BAB I

ANALISA HUKUM TERHADAP PERLINDUNGAN HUKUM BAGI NASABAH PENGGUNA *INTERNET BANKING*

1.1 Pengertian *Internet Banking*

Internet Banking pada dasarnya merupakan gabungan dua istilah dasar yaitu Internet dan Banking (bank). *Interconnected Network (Internet)* adalah system jaringan yang menghubungkan tiap-tiap computer secara global di seluruh penjuru dunia. Koneksi yang menghubungkan masing – masing computer tersebut memiliki standar yang digunakan yang disebut *Internet Protocol Suite* disingkat dengan TCP/IP.[1]

Adanya perkembangan ilmu pengetahuan dan teknologi informasi serta persaingan dalam dunia perbankan telah membuat bank-bank beralih untuk memanfaatkan dan menerapkan teknologi informasi dalam meningkatkan layanannya. Penerapan teknologi informasi telah membawa banyak perubahan dalam kegiatan operasional serta pengelolaan data bank sehingga dapat dilakukan secara lebih efisien dan efektif serta memberikan informasi secara lebih akurat dan cepat. Perkembangan produk perbankan berbasis teknologi informasi diantaranya berupa electronic banking memudahkan nasabah untuk melakukan transaksi perbankan secara *non cash* setiap saat melalui jaringan elektronik.[2]

[1] Achmad, ‚*Pengertian Internet dan Sejarah Internet*‘, dalam http://www.likethisya.com/ pengertian-internet.html,

[2] http://www.internetbanking.htm/virtual_banks/

Electronic Banking pada mulanya dalam bentuk ATM dan transaksi melalui telepon, namun dalam perkembangannya dengan inovasi di bidang teknologi internet telah membentuk delivery channel baru yang memberikan keuntungan bagi bank dan nasabah. *Electronic Banking* berbasis internet yang dikenal sebagai internet banking muncul sebagai aplikasi e-business bagi kegiatan dunia perbankan Bank menggunakan fasilitas internet untuk menawarkan produk jasa pelayanan perbankan dengan cara yang lebih efisien internet banking adalah bentuk *E-commerce* yang dilakukan oleh pihak bank.

Pada prinsipnya layanan *internet banking* hampir sama dengan layanan ATM. Layanan *internet banking* dirancang sebagai salah satu sarana akses ATM dimana saja yang disebut dengan virtual ATM sehingga apa yang dilakukan di ATM dapat dilakukan kecuali mengambil uang tunai." Perbedaan utama antara ATM dengan virtual adalah terletak pada awal dan akhirnya yaitu untuk mulai melakukan transaksi pada virtual ATM, nasabah terlebih dahulu harus mempunyai user ID dan nomor PIN. Sedangkan ATM cukup dengan nomor PIN saja. Perbedaan lainnya yaitu cara memberikan bukti transaksi ATM akan mengeluarkan kertas dari mesin tersebut, sedangkan virtual ATM akan memberikan konfirmasi melalui layar komputer dan mengirim ulang konfirmasi tersebut melalui e-mail nasabah.

Internet banking atau yang biasa disebut *online* banking merupakan sebuah system yang memungkinkan individu untuk melakukan kegiatan perbankan dari mana saja melalui *internet. Online banking* memungkinkan nasabah untuk melakukan transaksi rutin semua, seperti transfer rekening pertanyaan saldo, pembayaran tagihan, dan stop-pembayaran permintaan, dan beberapa bahkan menawarkan pinjaman online dan aplikasi kartu kredit.[3]

Karen Furst mendefinisikan *internet banking* sebagai penggunaan internet sebagai saluran perpanjangan jarak jauh untuk mengantarkan jasa-jasa perbankan. Jasa-jasa perbankan yang diberikan melalui *internet banking* adalah jasa-jasa yang juga diberikan melalui perbankan tradisional, seperti pembukaan rekening. melakukan transfer dana antar rekening, tagihan pembayaran elektronis yang memungkinkan nasabah untuk menerima dan melakukan pembayaran melalui internet banking.[4]

