

## **BAB IV**

### **HASIL PENELITIAN DAN ANALISIS**

#### **A. Perlindungan Hukum terhadap Nasabah Pengguna Layanan *Internet Banking* pada Bank BRI Cabang Cilacap**

Transparansi informasi produk jasa layanan *internet banking* yaitu hal yang krusial karena merupakan dasar bagi pelaksanaan hak-hak untuk memilih produk. Hal yang sering menjadi keluhan nasabah selaku konsumen bahwa mereka kurang mendapatkan informasi lengkap dan jelas pada awal melakukan perjanjian penggunaan jasa layanan bank. Dalam memberikan standar penerapan prinsip transparansi informasi produk termasuk jasa layanan *internet banking*, setiap bank pada dasarnya telah memiliki kebijakan dan prosedur sebagaimana yang diatur dalam Peraturan Bank Indonesia.

Setiap layanan perbankan terdapat kendala yang dihadapi oleh nasabah selaku pengguna layanan jasa perbankan, namun beberapa nasabah pada Bank BRI Cabang Cilacap tidak mempersoalkan kendala yang menyebabkan kerugian yang dialami dari penggunaan jasa layanan *internet banking*, hal ini dikarenakan :<sup>1</sup>

1. Kelemahan nasabah dalam segi pembuktian karena nasabah tidak menguasai teknologi transaksi *internet banking*.
2. Kurangnya pengetahuan nasabah untuk menuntut haknya ke pihak bank.

---

<sup>1</sup> Endah Citra, dalam wawancara dengan narasumber di Bank BRI Cabang Cilacap, 22 Desember 2017. Ijin mengutip telah diberikan.

3. Waktu yang lama dan biaya perkara di pengadilan yang tidak sebanding dengan uang nasabah yang hilang ketika bertransaksi melalui layanan *internet banking*.

Pelaksanaan terhadap pemenuhan hak untuk memperoleh informasi layanan *internet banking* dimaksudkan supaya nasabah mendapatkan pengetahuan yang diperlukan agar terhindar dari kerugian akibat penggunaan layanan *internet banking* secara tidak tepat. Dalam memberikan informasi terdapat banyak cara yang dapat dilakukan oleh bank yaitu dengan media brosur, iklan, media situs, maupun *website* bank.

Dalam kasus produk *internet banking*, hak atas informasi yang benar dan jelas agar nasabah dapat mendapatkan gambaran secara utuh mengenai produk *internet banking*. Hak atas informasi tersebut mengenai jenis produk, manfaat dan risiko, persyaratan dan tata cara penggunaan, biaya-biaya, dan jangka waktu berlakunya produk. Jika terdapat perubahan, penambahan, dan/atau pengurangan pada karakteristik produk, bank harus memberitahukan sebelum berlakunya perubahan, penambahan, dan/atau pengurangan pada karakteristik produk tersebut.

Dari hasil penelitian yang dilakukan penulis pada Bank BRI Cabang Cilacap, dapat disimpulkan bahwa terdapat 2 (dua) bentuk usaha perlindungan hukum yang dijalankan oleh Bank BRI Cabang Cilacap terhadap nasabah pengguna layanan *internet banking* dalam rangka melakukan transaksi perbankan yaitu :<sup>2</sup>

---

<sup>2</sup> Wasis Pitono, dalam wawancara dengan narasumber di Bank BRI Cabang Cilacap, 22 Desember 2017. Ijin mengutip telah diberikan.

## 1. Perlindungan preventif

Perlindungan preventif yaitu perlindungan yang dilakukan sebelum terjadinya kejahatan *e-banking* dan ditujukan agar kejahatan tersebut tidak dialami oleh para nasabahnya. Beberapa perlindungan preventif yaitu :

### a. Kebijakan privasi

Kebijakan privasi yaitu kebijakan untuk tidak menjual, memperlihatkan atau menukar segala informasi yang berhubungan dengan nasabah atau pengunjung situs dan *internet banking* BRI. Segala transaksi dan informasi rekening nasabah disimpan secara rahasia sesuai dengan ketentuan hukum yang berlaku serta sesuai dengan kebijakan *internet banking* BRI. Ketentuan hukum yang mengatur tentang rahasia nasabah diantaranya yaitu Pasal 40 ayat (1) dan ayat (2) Undang-Undang tentang Perbankan yang menyatakan bahwa :<sup>3</sup>

(1) Bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A.

(2) Ketentuan sebagaimana dimaksud dalam ayat (1) berlaku pula bagi pihak terafiliasi.

