PERTANGGUNGJAWABAN PIHAK BANK ATAS PERBUATAN MELAWAN HUKUM DALAM *E-TRANSACTION* DI BIDANG PERBANKAN

I. PERMASALAHAN YANG DIHADAPI

- Ppertanggungjawaban pihak bank atas perbuatan melawan hukum dalam *E-transaction* di bidang perbankan.
- Sejauh mana Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undnag Nomor 7 Tahun 1992 tentang Perbankan (untuk selanjutnya disebut **UU Perbankan**), Undang-Undang Nomor 11 Tahun 2009 tentang Informasi dan Transaksi Elektronik (untuk selanjutnya disebut **UU ITE**), dan Peraturan Bank Indonesia (untuk selanjutnya disebut **PBI**) mengakomodir perlindungan hukum yang dapat diberikan terhadap nasabah atas terjadinya perbuatan melawan hukum dalam *E-transaction* tersebut

II. BAHASAN

A. *E-Transaction* Dalam Perbankan

Transaksi Elektronik (*e-transaction*) dalam dunia perbankan erat kaitannya dengan *internet banking*. **Karen Furst** menjelaskan bahwa *internet banking* merupakan suatu bentuk pemanfaatan media internet oleh bank untuk mempromosikan dan sekaligus melakukan transaksi secara *on-line*, baik dari produk yang sifatnya konvensional maupun yang baru. Dengan adanya *internet banking* setiap nasabah mampu melakukan kegiatan transaksi elektronik setiap saat dengan mengaksesnya melalui *personal computer*, ponsel maupun media *wireless* lainnya.[1]

[1] Karen Furst, "*Internet Banking: Development and Prospects", Program on Information Resources Policy Harvard University,* April 2002, hlm.4

Sebagai dasar menciptakan sistem *internet banking* tersebut, lembaga keuangan bank harus menyediakan fasilitas layanan *internet banking* yang *real-time* dan *cross-channel view* dari semua informasi nasabah. Sehingga, lembaga keuangan bank dapat merespon dengan segera untuk setiap kontak atau transaksi dengan nasabah, memperbaiki layanan nasabah, membuka kesempatan keuntungan untuk penjualan secara silang, dan juga dengan layanan *internet banking* ini diharapkan lembaga keuangan mampu masuk pada generasi selanjutnya dari *retail banking.*[2]

Dalam pelaksanaan *internet banking*, terdapat beberapa potensi lubang atau bocornya keamanan (*security hole*) pada teknis pelaksanaan layanan *internet banking* itu sendiri. Pengguna menerima serangan berupa virus yang dapat menyadap, mengubah, menghapus, atau memalsukan data (PIN, nomor kartu kredit, dan kunci rahasia).[3] Selain itu, informasi dalam penyedia jasa layanan internet dapat disadap dan dipalsukan, sehingga penyadap dapat menerima informasi tentang pelanggan penyedia jasa layanan internet tersebut.

Dengan adanya kelemahan-kelemahan tersebut, diperlukan adanya upaya pengamanan terhadap layanan *internet banking.* Selain bentuk proteksi terhadap layanan itu sendiri, upaya pengamanan harus dilakukan dari segi regulasi. Dalam hal ini, Bank Indonesia telah menciptakan beberapa regulasi yang mengatur penyelenggaraan *internet banking* oleh bank pada umumnya sebagai berikut:

a. Surat Edaran Bank Indonesia Nomor 6/18/DPNP Tanggal 20 April 2004 Tentang Penerapan Manajemen Risiko Pada Aktivitas Pelayanan Jasa Bank Melalui Internet
b. Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum

---

[2] Budi Agus Riswandi, *Aspek Hukum Internet Banking,* Jakarta:PT Raja Grafindo Persada, 2005, hlm.20