Sedangkan menurut David whitely, *Intenet Banking* di definisikan sebagai salah satu jasa pelayanan yand di berikan bank kepada nasabahnya, dengan maksud agar nasabah dapat mengecek saldo rekening dan membayar tagihan secara 24 jam tanpa perlu dating ke kantor cabang.[5]

1.2 Tujuan dan Manfaat *Internet Banking* bagi Bank dan Nasabah

Institusi perbankan dalam penerapan internet banking harus memberikan jasa pelayanan yang lebih sesuai dengan kehendak nasabah dan lebih menjamin keamanannya sehingga dapat memberikan kenyamanan dan kepuasan kepada para nasabah. Penggunaan internet banking oleh nasabah akan memberikan pelayanan yang lebih baik tanpa mengenal tempat dan waktu.

1.2.1 Bagi bank

Tujuan internet banking bagi pihak bank yaitu :

1. Menjelaskan produk dan jasa seperti, pemberian pinjaman dan kartu kredit;

---

[3] *Onile banking*, http://www.investorwords.com

[5] David whitley, *E-commerce: Strategi, Technology and Application, (*London: Mc.Graw-Hill,2000), hal.226-227.

2. Menyediakan informasi mengenai suku bunga dan kurs mata uang asing yang terbaru;
3. Menunjukkan laporan tahunan perusahaan dan keterangan pers lainnya.
4. Menyediakan informasi ekonomi dan bisnis seperti perkiraan bisnis;Memberikan daftar lokasi kantor bank tersebut dan lokasi ATM;
5. Memberikan daftar pekerjaan yang membutuhkan tenaga kerja baru;
6. Memberikan gambaran mengenai bank;
7. Menyediakan informasi mengenai sejarah bank dan peristiwa terbaru;
8. Memberikan pelayanan kepada nasabah untuk memeriksa neraca tabungan dan memindahkan dana antar tabungan;
9. Menyediakan algorithma yang sederhana sehingga para nasabah dapat membuat perhitungan untuk pembayaran pinjaman, perubahan atau pengurangan pembayaran hipotik, dan lain sebagainya;
10. Menyediakan sambungan menuju situs lain di internet yang masih berhubungan dengan internet banking.[6]

1.2.2 Bagi Nasabah

Layanan *internet banking* yang mengedepankan kecepatan dan efisiensi memberikan kemudahan bagi naabah. Beberapa tujuan pihak nasabah menggunakan *internet banking* antara lain:

1. Mempermudah nasabah dalam bertransaksi perbankan, karena dengan *internet banking* akses perbankan dapat dilakukan di computer pribadi *(personal computer)* nasabah bahkan lebih dekat, tanpa harus dating ke kantor cabang .
2. Mempercepat kegiatan transaksi perbankan, hanya dengan komputer pribadi, nasabah dapat mengakses transaksi apapun dengan beberapa "klik" di mouse computer, hal ini dapat

[6] Mary j.Conin, *Banking and Finance on the Internet,*(Canada : wiley & Sons,1998).

dilakukan tanpa membuang-buang waktu untuk dating dan mengisi formulir di kantor bank.

3. Menghemat biaya seperti menghemat ongkos jalan ke kantor cabang.

Selain tujuan tersebut di atas, aspek manfaat sebagaimana yang ditawarkan oleh bank menjadi factor penting yang menarik minat nasabah menggunakan *Internet banking*. Beberapa manfaat *internet banking* bagi pihak nasabah antara lain:

1. Nasabah dapat menjaga hubungan dan melakukan transaksi langsung dengan beberapa bank dan perusahaan pelayanan financial hanya dengan menggunakan jaringan yang sama;
2. Nasabah dan bank menjadi lebih mandiri dan tidak lagi bergantung pada menjadi lebih dan tidak lagi satu kantor saja:
3. Dengan adanya internet banking maka akan menarik perusahaan perangkat lunak untuk saling bersaing, yang kemudian akan menghasilkan harga maupun kualitas yang lebih baik dan dapat menawarkan produk dan jasa yang lebih beragam, baik untuk nasabah dan bank:
4. Nasabah dapat berhubungan dengan semua institusi financial mereka tanpa harus memiliki perangkat lunak, penyedia jaringan penghubung yang berbeda;

5. Pengurangan biaya transaksi, karena bank berusaha untuk menyediakan harga yang lebih rendah untuk dapat bersaing dengan bank lain.