Peraturan tersebut merupakan penerapan dari asas kerahasiaan dimana bank wajib merahasiakan keterangan mengenai nasabah penyimpan beserta

---

<sup>3</sup> Pasal 40 ayat (1) dan ayat (2) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

simpanannya, keterangan yang dimaksud yaitu setiap data yang telah diberikan oleh pihak untuk bank. Tujuan peraturan tersebut yaitu supaya keterangan yang diberikan nasabah tidak dipergunakan untuk tindak kejahatan, dalam hal ini *e-banking* karena bisa saja dengan bocornya informasi tersebut pelaku tindak kejahatan *e-banking* akan menggunakan untuk memasuki *account* nasabah, karena tidak jarang *PIN code*, *password* berasal dari data pribadi nasabah seperti tanggal lahir, nama orang tua, dan lain-lain.

b. Sistem pengamanan

BRI menggunakan 3 (tiga) lapis sistem pengamanan untuk melindungi akses dan transaksi nasabahnya yaitu :

1) *Secure Socket Layer (SSL)*

*Secure Socket Layer (SSL)* yaitu teknologi pengamanan yang mengacak jalur antar komputer sehingga tidak dapat dibaca oleh pihak bank lain.

2) *User id, password, dan PIN code*

*User id* yaitu identitas yang dimiliki oleh nasabah pengguna layanan BRI Internet, *user id* harus dicantumkan oleh nasabah setiap kali akan memulai penggunaan BRI Internet. *PIN code* yaitu nomor identifikasi pribadi yang bersifat rahasia yang hanya diketahui oleh nasabah pengguna dan harus diinput atau dicantumkan pada saat memulai penggunaan BRI *e-banking*. Pada saat pembukaan awal rekening nasabah akan diberikan kartu ATM dan langsung diminta untuk segera

menginput PIN *code* dengan cara nasabah akan menginput nomor PIN *code* melalui mesin *Electronic Data Capture* (EDC) yang ada pada *teller* BRI, dalam pembuatan nomor PIN *code* nasabah tidak diperbolehkan untuk menginput nomor yang sama atau menginput nomor sesuai dengan tanggal lahir, jika nasabah menginput nomor tersebut untuk dijadikan PIN *code* maka secara otomatis sistem akan menolak dan nasabah diminta untuk kembali membuat PIN *code* yang mudah diingat tetapi tidak mudah ditebak oleh orang lain. Selain itu, kombinasi yang digunakan dalam BRI untuk PIN *code* adalah 6 (enam) digit karena jika PIN *code* terdiri dari 6 (enam) digit angka yang berbeda akan sangat susah ditebak kombinasinya jika dibandingkan dengan yang hanya menggunakan 4 (empat) digit angka untuk PIN *code*. Penggunaan PIN *code* bertujuan untuk membuktikan bahwa nasabah yang menggunakan yaitu nasabah yang berhak atas layanan BRI *e-banking*, misalnya dalam penggunaan *internet banking*, maka nasabah akan diminta untuk menginput nomor PIN *code* nasabah juga hanya diperkenankan untuk mengulang PIN *code* yang salah sebanyak 3 (tiga) kali sebelum akses diblokir untuk mencegah penyalahgunaan yang tidak bertanggung jawab.

### 3) *M-Token* BRI

*M-Token* BRI yaitu teknologi pengamanan tambahan yang selalu menghasilkan *password* yang berbeda setiap kali digunakan. *M-Token*

BRI menggunakan media handphone untuk setiap pengiriman kode *M-Token*. Nasabah diwajibkan untuk memasukkan kode *M-Token* BRI jika ingin melakukan transaksi finansial yang bertujuan untuk mengotentikasi setiap transaksi finansial yang dilakukan oleh nasabah dan sebagai tanda persetujuan nasabah terhadap transaksi yang dilakukan.

c. Proteksi komunikasi *internet banking* BRI

BRI menggunakan teknologi enkripsi *Secure Socket Layer* (SSL) 256 bit untuk memproteksi komunikasi antara komputer nasabah dengan *server* milik BRI selama nasabah mengakses *internet banking* BRI. Selain itu juga menggunakan sistem *auto log off* yang merupakan sistem yang akan menutup secara otomatis dalam kurun waktu yang telah ditentukan. Penerapan sistem *auto log off* yaitu ketika tidak terdapat aktivitas lagi selama 10 (sepuluh) menit, maka sistem akan secara otomatis akan mengakhiri atau *log out*.

d. Proteksi akses *internet banking*

BRI mewajibkan nasabah untuk memasukkan *user id* dan *password* sebelum melakukan akses *internet banking*. Tujuan penggunaan *user id* dan *password* untuk membuktikan bahwa nasabah yang menggunakan yaitu nasabah yang berhak atas layanan *internet banking* BRI, setiap kali *log in* nasabah hanya diperkenankan untuk mengulang *user id* dan *password* yang

salah sebanyak 3 (tiga) kali sebelum akses diblokir untuk mencegah penyalahgunaan yang tidak bertanggung jawab.