[3] Budi Rahardjo, *Aspek Teknologi dan Keamanan Dalam Internet Banking,* materi Seminar "Internet Banking: Implementasi dan Tantangannya ke Depan", *Banking Research and Regulation Directorate,* Bank Indonesia, 13 Agustus 2001

c. Surat Edaran Bank Indonesia Nomor 9/30/DPNP Tanggal 12 Desember 2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum
d. Peraturan Bank Indonesia Nomor:11/12/PBI/2009 Tentang Uang Elektronik
e. Surat Edaran Bank Indonesia Nomor:11/11/DASP Tanggal 13 April 2009 Tentang Uang Elektronik

B. *E-Transaction* Menurut UU ITE

Pasal 1 angka 2 UU ITE memberi pengertian secara jelas terhadap Transaksi Elektronik, yaitu perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Penggunaan transaksi elektronik erat kaitannya dengan sistem elektronik, yang pengertiannya dijelaskan dalam Pasal 1 angka 5 UU ITE, yaitu merupakan serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektornik.

Dalam penyelenggaraan sistem elektronik, UU ITE mengatur juga mengenai perlindungan terhadap kepentingan pengguna *e-transaction* tersebut. Hal ini termaktub dalam Pasal 15 dan Pasal 16 ayat (1) sebagai berikut:

Pasal 15:

1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem elektronik secara andaldan amanan serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
2) Penyelengara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 16 ayat (1)

Sepanjang tidak ditentukan lain oleh undang-undnag tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

a. Dapat menampilkan kembali Informasi Elektronik dan.atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
b. Dapat melindungi ketersediaan, keutuhan, keotenttikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaran Sistem Elektronik tersebut;
c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Lebih lanjut, Pasal 19 UU ITE menyatakan bahwa para pihak yang melakukan transaksi elektronik harus menggunakan sistem elektronik yang disepakati. Hal ini guna meminimalisir sengketa yang terjadi dalam suatu *e-transaction.* Namun, apabila terjadi sengketa UU ITE mengatur alternatif penyelesaian sengketa sebagaimana diatur dalam Pasal 38 yang berbunyi:

1) Setiap orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan sistem elektronik dan/atau menggunakan teknologi informasi yang menimbulkan kerugian.
2) Masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan sistem elektronik dan/atau menggunakan teknologi informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan Peraturan Perundang-undangan.

Berdasarkan ketentuan di atas, UU ITE memperbolehkan masyarakat yang dirugikan untuk mengajukan gugatannya secara *class action.* Lebih lanjut, gugatan yang dapat dilakukan sesuai dengan peraturan perundang-undangan tersebut mempertegas bahwa ketentuan yang terdapat dalam KUHPerdata berlaku dalam transaksi elektronik. Selain penyelesaian gugatan perdata yang sesuai dengan hukum acara perdata tersebut, berdasarkan Pasal 39 ayat (2) UU ITE terlihat bahwa memungkinkan bagi para pihak untuk menyelesaikan sengketa melalui badan arbitrase atau lembaga penyelesaian sengketa alternatif lainnya.

C. Perbuatan Melawan Hukum Berdasarkan KUHPerdata

Permasalahan mengenai Perbuatan Melawan Hukum diatur secara eksplisit dalam Kitab Undang-Undnag Hukum Perdata (selanjutnya disebut sebagai **KUHPerdata**). Pada pasal 1365 dijelaskan bahwa:

> *"Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut."*

Melihat dari Pasal 1365 KUHPerdata tersebut, dapat diketahui bahwa terdapat unsur-unsur melawan hukum sebagai berikut:

1. Adanya perbuatan melawan hukum

Putusan *Arrest Hooge Raad* tanggal 31 Januari 1919 menjadi suatu tonggak penting yang memperluas pengertian perbuatan melawan hukum (*onrechtmatigedaad)*. Suatu perbuatan melawan hukum apabila perbuatan tersebut melanggar hak orang lain, bertentangan dengan kewajiban hukum si pelaku,

bertentangan dengan kesusilaan yang baik, atau bertentangan dengan kepatutan yang terdapat dalam masyarakat terhadap diri atau benda orang lain. Oleh karena itu, suatu *onrechtmatigedaad* tidak saja bertentangan dengan peraturan perundang-undangan, tetapi juga bertentangan dengan hukum tidak tertulis (kesusilaan dan kepatutan dalam masyarakat).