1.3 Tipe- tipe Layanan *Internet Banking*

Internet banking merupakan salah satu pelayanan jasa bank yang memungkinkan nasabah untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi melalui internet. Jenis kegiatan *internet banking* dapat dibedakan menjadi 3 (tiga) yaitu *informational internet banking*, *communicative internet banking*, dan *transactional internet banking.*

1.3.1 *Informational Internet Banking*

Merupakan tingkatan atau tahapan yang paling sederhana yaitu pelayanan jasa bank kepada nasabah dalam bentuk informasi melalui jaringan internet dan tidak melakukan eksekusi transaksi *(execution of transaction)* atau sekedar brosur elektronik suatu bank sehingga tingkat risikonya rendah karena tidak terhubung dengan database bank.

1.3.2 *Communicative Internet Banking*

Pelayanan jasa bank kepada nasabah dalam bentuk komunikasi atau melakukan interaksi dengan bank penyedia layanan *internet banking* secara terbatas dan tidak melakukan eksekusi transaksi.

1.3.3 *Transactional internet banking*

merupakatn tingkatan paling lengkap yaitu pelayanan jasa bank kepada nasabah untuk melakukan interaksi dengan bank penyedia layanan internet banking dan melakukan eksekusi dan transaksi antara lain transfer dana, pembayaran tagihan, dan lainnya seperti layaknya pelayanan counter atau ATM kecuali penarikan kas Pada dasarnya bank yang menyediakan layanan met bank dapat bebas menetukan transaksi atau produk apa saja yang disediakan. Penentuan jenis produk/jasa tentunya akan disesuaikan dengan kemampuan dan strategi masing-masing bank. *Internet banking* memiliki banyak fitur dan kemampuan, juga memiliki beberapa aplikasi yang spesifik Fitur-fitur umum layanan *internet banking* terbagi menjadi:

1. Transaksional, melakukan transaksi keuangan misalnya transfer payment *gateway* (pembayaran fasilitas jasa tertentu), kliring pengajuan permohonan pinjaman, pembukaan rekening baru dan lain-lain.
2. Non-transaksional misalnya informasi saldo, informasi kartu kredit, notifikasi, registrasi layanan lain, informasi administrasi, dan lain-lain.

1.4 Pihak-pihak yang Terlibat dalam Layanan *Internet Banking*

Teknologi telah begitu maju dalam segala bidang dan begitu terbuka bagi semua orang, menyebabkan perusahaan harus berpacu

dengan kebutuhan teknologi yang tumbuh di dalam perusahaan dengan tingkat kemajuan teknologi di luar perusahaan. Penggunaan teknologi informasi dan komunikasi dalam perbankan nasional relatif lebih maju dibandingkan sektor lainnya Beberapa pihak yang terkait dalam penyelenggaraan layanan *internet banking*, yaitu:

1.4.1 Bank

Dalam Pasal 1 angka 2 Undang Undang tentang Perbankan menyebutkan bahwa Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak. Bidang jasa perbankan meliputi berbagai kegiatan dalam rangka penyelenggaraan transaksi-transaksi yang berkaitan dengan kepentingan masyarakat dan dunia usaha. Dalam *layanan internet banking* bank dapat menyelenggarakan teknologi informasi sendiri atau menggunakan pihak penyedia jasa teknologi informasi, sebagaimana diatur dalam pasal 18 Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Pihak Bank Umum.