## 2. Perlindungan represif

Perlindungan represif yaitu perlindungan yang bertujuan untuk mendapat jaminan santunan hukum atas penderitaan atau kerugian yang diperoleh.

Beberapa perlindungan represif yaitu :

### a. Menyediakan layanan pengaduan atau *call center* 14017

*Call center* dihubungi oleh nasabah jika terjadi ketidakpuasaan atau kerugian finansial yang diduga karena kesalahan atau kelalaian pihak bank. Nasabah yang terkena kejahatan *e-banking* dapat menghubungi layanan *call center* dan pihak BRI akan menindaklanjuti pengaduan nasabah tersebut. Layanan pengaduan dilakukan oleh pihak BRI yaitu sebagai wujud implementasi dari Surat Edaran Otoritas Jasa Keuangan Nomor 2/SEOJK.07/2014 tentang Pelayanan dan Penyelesaian Pengaduan Konsumen pada Pelaku Usaha Jasa Keuangan. Surat Edaran tersebut diterbitkan merupakan peraturan pelaksana dari Pasal 32 sampai dengan Pasal 39 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Jasa Keuangan. Pengadaan unit pengaduan konsumen atau nasabah selaras dengan hak yang diperoleh nasabah yang diatur dalam Undang-Undang tentang Perlindungan Konsumen. Pasal 4 huruf d menyatakan bahwa konsumen berhak untuk didengar pendapat dan

keluhannya atas barang dan/atau jasa yang digunakan.<sup>4</sup> Berdasarkan kedua ketentuan di atas, maka BRI mempunyai kewajiban untuk menerima setiap pengaduan yang diajukan oleh nasabah dan bank wajib menyelesaikan pengaduan tersebut selama paling lambat 20 (dua puluh) hari kerja dan dapat diperpanjang 20 (dua puluh) hari. Ketentuan tersebut merupakan pelaksanaan dari Surat Edaran Otoritas Jasa Keuangan Nomor 2/SEOJK.07/2014 tentang Pelayanan dan Penyelesaian Pengaduan Konsumen pada Pelaku Usaha Jasa Keuangan yang menyatakan bahwa pelaku usaha jasa keuangan wajib segera menindaklanjuti dan menyelesaikan pengaduan paling lambat 20 (dua puluh) hari kerja setelah tanggal penerimaan pengaduan.<sup>5</sup> Dalam hal kondisi tertentu, pelaku usaha jasa keuangan dapat memperpanjang jangka waktu sampai dengan paling lama 20 (dua puluh) hari kerja berikutnya.

Pihak Bank BRI akan membantu menyelesaikan masalah yang telah disampaikan pada pelayanan pengaduan dan/atau memberikan ganti kerugian sesuai dengan ketentuan yang telah diperjanjikan. Unit pengaduan nasabah sebagai salah satu upaya perlindungan hukum secara represif serta menjadi bentuk pertanggungjawaban yang dilakukan oleh Bank BRI.

b. Sanksi atas dilarangnya kebijakan privasi

---

<sup>4</sup> Pasal 4 huruf d Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

<sup>5</sup> Surat Edaran Otoritas Jasa Keuangan Nomor 2/SEOJK.07/2014 tentang Pelayanan dan Penyelesaian Pengaduan Konsumen pada Pelaku Usaha Jasa Keuangan.

Tujuan diberikannya sanksi jika ada pihak yang membuka data nasabah dan tidak dapat merahasiakan data nasabah terkena hukuman yang sesuai agar tidak melakukannya kembali atau menimbulkan efek jera bagi pelaku, karena menjaga kerahasiaan mengenai data nasabah merupakan suatu hal yang penting untuk mengurangi potensi terjadinya kejahatan *e-banking*, khususnya kejahatan pada *internet banking*. Ketentuan yang mengatur adanya sanksi atas dilarangnya kebijakan privasi yaitu Pasal 47 ayat (1) dan ayat (2) Undang-Undang tentang Perbankan yang menyatakan bahwa :<sup>6</sup>