2. Adanya kesalahan

Pada dasarnya, akibat-akibat dari suatu perbuatan melawan hukum dapat dipertanggungjawabkan kepada pelakunya, dan hanya dalam beberapa hal saja terdapat pengecualian, maka penggugat tidak perlu membuktikan adanya kesalahan, akan tetapi tergugat yang mengemukakan bahwa dirinya tidak bersalah yang dibebani pembuktian.

3. Adanya kerugian

Dalam Pasal 1365 KUHPerdata, yang dimaksud dengan kerugian adalah kerugian yang ditimbulkan oleh perbuatan melawan hukum. Kerugian ini dapat bersifat harta kekayaan, umumnya meliputi kerugian yang diderita dan keuntungan yang seharusnya diperoleh, dan terdapat kerugian idiil yang meliputi sakit, luka, cacat, dsb.

4. Adanya hubungan sebab akibat

Dalam mengajukan gugatan ganti rugi berdasarkan perbuatan melawan hukum ini, harus terdapat hubungan sebab akibat antara perbuatan melawan hukum dengan kerugian yang ditimbulkannya. Dikatakan terdapat hubungan kausalitas apabila kerugian menurut pengalaman yang layak merupakan akibat yang dapat diharapkan akan timbul dari perbuatan melawan hukum.

D. Perbuatan Melawan Hukum Pada *E-Transaction* Dalam Aktivitas Perbankan

UU Perbankan tidak mengatur perbuatan melawan hukum dalam aktivitas perbankan. Namun, sebagaimana telah dijelaskan di poin sebelumnya, perbuatan

melawan hukum tidak saja perbuatan yang melanggar aturan yang terdapat dalam perundang-undangan. Perbuatan melawan hukum juga termasuk perbuatan yang bertentangan dengan norma-norma dalam masyarakat.

Pasal 2 UU Perbankan menyatakan bahwa "Perbankan Indonesia dalam melakukan usahanya berasaskan demokrasi ekonomi dengan menggunakan prinsip kehati-hatian". Hal ini penting untuk diterapkan dalam pelaksananan kegiatan demi meminimalisir risiko perbankan yang dapat terjadi. Bank harus mengerti dan mengenal risiko-risiko yang mungkin timbul dalam melaksanakan kegiatan usahanya, sehingga dapat mengetahui kapan risiko tersebut muncul untuk dapat mengambil tindakan yang tepat.[4]

Jika dikaitkan dengan kelemahan-kelemahan dalam *internet banking* yang telah dijelaskan sebelumnya, bank harus melakukan sistem pengamanan demi melindungi kepentingan semua pihak yang terlibat di dalamnya. Sistem pengamanan ini sangat penting karena secara teknis keutuhan informasi dan/atau sistem itu sendiri sangatlah rentan untuk tidak bekerja sebagaimana mestinya, dapat diubah atau diterobos oleh pihak yang bermaksud jahat (*intentional threats*) maupun oleh pihak yang tidak bermaksud jahat (*unintetional threats*).[5]

Menurut Turban, Rainer, dan Potter, *unintetional threats* dapat dikategorikan menjadi tiga hal, yaitu *human errors* (dalam hal kesalahan pemprograman oleh manusia), *enviromental hazards* (dalam hal bencana yang terjadi oleh lingkungan/alam), seerta *computer system failures* (seperti pengembangan *software* yang tidak kompatibel dengan sistem yang ada sehingga terhadi kesalahan produksi terhadap material-material yang digunakan). Untuk mencegah hal-hal tersebut, dibutuhkan strategi pertahanan yang mencakup kontrol fisik terhadap fasilitas komputer, akses komputer, serta melindungi atau membatasi akses terhadap sistem secara sebagian atau keseluruhan, kontrol terhadap