1.4.2 Nasabah

Dalam Pasal 1 angka 16 Undang – undang Perbankan menyebutkan bahwa nasabah adalah pihak yang menggunakan jasa bank. Nasabah perbankan menjadi 2 (dua), yaitu nasabah penyimpan

(nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan) dan nasabah debitur (nasabah yang memperoleh fasilitas kredit atau pembiayaan berdasarkan Prinsip Syariah atau yang dipersamakan dengan itu berdasarkan perjanjian bank dengan nasabah yang bersangkutan). Dalam layanan *internet banking*, nasabah yang dimaksud adalah nasabah yang telah terdaftar dalam layanan *internet banking bank.*

1.4.3 *Internet Service Provider (ISP)*

Dalam Pasal 1 angka 12 Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi disebutkan bahwa penyelenggaraan telekomunikasi adalah kegiatan penyediaan dan pelayanan telekomunikasi sehingga memungkinkan terselenggaranya telekomunikasi. *Internet Service Provider (ISP)* merupakan perusahaan yang menjual koneksi internet kepada pelannggan. Pada awalnya ISP lebih dikenal dengan jaringan telepon, sebab ISP pertama kali menjual koneksi internet melalui jaringan telepon, saat ini ISP bukan hanya digunakan dalam jaringan telepon, namun telah menggunakan teknologi *fiber optic wiress* dan lainnya. Layanan ISP dibedakan menjadi 2 di macam yaitu *deal on demand* yang merupakan sebuah layanan internet dimana pelanggan tidak dapat selalu terhubung dengan internet, dan *dedicated*, yaitu sebuah layanan internet dimana pengguna selalu terhubung dengan internet.

1.5 Risiko-risiko dalam Layanan *Internet Banking*

Kemunculan internet dapat dikatakan merupakan hasil dari revolusi informasi yang sangat mengagumkan, membanggakan oleh karena itu secara mendasar mengandung ciri praktis dan memudahkan, baik untuk penggunaan secara orang perorangan maupun organisasi atau institusional, selama berbagai aspek kehidupan. Ciri tersebut tidak terlepas dari kekuatan dan kecepatan internet dalam tatanan operasionalnya yang antara lain dapat menembus ruang dan waktu. Dengan berkembangnya penggunaan sarana komputer juga membuka peluang bagi orang - orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Beberapa macam kejahatan dengan menggunakan sarana komputer;

1.5.1 Pencurian dan penyadapan data *Internet Banking*

Tindakan kejahatan penyebab oleh *Hacker* yang di lakukan menggunakan penyadapan jaringan internet dengan tujuan utama untuk mencuri data dan informasi penting seperti *username* dan *password m-banking,* informasi data kredit *password email,* dan data penting lainnya, atau disebut juga dengan *Sniffing.* Biasanya pelaku *Sniffing* berusaha membuat korban membuka linknnatau file yang di kirim lalu menginstalnya. Setelah itu para pelaku akan berusaha mengakses perangkat dan mencuri data pribadi korbannya.

Ada dua jenis serangan sniffing yang harus kamu ketahui, yaitu *sniffing* aktif dan pasif. Berikut penjelasan kedua jenis serangan *sniffing* tersebut.

1. *Sniffing* aktif

Sniffing aktif merupakan bentuk kejahatan siber dengan cara mengubah isi paket data. *Sniffing* aktif dilakukan pada *switch* jaringan, bukan hub, dengan menyuntikkan lalu lintas ke LAN dengan berbagai cara.

2. *Sniffing* Pasif

Berbeda dari sniffing aktif, sniffing pasif dilakukan melalui hubungan Setiap data dari LAN ke LAN sebenarnya dikirim lebih dulu ke mesin yang menghubungkan keduanya, jenis sniffing ini menyerang hub yang menghubungkan data dari LAN ke LAN dengan menunggu data yang dikirim.