- (1) Barang siapa tanpa membawa perintah tertulis atau izin dari pemimpin Bank Indonesia sebagaimana dimaksud dalam Pasal 41, Pasal 41A, dan Pasal 42A, dengan sengaja memaksa pihak bank atau pihak terafiliasi untuk memberikan keterangan sebagaimana dimaksud dalam Pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun serta denda sekurang-kurangnya Rp 10.000.000.000,00 (sepuluh miliar rupiah) dan paling banyak Rp 200.000.000.000,00 (dua ratus miliar rupiah).
- (2) Anggota dewan komisaris, direksi, pegawai bank atau pihak terafiliasi lainnya yang dengan sengaja memberikan keterangan yang wajib dirahasiakan menurut Pasal 40 diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun

---

<sup>6</sup> Pasal 47 ayat (1) dan ayat (2) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

serta denda sekurang-kurangnya Rp 4.000.000.000,00 (empat miliar rupiah).

Penerapan sistem kemanan yang dilakukan BRI selaras dengan pemenuhan hak dari konsumen dalam hal ini nasabah yang diatur dalam Pasal 4 huruf a Undang-Undang tentang Perlindungan Konsumen yang menyatakan bahwa konsumen berhak memperoleh kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa.<sup>7</sup> Sistem kemanan yang dilakukan juga sesuai dengan ketentuan yang diatur dalam Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Dalam peraturan tersebut dijelaskan bahwa bank yang menyelenggarakan kegiatan *e-banking* wajib memenuhi ketentuan Bank Indonesia yang berlaku. Penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank sesuai dengan tujuan, kebijakan usaha, ukuran, dan kompleksitas usaha bank. Kewajiban yang diatur dalam peraturan tersebut juga selaras dengan kewajiban yang diatur dalam Undang-Undang tentang Perlindungan Konsumen. Pasal 7 huruf d Undang-Undang tentang Perlindungan Konsumen menyatakan bahwa pelaku usaha berkewajiban untuk menjamin mutu barang dan/atau jasa yang diproduksi dan/atau

---

<sup>7</sup> Pasal 4 huruf a Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

diperdagangkan berdasarkan ketentuan standar mutu barang dan/atau jasa yang berlaku.<sup>8</sup>

Dari kasus yang terjadi terkait penyalahgunaan *internet banking* pada Bank BRI Cabang Cilacap adanya bentuk pertanggungjawaban terhadap nasabah yaitu sesuai dengan Pasal 7 huruf f Undang-Undang tentang Perlindungan Konsumen bahwa kewajiban pelaku usaha adalah memberikan kompensasi, ganti rugi, dan/atau penggantian atas kerugian akibat penggunaan, pemakaian, dan pemanfaatan barang dan/atau jasa yang diperdagangkan.<sup>9</sup> Pertanggungjawaban yang dilakukan bank mempunyai batasan-batasan sesuai dengan ketentuan perjanjian yang telah dilakukan sebelumnya, dimana dalam perjanjian tersebut terdapat ketentuan yaitu :

1. Segala penyalahgunaan *user id* atau *password internet banking* BRI (termasuk *M-Token*) merupakan tanggung jawab nasabah pengguna. Nasabah pengguna membebaskan BRI dari segala tuntutan apapun yang mungkin timbul, baik dari pihak lain maupun nasabah pengguna sendiri sebagai akibat penyalahgunaan *user id* atau *password internet banking* BRI.
2. Nasabah pengguna akan membebaskan BRI dari segala tuntutan apapun, dalam hal BRI tidak dapat melaksanakan perintah dari nasabah pengguna baik sebagian maupun seluruhnya karena kejadian-kejadian atau sebab-sebab di

---

<sup>8</sup> Pasal 7 huruf d Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

<sup>9</sup> Pasal 7 huruf f Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

luar kekuasaan atau kemampuan BRI namun tidak terbatas pada segala gangguan virus komputer atau sistem *trojan horses* atau komponen membahayakan yang dapat mengganggu layanan *internet banking* BRI, *web browser* atau komputer sistem BRI, nasabah pengguna atau *Internet Service Provider* (ISP) karena bencana alam, perang, huru-hura, keadaan peralatan, sistem atau transmisi yang tidak berfungsi, gangguan listrik, gangguan telekomunikasi, kebijakan pemerintah, serta kejadian atau sebab lain di luar kekuasaan atau kemampuan BRI.