---

[4] Ferry N Idroes dan Sugiarto, *Manajemen Risiko Perbankan Dlam Konteks Kesepakatan Basel dan Peraturan Bank Indonesia,* Yogyakarta: Graha Ilmu, 2006, hlm. 6

[5] Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian,* Jakarta: PT Raja Grafindo Persada, 2005, hlm.105

pengamanan data, kontrol terhadap jaringan komunikasi, serta kontrol terhadap sistem administrasi. Kontrol ini akan menjadi dasar dalam mengukur apakah suatu sistem elektronik telah berjalan sebagaimana mestinya dan hal ini harus dilaksanakan dalam fungsi audit secara kontinu.[6]

Dalam membangun sistem elektronik, juga harus memperhatikan aspek hukum. Sejauhmana sistem elektronik ini aman, tidak hanya bergantung kepada sejauhmana potensi risiko dapat diminimaliskan, tapi juga bergantung kepada sejauhmana hal tersebut memenuhi kewajiban hukum. Pada saat sistem elektronik diluncurkan kepada publik, aspek pertanggungjawaban hukum harus menjadi perhatian utama dan sesuai dengan prinsip kehati-hatian. Hal ini sesuai dengan Pasal 3 UU ITE yang menyatakan sebagai berikut

> *"Pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi".*

Berdasarkan uraian yang telah dijelaskan sebelumnya dikaitkan dengan Pasal 3 UU TIE, apabila terdapat perbuatan yang melanggar prinsip penyelenggaraan sistem elektronik, hal tersebut dapat dikategorikan sebagai perbuatan melawan hukum.

III. PENYELESAIAN MASALAH

A. Bentuk Pertanggungjawaban Pihak Bank Atas Perbuatan Melawan Hukum Dalam *E-transaction* Di Bidang Perbankan.

Internet banking rentan terhadap masalah-masalah seperti yang telah dijelaskan sebelumnya. Masalah yang terjadi dalam *internet banking* tersebut dapat diakibatkan oleh kelalaian pegawai bank maupun disebabkan oleh kerusakan perangkat komputer yang menjadi dasar pelayanan transaksi elektronik tersebut. Pemanfaatan *e-transaction* dalam aktivitas perbankan yang menyebabkan kerugian terhadap nasabah menyebabkan adanya perbuatan melawan hukum

[6] *Ibid,* hlm. 107

sehingga nasabah dapat meminta ganti kerugian kepada pihak bank atas kerugian yang dideritanya.

Berkaitan dengan penyelenggaraan sistem atau teknologi informasi oleh bank pada umumnya, PBI Nomor 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum pada Pasal 2 disebutkan bahwa bank wajib menerapkan manajemen risiko secara efektif dalam penggunaan teknologi informasi. Dalam hal manajemen risiko ini, perlu diciptakan "*IT Strategic Plan*" atau rencana strategis teknologi informasi, yaitubank wajib melakukan langkah-langkah pengendalian untuk menghasilkan sistem yang terjaga kerahasiaannya dan integritasnya. Langkah-langkah pengendalian ini antara lain dengan cara:

1. Menetapkan dan menerapkan prosedur dan metodologi pengembangan dan pengadaan teknologi informasi secara konsisten;
2. Melakukan testing yang memadai pada saat pengembangan dan pengadaan suatu sistem, termasuk uji coba bersama satuan kerja pengguna, untuk memastikan keakuratan dan berfungsinya sistem sesuai kebutuhan pengguna serta kesesuaian satu sistem dengan sistem yang lain; dan
3. Melakukan dokumentasi sistem yang dikembangkan dan pemeliharaannya;

