atau sebagian termasuk kepunyaan orang lain, dengan maksud akan memiliki barang itu dengan melawan hak, dihukum karena pencurian dengan hukuman penjara selama-lamanya lima tahun atau denda sebanyak-banyaknya Rp.900[17].

Berdasarkan pasal di atas, maka dapat diketahui bahwa delik pencurian adalah salah satu jenis kejahatan terhadap kepentingan individu yang merupakan kejahatan terhadap harta benda atau kekayaan. Pengertian pencuri dibagi menjadi dua golongan, yaitu: pencurian secara aktif dan pencurian secara pasif:

a. Pencurian secara aktif

   Pencurian secara aktif adalah tindakan mengambil hak milik orang lain tanpa sepengetahuan pemilik.

b. Pencurian secara pasif adalah tindakan menahan apa yang seharusnya menjadi milik orang lain.

Seseorang yang melakukan tindakan atau berkarir dalam pencurian disebut pencuri dan tindakanya disebut mencuri. Dalam Kamus Hukum Sudarsono pencurian dikatakan proses, perbuatan atau cara mencuri[18].

1. *Phising*

[16] Ridwan Hasibuan, 1994. "Kriminologi Dalam Arti Sempit Dan Ilmu-Ilmu Forensik", Usu Press,Medan, Hlm.8

[17] R.Soesilo, Op Cit, Hlm.249

[18] Sudarsono, 2007, "Kamus Hukum", Cetakan Ke empat, Rineka Cipta , Jakarta, Hlm. 85

Penipuan *Phising* biasanya dilakukan dengan adanya pesan email penipuan dari perusahaan yang sah (misalnya, universitas, penyedia layanan internet, bank). Pesan-pesan ini biasanya mengarahkan seseorang kesitus laman palsu atau membuat seseorang untuk membocorkan informasi pribadi (misalnya, kata sandi, kartu kredit, atau *update* akun lainnya). Para pelaku kemudian menggunakan informasi pribadi untuk melakukan pencurian identitas. Identitas tersebut kemudian digunakan untuk kejahatan yang merugikan pemilik. Kejahatan ini biasa terjadi pada pengguna *online banking*[19].

Phising dapat juga dioprasikan dengan cara mengirimkan *e-mail* atau membuat suatu *website* yang seakan-akan sebagai penyelenggara *e-commerce*, sehingga banyak pengguna internet yang memasukkan data atau *Personal Identification Number* (PIN) untuk melakukan transaksi *online* ke alamat yang diperkenalkan tersebut. Para pelaku *phising* ini dapat dijerat dengan Pasal 378 Kitab Undang-undang Hukum Pidana. Pasal ini merupakan ketentuan pidana mengenai penipuan, isinya adalah sebagai berikut:

"Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu dengan tipu muslihat, atau rangkaian kebohongan, menggerakan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama empat tahun".

Serangan *Phising* dilakukan dengan mendistribusikan *e-mail* yang berisi pesan tentang alamat pengirim, mekanisme kerja, dan nama suatu perusahaan sehingga seakan-akan tampak menunjukkan identitas bank, atau perusahan asuransi, atau perusahaan pengelola kartu kredit, atau lembaga keuangan lain. Pesan *e-mail* tersebut dirancang secara meyakinkan untuk mengelabuhi penerima pesan, dengan cara membuat pengumuman data dengan identitas perusahaan palsu yang meliputi rekening, penanggungjawab, kartu kredit, jaminan sosial, dan lain-lain.

[19] Mr.Roeslan Saleh, Perbuatan Pidana Dan Pertanggung Jawaban Pidana, Aksara Baru, 1983, Jakarta, Hlm.76.

Bahkan seringkali dalam *e-mail* tersebut disertakan foto para pejabat palsu dan sejumlah data perusahaan palsu. Jika ada penerima *e-mail* tertarik dengan isi pesan tersebut, maka akan melakukan transaksi melalui internet sehingga data korban dan PIN dapat direkam oleh pelaku *phising*. Perbuatan ini merugikan banyak orang, karena akan dapat menyebabkan penipuan uang, pencurian identitas, dan aktivitas curang lainnya melalui internet[20].

Kejahatan siber merupakan tindak kejahatan yang dilakukan secara tidak langsung. Kejahatan semacam ini dapat terjadi kapanpun dan siapapun bisa menjadi korbannya. Kejahatan siber dapat terjadi pada siapapun dan dimana pun mereka berada. Pelaku kejahatan siber mempunyai tujuan beragam mulai dari hanya sekedar main-main sampai dijadikan pekerjaan tetap oleh pihak yang tidak bertanggungjawab yang menimbulkan banyak kerugian pada korbannya.