Pembatasan pertanggungjawaban telah sesuai dengan Pasal 21 ayat (2) Undang-Undang tentang ITE mengenai pihak yang bertanggung jawab atas segala akibat hukum dalam transaksi elektronik. Pasal 21 ayat (2) Undang-Undang tentang ITE menyatakan bahwa pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik sebagaimana dimaksud pada ayat (1) yaitu :<sup>10</sup>

1. Jika dilakukan sendiri maka segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab yang melakukan transaksi.
2. Jika dilakukan melalui pemberi kuasa maka segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab pemberi kuasa.
3. Jika dilakukan melalui agen elektronik maka segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab penyelenggara agen elektronik.

---

<sup>10</sup> Pasal 21 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasal 21 Undang-Undang tentang ITE menyatakan bahwa jika kerugian transaksi elektronik disebabkan gagal beroperasinya agen elektronik akibat kelalaian pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.<sup>11</sup> Agen elektronik berdasarkan Pasal 2 angka 8 yaitu perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik secara otomatis yang diselenggarakan oleh seseorang.<sup>12</sup> Klausula baku dalam perjanjian *e-banking* mengenai pembatasan pertanggungjawaban di atas sudah sesuai dengan ketentuan dalam Undang-Undang tentang ITE. Meskipun perjanjian baku yang mencantumkan adanya klausula baku terkait pengalihan tanggung jawab tidak dibenarkan berdasarkan Pasal 18 Undang-Undang tentang ITE, namun dalam hal ini dapat dibenarkan karena klausula tersebut dibuat untuk perjanjian *e-banking*. Undang-Undang tentang ITE termasuk undang-undang khusus untuk teknologi dan dapat dibenarkan berdasarkan asas *lex specialis derogat legi generalis*. *Lex specialis derogat legi generalis* yaitu salah satu asas hukum yang mengandung makna bahwa aturan hukum yang khusus akan mengesampingkan aturan hukum yang umum. Adanya peraturan tersebut sebagai suatu bentuk menyeimbangkan kedudukan antara pihak nasabah dengan bank yang bersangkutan dalam hal terjadinya suatu risiko kerugian dikemudian hari, dapat dikatakan juga dengan adanya peraturan tersebut bahwa nasabah maupun bank

---

<sup>11</sup> Pasal 21 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

<sup>12</sup> Pasal 2 angka 8 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

haknya dapat dilindungi. Tanggung jawab perdata atas kesalahan atau kelalaian yang terjadi pada bank dapat dihubungkan dengan kepentingan bank tersebut. Pengurus bank adalah pihak yang bertindak mewakili badan hukum bank berdasarkan ketentuan anggaran dasar perusahaan, maka terdapat 2 (dua) bentuk tanggung jawab pengurus terhadap perbuatannya yaitu :<sup>13</sup>

1. Tanggung jawab pribadi

Menjadi tanggung jawab pribadi apabila pengurus bertindak di luar kewenangan yang telah ditentukan dalam anggaran dasar perusahaan sewaktu pemberian kuasa perwakilan tersebut. Bentuk tanggung jawab ini yang dilakukan BRI terhadap pengaduan yang dilakukan nasabah yang mengalami kerugian akibat kejahatan *e-banking*, khususnya dalam penyalahgunaan *internet banking* yaitu dengan melakukan *complain handling*. *Complain handling* termasuk implementasi dari Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Jasa Keuangan sebagai upaya perlindungan hukum terhadap nasabah. Adanya *complain handling* yang dilakukan maka BRI memiliki itikad baik untuk mendengarkan keluhan nasabah, walaupun kerugian nasabah dalam penyalahgunaan *internet banking* belum tentu akibat kesalahan dari pihak bank. BRI dalam melakukan *complain handling* terhadap keluhan nasabah khususnya terhadap kerugian transaksi

---

<sup>13</sup> Arie Prihandoko, dalam wawancara dengan narasumber di Bank BRI Cabang Cilacap, 22 Desember 2017. Ijin mengutip telah diberikan.