Hal ini bersesuaian dengan Pasal 12 ayat (1) PBI No. 9/15/PBI/2007 yang menyebutkan bahwa pihak bank wajib mengidentifikasi, memantau serta mengendalikan risiko yang terdapat pada aktivitas operasional teknologi informasi, pada jaringan komunikasi serta pada pengguna akhir (*end user computing*) untuk memastikan efektifitas, efisiensi, dan keamanan aktivitas tersebut dengan cara:

1. Menerapkan pengendalian fisik dan lingkungan terhadap fasilitas Pusat Data (*Data Center*) dan *Disaster Recovery Center*.[7]

[7] *Disaster Recovery Center* (DRC) merupakan fasilitas pengganti pada saat pusat data (data center) mengalami gangguan atau tidak dapat berfungsi antara lain karena tidak adanya aliran listrik ke ruang komputer, kebakaran, ledakan, atau keruskan pada komputer, yang digunakan

2. Menerapkan pengendalian hak akses secara memadai sesuai kewenangan ang ditetapkan
3. Menerapkan pengendalian pada saat input, proses, dan output dari informasi
4. Memperhatikan risiko yang mungkin timbul dari ketergantungan bank terhadap penggunaan jaringan komunikasi
5. Memastikan aspek desain dan pengoperasian dalam implementasi jaringan komunikasi sesuai dengan kebutuhan
6. Melakukan pemantauan kegiatan operasional teknologi informasi termasuk adanya *audit trail*
7. Melakukan pemantauan penggunaan aplikasi yang dikembangkan atau diadakan oleh satuan kerja di luar satuan kerja teknologi informasi.

Sehubungan dengan pelaksanaan dari layanan *internet banking* yang berbasis teknologi informasi tersebut, bank wajib memastikan *business contuinity plan*[8] dan *disaster recovery plan* dapat dilaksanakan secara efektif agar kegiatan usaha bank tetap dapat berjalan saat terjadi gangguan yang signifikan pada sarana teknologi informasi yang digunakan bank. Demi kepentingan hal tersebut, bank wajib melakukan uji coba atas *business continuity plan* dan *disaster recovery plan* terhadap seluruh sistem paling tidak sekali dalam setahun.

Dalam menyelenggarakan teknologi informasi yang menjadi basis dalam pelayanan *internet banking*, bank pada umumnya menyelenggarakan secara mandiri maupun menggunakan pihak ketiga. Pada dasarnya, pihak ketiga tersebut merupakan sebagai penyedia jasa teknologi informasi. Dalam hal ini, bank harus memastikan bahwa pihak ketiga ini juga menerapkan manajemen risiko yang bersesuaian dengan peraturan yang dikeluarkan Bank Indonesia.

---

sementara waktu selama dilakukannya pemulihan Pusat Data Bank untuk menjaga kelangsungan kegiatan usaha bank

[8] Business Continuity Plan (BCP) adalah kebijakan dan prosedur yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pengurangan risiko, penanganan dampak gangguan atau bencana dan proses pemulihan agar kegiatan operasional bank dan pelayanan kepada nasabah tetap dapat berjalan

Selain itu, pemanfaatan teknologi informasi ini juga tidak luput dari potensi risiko kegagalan sistem maupun *cybercrime* oleh orang tidak bertanggung jawab. Hal ini dapat merugikan nasabah dan menimbulkan pertanyaan pihak mana yang harus bertanggung jawab atas kejadian tersebut. Komputer yang merupakan sebuah alat tidak dapat dipersalahkan jika terjadi permasalahan di dalamnya, sehingga pertanggungjawaban meleka pada pihak yang menjalankan komponen tersebut atau pihak yang menyediakan jasa layanan. Namun, dalam hal tertentu yang wajib bertanggung jawab adalah pihak yang mengembangkan atau membuat komponen tersebut sekiranya terdapat cacat tersembunyi dalam program yang bersangkutan.