Ada beberapa cara menghindari *sniffing* yang bisa di praktekkan seperti berikut:

1. Jangan asal mengunduh aplikasi atau klik tautan (link) yang dikirim melalui WhatsApp, SMS, atau email dari sumber tidak jelas.
2. Cek keaslian nomor telepon, WhatsApp, SMS, dan email dengan cara menghubungi *call center* resmi perusahaan terkait yang dicatut namanya pada pesan tersebut.
3. Unduh aplikasi hanya dari sumber terpercaya seperti *Google Playstore* dan *App Store.*
4. Aktifkan notifikasi dari berbagai transaksi rekening agar kamu bisa memantau segala transaksi baik yang kamu lakukan maupun yang mencurigakan.
5. Ganti kata sandi dan PIN di berbagai aplikasi layanan keuangan seperti *mobile banking*, *e-wallet*, dan lainnya.
6. Jangan asal gunakan jaringan internet *(Wifi)* di ruang publik ketika akan melakukan transaksi keuangan.[7]

[7] https://bankmas.co.id/id/blog/kenali-apa-itusniffing-dan-bahaya/

1.5.2 Kejahatan Online Internet Banking

Seiring dengan perkembangan teknologi internet, menyebabkan munculnya kejahatan yang di sebut juga dengan *Cybercrime* atau kejahatan melalui jaringan Internet. Bagi CyberCrimer, kejahatan melalui *internet banking / mobile banking* dapat menjangkau jutaan calon korban dengan biaya yang tidak mahal. Kejahatan *internet banking/ mobile banking* ini telah merugikan banyak pengguna dan terus mengalami peningkatan.

Modus yang sering digunakan :

1. *Pharming*

Penipu atau *hacker* melakukan pengalihan dari situs yang sah ke situs palsu tanpa diketahui dan disadari oleh korban. Kemudian mengambil data yang dimasukkan oleh korban sehingga masuk ke dalam area yang menjadi permainan penipu tersebut.

2. *Spoofing*

Menggunakan perangkat lunak untuk menutupi identitas dengan menampilkan alamat *e-mail*/ nama/ nomor telepon palsu di komputer agar menyembunyikan identitas. Untuk melakukan penipuan mereka menimbulkan kesan berurusan dengan pebisnis terkemuka.

3. *Keylogger*

Software yang dapat menghafal tombol keyboard yang digunakan tanpa diketahui oleh pengguna.

4. *Phising.*

Tindakan memperoleh informasi pribadi seperti user ID, PIN, nomor rekening bank/ nomor kartu kredit secara tidak sah. Informasi ini kemudian dimanfaatkan untuk mengakses rekening, melakukan penipuan kartu kredit atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.

Yang dapat kita lakukan agar semuanya terlindungi adalah;

1. Lindungi komputer Anda dengan perangkat lunak *anti-virus, spyware filter, filter e-mail* dan *program firewall*.
2. Segera hubungi Bank yang bersangkutan dan laporkan kecurigaan Anda.
3. Jangan membalas *e-mail* yang meminta informasi pribadi. Bank tidak pernah meminta informasi pribadi seperti PIN atau *password.*
4. Pastikan akses alamat website internet banking Anda yang benar. Jangan klik dengan kata yang sengaja disalah ejakan atau mirip dengan yang asli.[8]

1.5.3 Serangan *Malware Internet Banking*

Malware adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, server atau jejaring komputer tanpa izin (informed consent) dari pemilik. *Malware* bisa

[8] https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/356

menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data /informasi.[9]

Malware dapat menyebabkan kerusakan serius pada sistem komputer dan jaringan, termasuk kehilangan data, penyalahgunaan informasi pribadi, dan pencurian identitas.

Motif dibalik serangan malware sebenarnya cukup bervariatif. Meskipun demikian, secara garis besar peretas atau *cyber hacker* melakukan serangan *malware* untuk beberapa tujuan, seperti:

1. Mencuri data-data sensitif
2. Mengirim spam
3. Menyediakan akses remote control bagi penyerang untuk bisa menggunakan mesin yang sudah terinfeksi.