*internet banking* yang diakibatkan karena penyalahgunaan *internet banking* sudah mempunyai SOP, SOP tersebut berfungsi sebagai pedoman alur kerja dalam menangani pengaduan dimana dalam SOP tersebut salah satunya menjelaskan bahwa lama penyelesaian pengaduan tersebut selama 40 (empat puluh) hari. Dengan adanya SOP, nasabah mendapat kepastian jangka waktu untuk mendapatkan penyelesaian keluhan atas kerugian yang dialami. Lama jangka waktu diukur berdasarkan tingkat kesulitan kasus dan kerugian yang dialami oleh nasabah. Keluhan nasabah bisa disampaikan melalui *call center* BRI dengan menelpon nomor 14017, jika sudah tersambung maka pihak BRI akan menanyakan data nasabah. Setelah data telah sesuai, maka pihak nasabah diperkenankan untuk menjelaskan keluhannya. Setelah itu nasabah akan mendapatkan nomor registrasi pengaduan yang dapat digunakan untuk melihat perkembangan penyelesaian pengaduan di kantor BRI atau *call center* BRI. Nasabah yang hendak menyampaikan pengaduan terkait kasus seperti penyalahgunaan internet banking diwajibkan untuk melaporkan terlebih dahulu kepada kepolisian. Setelah memperoleh Surat Keterangan dari polisi maka BRI dapat memproses pengaduan tersebut. Tindakan yang akan dilakukan BRI sebelum nasabah memperoleh Surat Keterangan dari polisi yaitu melakukan pemblokiran rekening milik nasabah dan milik seseorang yang diduga merupakan pelaku dari penyalahgunaan *internet banking*. Hal ini dilakukan agar tidak menimbulkan korban lain, namun apabila dalam jangka waktu 1 x 24 jam nasabah tidak menyampaikan Surat Keterangan dari kepolisian kepada

bank maka bank diperkenankan untuk membuka pemblokiran. Namun apabila Surat Keterangan telah diterima bank, maka bank wajib melakukan pemblokiran atas rekening sesuai dengan ketentuan hukum yang berlaku. Pengaduan nasabah tersebut kemudian akan diteruskan ke divisi *complain* untuk ditindak lanjuti dan diidentifikasi oleh bank apakah kerugian tersebut disebabkan bank atau nasabah. Proses penyelesaian pengaduan selama 40 (empat puluh) hari kerja dan jika kerugian dikarenakan kelalaian atau kesalahan nasabah sendiri maka bank tidak akan memberi ganti rugi melainkan hanya memberi edukasi kepada nasabah agar tidak terjadi kembali, namun jika kerugian dikarenakan pihak bank atau pihak *intern* bank maka bank akan memberi ganti rugi kepada nasabah.

## 2. Tanggung jawab perusahaan

Menjadi tanggung jawab perusahaan apabila tindakan pengurus masih dalam pelaksanaan dan wewenang yang tertuang dalam anggaran dasar perusahaan. Bentuk pertanggungjawaban yang dilakukan BRI dalam hal kerugian disebabkan oleh kelalaian atau kesalahan bank yaitu melakukan upaya damai dalam menyelesaikan masalah tersebut. Upaya damai dilakukan secara kekeluargaan antara nasabah dengan bank yang dilakukan dengan cara mengkomunikasikan kepada nasabah untuk mencari penyelesaian yang tidak merugikan bagi BRI dan nasabah. BRI selalu mengusahakan supaya penyelesaian secara kekeluargaan dan damai karena jika harus sampai ke tahap selanjutnya maka proses akan lebih panjang dan menyita waktu serta bank

terkena risiko penurunan reputasi apabila nasabah tidak merasa puas dengan pelayanan BRI. Penyelesaian pengaduan atas kerugian nasabah maka nasabah dapat dilakukan sesuai dengan Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2014 tentang Lembaga Alternatif Penyelesaian Sengketa di Sektor Jasa Keuangan. Pasal 4 huruf a Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2014 tentang Lembaga Alternatif Penyelesaian Sengketa di Sektor Jasa Keuangan menjelaskan bahwa Lembaga Alternatif Penyelesaian Sengketa yang dimuat dalam Daftar Lembaga Alternatif Penyelesaian Sengketa yang ditetapkan oleh Otoritas Jasa Keuangan meliputi Lembaga Alternatif Penyelesaian Sengketa yang memiliki layanan penyelesaian sengketa paling kurang berupa mediasi, adjudikasi, dan arbitrase.<sup>14</sup> Apabila tidak menemukan penyelesai maka pihak bank dan nasabah dapat melanjutkan melalui proses pengadilan. Proses pengadilan sebagai cara terakhir dalam penyelesaian sengketa jika putusan pengadilan sudah mempunyai kekuatan hukum tetap maka para pihak wajib untuk menjalankan putusan yang telah ditetapkan.

## **B. Pembuktian Atas Transaksi Melalui *Internet Banking* pada Bank BRI Cabang Cilacap**

---

<sup>14</sup> Pasal 4 huruf a Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2014 tentang Lembaga Alternatif Penyelesaian Sengketa di Sektor Jasa Keuangan.