Dalam menentukan pertanggungajawaban atas kejadian tersebut, kita haus kaitkan permasalahan ini dengan dasar pokok aturan yang terdapat dalam PBI No.9/15/PBI/2007 mengenai kewajiban Bank Umum dalam menggunakan teknologi informasi untuk kegiatan perbankan sebagai berikut:

a. Bank (dalam hal ini Bank Umum) wajib menerapkan manajemen risiko secara efektif dalam penggunaan Teknologi Informasi.
b. Penerapan manajemen risiko harus dilakukan secara terintegrasi dalam setiap tahapan penggunaan Teknologi Informasi sejak proses perencanaan, pengadaan, pengembangan, operasional, pemeliharaan hinga penghentian dan penghapusan sumber daya Teknologi Informasi.
c. Penerapan manajemen risiko dalam penggunaan Teknologi Informasi oleh Bank wajib disesuaikan dengan tujuan, kebijakan usaha, ukuran dan kompleksitas usaha bank.
d. Bank wajib menetapkan wewenang dan tanggung jawab yang jelas pada setiap jenjang, jabatan yang terkait dengan penggunaan Teknologi Informasi.
e. Bank wajib memiliki Komite Pengarah Teknologi Informasi (*Information Technology Steering Committee*). Komite ini bertanggung jawab memberikan rekomenasi kepada Direksi.
f. Bank wajib memiliki kebijakan dan prosedur penggunaan Teknologi Informasi.

g. Bank wajib menetapkan limit risiko yang dapat ditoleransi untuk dapat memastikan aspek-aspek terkait Teknologi Informasi berjalan dengan optimal.
h. Bank wajib memiliki Rencana Strategis Teknologi Informasi (*Information Technology Strategic Plan*) yang mendukung rencana strategis kegiatan usaha Bank, dimana Rencana Strategis Teknologi Informasi ini dijabarkan dalam Rencana Bisnis Bank.
i. Bank wajib melakukan proses manajemen risiko yang mencakup identifikasi, pengukuran, pemantauan dan pengendalian atas risiko terkait penggunaan Teknologi Informasi. Dalam hal Bank menggunakan jasa pihak lain untuk menyelengarakan Teknologi Informasi, Bank wajib memastikan bahwa pihak penyedia jasa Teknologi Informasi menerapkan juga manajemen risiko yan paling kurang sesuai dengan ketentuan dalam Peraturan Bank Indonesia ini.

Selain yang diatur di dalam PBI tersebut, UU ITE juga mengatur terkait penyelenggaraan sistem elektronik yang aman dan dapat melindungi kepentingan penggunanya sebagaimana tertera dalam Pasal 15 dan Pasal 16 ayat (1) sebagai berikut:

Pasal 15:

4) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem elektronik secara andaldan amanan serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
5) Penyelengara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
6) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 16 ayat (1)

Sepanjang tidak ditentukan lain oleh undang-undnag tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

f. Dapat menampilkan kembali Informasi Elektronik dan.atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
g. Dapat melindungi ketersediaan, keutuhan, keotenttikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaran Sistem Elektronik tersebut;
h. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
i. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
j. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Adanya kewajiban bagi pihak bank dan/atau pihak penyedia jasa teknologi indormasi yang harus dipenuhi dalam menyelenggarakan suatu sistem elektronik perbankan yang menjadi basis dari layanan *internet banking* menyebabkan jika terjadi kerusakan sistem elektronik pada layanan terebut yang disebabkan oleh pihak bank maupun pihak penyedia jasa teknologi informasi, menyebabkan nasabah dapat meminta pertanggungjawaban pihak bank atas kerugian yang dideritanya atas dasar Perbuatan Melawan Hukum.