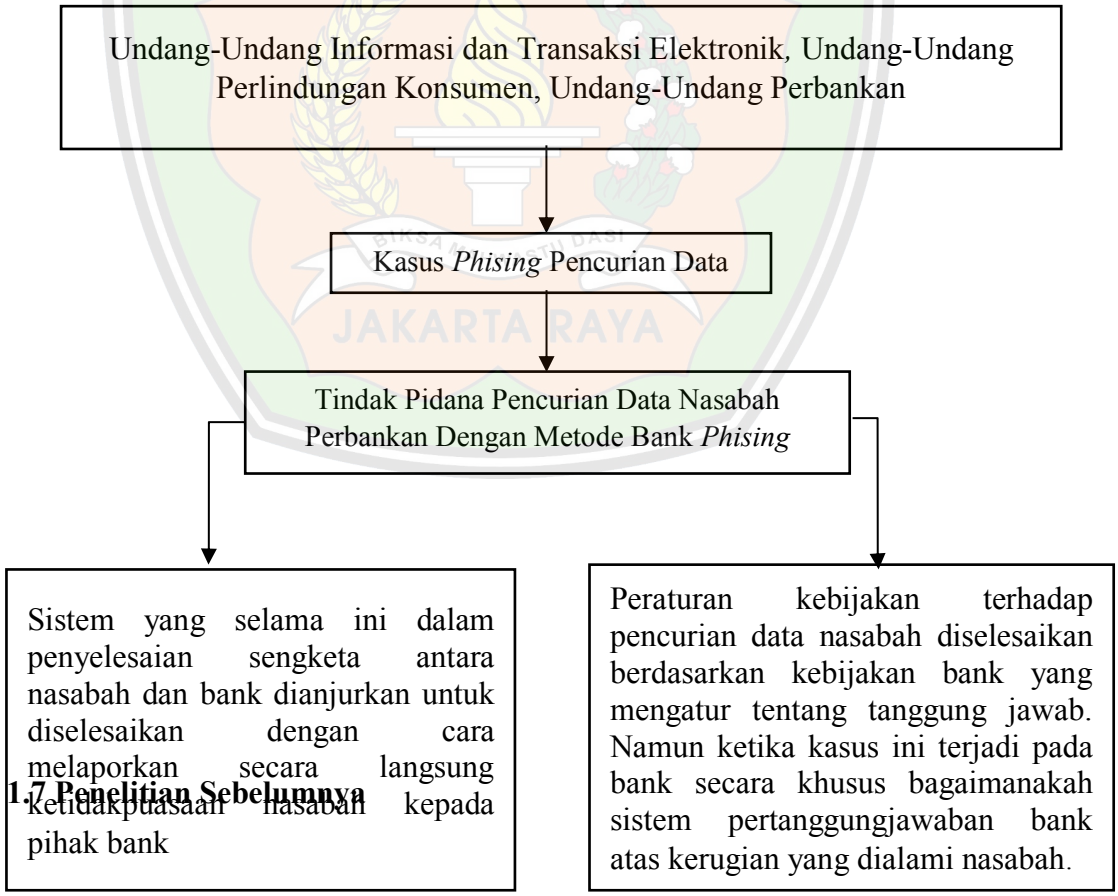
Bank Indonesia mengeluarkan Peraturan No.7/7/PBI/2006 tentang Penyelesaian Pengaduan Nasabah sebagaimana direvisi menjadi PBI No. 10/10/PBI/2008 sebagai standar minimal dalam sistem penyelesaian pengaduan nasabah untuk mengurangi persuasi dan dampak buruk untuk bisnis dibidang perbankan. Di dalam Peraturan BI No.10 Tahun 2008 juga dijelaskan tentang beberapa cara untuk menyelesaikan sengketa perbankan yaitu dengan cara litigasi (jalur pengadilan) dan non-litigasi (jalur diluar pengadilan).

Alur pelaksanaan mediasi melalui jalur litigasi biasanya dilakukan pada tahap awal persidangan. Dimana sebelum memulai persidangan hakim wajib mengupayakan perdamaian kepada para pihak melalui mediasi, hal ini sesuai dengan PERMA Nomor 1 Tahun 2008 tentang Prosedur Mediasi Di Pengadilan. Sementara itu untuk jalur non-litigasi dilakukan diluar pengadilan dengan pedoman Undang-Undang No.30 Tahun 1999 tentang Abitrase dan Alternatif Penyelesaian Sengketa melalui konsultasi, negosiasi dan mediasi. Penyelesaian sengketa antara nasabah dan bank dianjurkan untuk diselesaikan dengan cara melaporkan

[20] Widodo, Aspek Hukum Pidana Kejahatan Mayantara, Aswaja Pressindo, Yogyakarta, 2013, Hlm 85.

secara langsung ketidakpuasan nasabah kepada pihak bank. Akan tetapi jika bank tidak dapat menyelesaikan sengketa dengan baik serta tuntutan nasabah tidak terpenuhi dengan baik oleh pihak bank, maka penyelesaian dengan mediasi perbankan merupakan opsi terbaik.