Berkembangnya penggunaan sarana elektronik dalam berbagai transaksi terutama bidang perbankan disamping memberi manfaat yang positif yaitu adanya kemudahan pelayanan kepada nasabah, juga memberikan manfaat yang besar bagi pihak perbankan khususnya dalam penyimpanan dokumen sebagai hasil kegiatan usaha yang dilakukan. Namun diakui juga dalam penggunaan sarana elektronik terdapat kekurangan atau kelemahan apabila dihadapkan pada masalah bukti di pengadilan.

Dalam hukum acara perdata sebagaimana diatur dalam Pasal 1866 Kitab Undang-Undang Hukum Perdata menjelaskan terkait macam-macam alat bukti yang meliputi bukti tertulis, bukti saksi, persangkaan, pengakuan, dan sumpah.<sup>15</sup> Bukti tertulis biasanya dalam bentuk tulisan diatas kertas yang bertanda tangan. Fungsi tanda tangan sebaga tanda bahwa orang yang menandatangani pada kertas tersebut mengetahui dan menyetujui terhadap isi dari apa yang tertulis pada kertas tersebut. Selain itu tanda tangan berfungsi untuk memberikan ciri atau mengindividualisir sebuah dokumen atau akta yang tertulis pada kertas. Dalam persoalan perdata alat bukti yang berbentuk tulisan merupakan alat bukti yang diutamakan jika dibandingkan dengan alat bukti lainnya.

Permasalahan akan timbul apabila sebuah perbuatan hukum berupa transaksi menggunakan sistem elektronik yang dalam hal ini berupa *internet banking*. Ketentuan mengenai penggunaan *internet banking* serta bukti bahwa telah terjadi

---

<sup>15</sup> Pasal 1866 Kitab Undang-Undang Hukum Perdata.

transaksi elektronik dengan menggunakan sarana elektronik tidak tertulis pada suatu kertas yang bertanda tangan melainkan tersimpan pada sarana elektronik dimana sistem kerja serta proses bertransaksi berbeda dengan transaksi pada umumnya. Dalam transaksi yang dilakukan secara konvensional yaitu suatu transaksi yang ditulis menggunakan kertas yang ditandatangani oleh para pihak, bukti transaksi dapat berupa kuitansi atau nota yang berfungsi sebagai alat bukti bahwa telah terjadi transaksi antara para pihak. Hal yang berbeda terjadi pada pola transaksi melalui media elektronik, ada sebagian transaksi elektronik yang ketika telah dilakukan suatu transaksi dapat dibuktikan melalui bukti transaksi yang tercetak pada suatu kertas yang dapat berfungsi sebagai alat bukti, sebagai contoh yaitu transaksi dilakukan melalui ATM, setelah transaksi dilakukan maka akan tercetak *receipt* yaitu bukti tertulis yang tercetak dari mesin ATM yang menunjukkan bahwa transaksi telah dilakukan. Berbeda halnya apabila nasabah bertransaksi melalui *internet banking*. Bukti transaksi atau *receipt* tidak dapat tercetak karena proses dalam bertransaksi dilakukan melalui telepon seluler. Pertanyaan muncul apakah bukti transaksi yang dilakukan melalui *internet banking* yaitu berupa pemberitahuan dari bank kepada nasabah dalam bentuk *SMS email* dapat dijadikan sebagai alat bukti.

Jika dalam transaksi secara konvensional otentifikasi suatu perjanjian, dokumen atau akta dapat dibuktikan dengan tanda tangan yang tertera dalam suatu kertas, berbeda halnya dalam setiap transaksi yang menggunakan sarana elektronik sebagai media untuk bertransaksi, keotentikan suatu perjanjian menggunakan

sarana elektronik dibuktikan melalui tanda tangan digital atau tanda tangan elektronik yang tentu saja fungsi tanda tangan sama dengan tanda tangan secara manual. Tanda tangan digital termasuk teknik *kriptografi* yaitu suatu sistem yang membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Di dalam teknik *kriptografi* terdapat apa yang disebut *enkripsi* yaitu proses mengamankan informasi sehingga informasi tersebut tidak dapat dibaca tanpa pengetahuan khusus. Pengetahuan khusus yang dimaksud yaitu pengidentifikasian tanda tangan digital apakah sesuai dengan tanda tangan pemilik yang berfungsi sebagai representasi dari pemilik tanda tangan digital tersebut sebagai nasabah Bank BRI Cabang Cilacap.