Terjadinya kerusakan sistem elektronik pada layanan *internet banking* ini telah memenuhi unsur-unsur perbuatan hukum karena tidak dilaksanakannya kewajiban-kewajiban oleh pihak bank dan/atau penyedia jasa teknologi informasi

dalam penyelenggaraan sistem elektronik perbankan dan merupakan perbuatan yang melanggar ketentuan PBI No.9/15/PBI/2007 dan ketentuan dalam Pasal 15 serta Pasal 16 ayat (1) Undang-Undang ITE. Kelalaian pihak bank dan/atau penyedia jasa teknologi informasi tersebut memenuhi unsur kesalahan yang menimbulkan kerugian bagi nasabah pengguna layanan *internet banking*. Oleh karenanya, dengan terpenuhinya unsur-unsur dari Perbuatan Melawan Hukum tersebut, nasabah dapat meminta pertanggungjawaban pihak bank atas dasar Pasal 1365 KUHPerdata. Hal ini dikecualikan dalam hal perbuatan melawan hukum terjadi akibat karyawan bank yang bersangkutan, sebagaimana disebutkan dalam Pasal 1367 ayat (3) KUHPerdata sebagai berikut:

> "*Majikan-majikan dan mereka yang mengangkat orang-orang lain untuk mewakili urusan-urusan mereka, bertanggungjawab atas kerugian yang disebabkan olep pelayan-pelayan atau bawahan-bawahan mereka dalam melakukan pekerjaan yang ditugaskan kepada orang-orang itu."*

Selanjutnya dalam Pasal 1367 ayat (5) KUHPerdata disebutkan bahwa tanggungjawab tersebut berakhir jika majikan dapat membuktikan bahwa mereka tidak dapat mencegah perbuatan itu atas mana mereka seharusnya bertanggung jawab. Sehingga apabila bank dapat membuktikan bahwa mereka telah melakukan segala upaya untuk mencegah terjadinya kesalahan dalam pelaksanaan layanan *internet banking,* terutama yang berkenaan dengan penerapan prinsip kehati-hatian dan manajemen risiko perbankan, serta dapat juga membuktikan bahwa kesalahan yang dilakukan oleh petugas bank tersebut adalah merupakan kesalahan yang berada di luar kekuasaan pihak bank, maka bank tersebut tidak dapat dimintakan pertanggungjawaban.

Sebagaimana dijelaskan sebelumnya, bank dalam menyelenggarakan *internet banking* menggunakan bantuan pihak ketiga selaku penyedia jasa teknologi informasi. Dalam hal terjadi kerusakan komponen penyelenggara *internet banking* disebabkan oleh pihak ketiga tersebut, maka pertanggungjawaban terhadap penyedia jasa teknologi informasi dapat berdasarkan hukum perjanjian. Hal ini dikarenakan penggunaan pihak penyedia jasa teknologi informasi oleh bank tersebut didasarkan pada perjanjian tertulis yang antara lain berisi kesediaan pihak

penyedia jasa teknologi informasi untuk melaksanakan prinsip kehati-hatian dan manajemen risiko sebagaimana diatur dalam PBI No.9/15/PBI/2007. Tidak dilaksanakannya prinsip kehati-hatian tersebut menyebabkan penyedia jasa teknologi informasi telah melanggar perjanjiannya terhadap bank, dan pihak bank dapat melakukan gugatan terhadap pihak ketiga tersebut atas dasar wanprestasi.

IV. KESIMPULAN

Dalam hal *e-transaction*, khususnya dalam aktivitas perbankan biasa digunakan istilah *internet banking*, terdapat beberapa kelemahan dalam penyelenggaraan sistem informasi tersebut sehingga dapat menimbulkan kerugian pada nasabah bank. Hal ini bisa disebabkan karena kesalahan sistem atau kelalaian pihak terkait. Terpenuhinya unsur perbuatan melawan hukum akibat kelalaian atau kesalahan sistem tersebut menyebabkan nasabah pengguna layanan *internet banking* yang mengalami kerugian dapat melakukan gugatan terhadap pihak bank. Dalam hal ini, pihak bank wajib bertanggungjawab dikarenakan terlanggarnya kewajiban pihak bank untuk menerapkan prinsip kehati-hatian serta manajemen risiko perbankan sebagaimana diakomodir PBI No.9/15/PBI/2007.