Beberapa jenis *malware* :

1. VIRUS

Malware tipe ini pada umumnya akan menginfeksi perangkat atau sistem dengan cara menempel atau menyisipkan dirinya sendiri ke dalam kode dari suatu program. Ketika user atau korban membuka program tersebut, maka virus akan mulai menginfeksi perangkat.

2. *WORMS*

Worm merupakan jenis *malware* yang dapat mereplikasi dirinya sendiri tanpa membutuhkan interaksi manusia. Selain itu, *worms* juga

[9] http://educsirt.kemdikbud.go.id/portal/berita/69

tidak perlu melampirkan dirinya ke program perangkat lunak lain untuk bisa menginfeksi sistem dan menyebabkan kerusakan. *Worms* dapat menyebar dengan berbagai cara, seperti melalui *email attachments*, USB drives, atau situs web yang terinfeksi.

3. *TROJAN HORSE (Trojan)*

Trojan horse adalah jenis *malware* yang sering menyamar sebagai file atau perangkat lunak yang sah seperti antivirus palsu, mp3, atau iklan. Dengan beragam teknik social engineering, peretas akan membujuk dan mendorong user untuk membuka, mengunduh, dan menjalankan perangkat lunak/file palsu tersebut pada sistem mereka. Jika hal tersebut berhasil dijalankan, maka trojan memungkinkan peretas untuk dapat mencuri data sensitif, mendapatkan *backdoor access* ke dalam sistem, atau bahkan memata-matai Anda.

4. *RANSOMEWARE*

Ransomware adalah jenis *malware* yang digunakan oleh peretas untuk memblokir sistem atau file sampai sejumlah uang dibayarkan. Sebagian besar *ransomware* dapat mengenkripsi data di komputer dengan kunci yang tidak diketahui oleh pengguna. Selanjutnya, peretas akan meminta uang tebusan agar user atau korban bisa memperoleh kembali akses file tersebut. Ketika menjalankan serangan *ransomware* ini, peretas pada umumnya akan mengancam bahwa data-data penting yang tersimpan di dalam

sistem dapat dihancurkan atau dijual apabila uang tebusan tidak segera dibayarkan.

5. *SPYWARE*

Spyware adalah perangkat lunak yang diinstal secara diam-diam oleh peretas dan digunakan untuk memantau perilaku online para korbannya. Dengan perangkat ini, peretas dapat mengetahui kebiasaan korban saat berselancar di internet seperti mengetahui tombol apa yang ditekan user, kata sandi, identitas pribadi, serta informasi sensitif yang dimiliki user secara online.

6. *ADWARE*

Adware merupakan jenis *malware* untuk menampilkan iklan pop-up yang tidak diinginkan di perangkat Anda. Program *adware* dapat mengubah tampilan *homepage browser*, menyuntikkan iklan jahat ke situs web sah, dan memicu jendela *pop-up* secara terus-menerus di web browser Anda.

Malware ini biasanya menginfeksi sistem Anda karena dua penyebab utama yaitu:

1. *Users* secara tidak sadar ketika menginstal aplikasi sah yang dibundel dengan adware di dalamnya.
2. Terdapat kerentanan di dalam perangkat lunak atau sistem operasi yang Anda gunakan. Kerentanan tersebut kemudian dieksploitasi oleh peretas untuk memasukan malware di dalamnya.

7. *FILELES MALWARE*

Fileless malware adalah jenis perangkat lunak berbahaya yang menggunakan program yang sah untuk menginfeksi komputer. *Malware* ini beroperasi dari memori komputer korban dan bukan dari file di hard drive. *Fileless malware* juga akan membonceng skrip yang sah dengan menjalankan aktivitas berbahaya sementara program yang sah terus berjalan. Dengan cara inilah, *fileless malware* tidak akan meninggalkan jejak sehingga sulit untuk dideteksi atau dihapus. [10]

[10] http://www.logique.co.id/blog/2021/07/15/apa-itu-malware/