Berdasarkan kerangka konseptual diatas, kerangka pemikiran yang digunakan dalam penelitian ini adalah sebagai berikut:



1.7 Penelitian Sebelumnya

1. **PERTANGGUNGJAWABAN PIDANA BAGI PELAKU TINDAK PIDANA PENCURIAN DATA NASABAH PERBANKAN DENGAN METODE *SKIMMING* DI TINJAU MENURUT UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK**

   Oleh Surya Ari Wibowo, Program Ilmu Studi Hukum Fakultas Hukum Universitas Sumatera Utara 2021

   Pada penelitian ini, ditemukan hasil penelitian berupa berdasarkan Putusan Pengadilan Negeri Denpasar Nomor 262/Pid.Sus/2017/PN. Dps dan Putusan Pengadilan Negeri Denpasar Nomor 573/Pid.Sus/2018/PN. Dps di atas di atas, maka dapat disimpulkan bahwa sebelum terdakwa mempertanggungjawabkan tindak pidana yang dilakukannya, selain harus melihat dan memeriksa alat-alat bukti yang diajukan ke depan persidangan maka harus dilihat juga adanya kemampuan bertanggung jawab terdakwa, adanya kesalahan terdakwa, dan tidak adanya alasan penghapus pidana atas perbuatan yang dilakukan oleh terdakwa.

2. **PERTANGGUNGJAWABAN LEMBAGA PERBANKAN TERHADAP PENCURIAN DATA NASABAH**

   Oleh Lukmanul Hakim, Program Ilmu Studi Hukum Fakultas Hukum Universitas Bandar Lampung 2018

   Pada penelitian ini, ditemukan hasil penelitian berupa Berdasarkan pembahasan yang telah disampaikan pada bab sebelumnya tentang aspek perlindungan hukum atas data pribadi nasabah, dengan menggunakan perlindungan secara implisit yaitu Perlindungan secara implisit (*implicit deposit protection*), yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif yang dapat menghindarkan terjadinya kebangkrutan bank. dan Perlindungan secara eksplisit (*explicit deposit protecti*on) yaitu perlindungan melalui pembentukan suatu lembaga yang menjamin simpanan masyarakat, sehingga apabila bank mengalami kegagalan, lembaga tersebut yang akan mengganti dana masyarakat.

3. **PERTANGGUNGJAWABAN PIDANA TERHADAP KORPORASI PERBANKAN AKIBAT DARI TINDAK PIDANA PEMBOBOLAN BANK**

Oleh Frilly Margareth Wurangian, Program Ilmu Studi Hukum Fakultas Hukum 2015

Pada penelitian ini, ditemukan hasil penelitian berupa berdasarkan Meskipun Undang-Undang Perbankan belum mengatur bahwa korporasi dapat dikenakan pertanggungjawaban pidana sebagimana terdapat dalam pasal 46 ayat (2) Undang-Undang No. 10 tahun 1998 tentang Perbankan, namun dalam hal ini setiap tindakan kejahatan yang dilakukan oleh para pihak dalam korporasi dikenakan sanksi terhadap pihak pengurus tersebut, berdasarkan ajaran pertanggungjawaban pidana vikarius, dimana jika dihubungkan dengan pertanggungjawaban korporasi, maka yang bertanggungjawab adalah pengurus korporasi.

4. **PERTANGGUNGJAWABAN PIDANA DALAM KEJAHATAN PERBANKAN**

   Oleh Yohana, Program Ilmu Studi Hukum Fakultas Hukum Universitas Sumatera Utara 2014

   Pada penelitian ini, ditemukan hasil penelitian berupa berdasarkan Undang-Undang Perbankan sudah jelas mengatur siapa saja yang dapat dimintai pertanggungjawaban pidana atas terjadinya tindak pidana terkait kejahatan perbankan, akan tetapi belum jelas mengatur lebih spesifik mengenai alasan pemaaf ataupun pembenar terhadap pelaku tindak pidana perbankan. Undang-Undang Perbankan juga perlu dilakukan revisi terkait beralihnya beberapa tugas, fungsi, dan wewenang Bank Indonesia kepada Otoritas Jasa Keuangan setelah dikeluarkannya Undang-Undang Nomor 21 Tahun 2011 tentang OJK, serta guna menegaskan berlakunya penerapan *ultimum remedium* dalam Undang-Undang No. 10 Tahun 1998 tentang Perbankan.

1.8 Metode Penelitian

1.8.1 Jenis Penelitian

Penelitian normatif menurut Marzuki merupakan penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder". Penelitian hukum normatif disebut juga penelitian hukum doktrinal.

Hukum normatif adalah suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi [21]. Penelitian ini termasuk kategori penelitian hukum normatif yang diawali dengan mengkaji data sekunder dalam bentuk data kepustakaan yang berkaitan dengan permasalahan yang dipelajari melalui bahan hukum primer, sekunder dan tersier terkait pertanggungjawaban pidana pribadi atas pencurian data nasabah perbankan dengan metode bank *phising*.

1.1.2 Pendekatan Penelitian

Jenis pendekatan yang digunakan dalam penelitian ini adalah dengan menggunakan pendekatan studi kasus dan pendekatan peraturan perundang-undangan mengenai bagaimana bentuk Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Bank *Phising*.

1.8.2 Sumber Bahan Hukum.

Data yang digunakan bersumber pada data primer dan sekunder.

a. Bahan hukum primer

   Yaitu bahan hukum yang mengikat yang terdiri dari norma atau kaidah dasar, peraturan dasar dan peraturan perundang-undangan yang digunakan adalah Perlindungan Undang - Undang Nomor 10 Tahun 1998 Tentang Perbankan, Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Peraturan No.7/7/PBI/2006 tentang Penyelesaian Pengaduan Nasabah sebagaimana direvisi menjadi PBI No. 10/10/PBI/2008 sebagai standar minimal dalam sistem penyelesaian pengaduan nasabah.

b. Bahan Hukum Skunder

   Yaitu bahan-bahan yang erat hubungannya dengan bahan hukum primer dan dapat membantu menganalisis bahan-bahan hukum primer antara lain dari jurnal-jurnal hukum atau karya ilmiah yang sudah di publikasikan, pendapat-pendapat para ahli hukum dan Internet.

[21] Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta: Kencana, 2007, hlm.23

1.8.3 Metode Pengumpulan Bahan Hukum

Bahan hukum dikumpulkan melalui prosedur inventarisasi dan identifikasi peraturan perundang-undangan, serta klasifikasi dan sistematisasi bahan hukum sesuai permasalahan penelitian. Oleh karena itu, teknik pengumpulan bahan hukum yang digunakan dalam penelitian ini adalah dengan studi kepustakaan. Studi kepustakaan dilakukan dengan cara membaca, menelaah, mencatat membuat ulasan bahan-bahan pustaka, maupun penulusuran melalui media internet yang ada kaitannya dengan Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Bank *Phising*.

1.8.4 Teknik Analisis Bahan Hukum

Teknik analisis bahan buku yang dipergunakan pada penelitian ini adalah deskriptif yuridis yang dikaji dari jenis penelitian yuridis normatif dan dijelaskan secara deskriptif dengan memaparkan, menguraikan dari penelitian ini berdasarkan bahan hukum yang diperoleh terkait dengan Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Bank *Phising*.

1.9 Sistematika Penulisan

BAB I. PENDAHULUAN

Bagian ini menjelaskan latar belakang masalah dari pertanggungjawaban pidana bagi pelaku tindak pidana pencurian data nasabah perbankan dengan metode bank pishing serta metode penelitian yang digunakan dalam menjawab rumusan masalah penelitian.

BAB II. PENGATURAN DATA PRIBADI NASABAH PADA SEKTOR PERBANKAN

Bagian ini mengandung teori-teori Pengaturan Data Pribadi Nasabah Pada Sektor Perbankan.

BAB III. PENINDAKAN HUKUM PENCURIAN DATA PRIBADI NASABAH DENGAN METODE BANK PHISING

Bab ini akan menjelaskan Penindakan Hukum Pencurian Data Pribadi

Nasabah Dengan Metode Bank *Phising*

BAB IV. PERTANGGUNGJAWABAN PIDANA DALAM PENCURIAN DATA NASABAH PERBANKAN DENGAN MENGGUNAKAN METODE BANK PHISING

Bagian ini akan menguraian mengenai Pertanggungjawaban Pidana Dalam Pencurian Data Nasabah Perbankan Dengan Menggunakan Metode Bank *Phising.*

BAB V. PENUTUP

Bagian ini mengandung simpulan dari hasil penelitian yang akan menjadi bahan masukan dalam Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Bank *Phising*