Menangani hal ini maka dapat dilandaskan berdasarkan ketentuan Pasal 5 ayat (1) Undang-Undang tentang ITE menyatakan bahwa informasi elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah.<sup>16</sup> Ketentuan dalam undang-undang tersebut diaplikasikan dalam bentuk perjanjian antara bank dengan nasabah dalam formulir aplikasi pembukaan rekening. Dalam ketentuan Formulir Aplikasi Pembukaan Rekening pada Bank BRI Cabang Cilacap menyatakan bahwa dokumen berupa catatan-catatan transaksi, surat-surat, serta dokumen lainnya yang disimpan dan dipelihara oleh bank secara tertulis di atas kertas atau media lain maupun rekaman yang dapat dilihat, dibaca ataupun didengar merupakan alat bukti yang sah dan lengkap atas transaksi yang dilaksanakan nasabah melalui fasilitas

---

<sup>16</sup> Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

*electronic channel*.<sup>17</sup> *Electronic channel* atau yang disebut *e-channel* yaitu suatu jalur pengiriman informasi dengan menggunakan sarana elektronik. Ketentuan yang lebih spesifik mengenai transaksi melalui *internet banking* dinyatakan dalam Pernyataan Legal Aktifasi yang dilakukan ketika nasabah hendak melakukan registrasi *internet banking* pada Bank BRI Cabang Cilacap. Pada Pernyataan Legal Aktifasi menyatakan bahwa semua catatan elektronik transaksi yang dilakukan via *e-channel* merupakan bukti legal. Sebagai media untuk melakukan transaksi via *e-channel* Bank BRI merupakan sistem *core banking*. *Core banking* yaitu sistem yang berfungsi untuk menyimpan informasi mengenai rekening bank nasabah sekaligus melayani permintaan nasabah. Permintaan yang dilakukan nasabah yaitu berupa permintaan untuk melakukan transaksi melalui media elektronik. Jadi semua transaksi yang dilakukan nasabah menggunakan sarana *e-banking* melalui *internet banking* tersimpan dan terekam dalam sistem *core banking*. Sistem *core banking* pada Bank BRI Cabang Cilacap bernama *BRI ICONS (Integrated Centralized Online System)*. *BRI ICONS* ditempatkan diseluruh Cabang BRI serta BRI syariah di seluruh Indonesia. Semua catatan transaksi yang dilakukan melalui media elektronik tersimpan dan terekam dalam *BRI ICONS*. Bukti mengenai catatan hasil transaksi yang disimpan dalam *BRI ICONS* dapat ditunjukkan kepada nasabah yang bersangkutan apabila nasabah memerlukan informasi mengenai

---

<sup>17</sup> Formulir Aplikasi Pembukaan Rekening pada Bank BRI Cabang Cilacap.

transaksi yang telah dilakukan dengan menunjukkan *BRI Card* dan/atau kartu identitas yang telah didaftarkan sebagai penggunaan fasilitas *internet banking*.

Berdasarkan ketentuan di atas maka dapat disimpulkan bahwa pada saat nasabah melakukan transaksi elektronik melalui *internet banking* pada Bank BRI Cabang Cilacap segala sesuatu yang tersimpan dalam saran elektronik baik melalui pemberitahuan atau notifikasi dari Bank BRI kepada nasabah dalam bentuk *SMS email* maupun catatan hasil transaksi yang tersimpan dan terekam dalam sistem BRI merupakan alat bukti yang sah karena selain ditentukan dalam undang-undang, juga ditentukan dalam perjanjian antara nasabah dengan Bank BRI.

Ketentuan antara nasabah dengan bank menggunakan sarana elektronik mendasarkan pada asas kebebasan berkontrak. Ketentuan Pasal 1338 ayat (1) Kitab Undang-Undang Hukum Perdata yang menyatakan bahwa semua perjanjian dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya.<sup>18</sup> Asas kebebasan berkontrak tersebut tak terkecuali pada transaksi yang dilakukan secara elektronik berupa *internet banking* yang melibatkan nasabah dengan Bank BRI Cabang Cilacap. Suatu transaksi tidak dapat dibuktikan atas suatu transaksi. Pada transaksi elektronik keabsahan suatu ketentuan yang merupakan perjanjian antara nasabah dengan bank dibuktikan dengan tanda tangan digital. Keabsahan tanda tangan digital pada transaksi elektronik berupa *internet banking* melandaskan ketentuan Pasal 11 ayat (1) Undang-Undang tentang ITE yang menyatakan bahwa

---

<sup>18</sup> Pasal 1338 ayat (1) Kitab Undang-Undang Hukum Perdata.

tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut :<sup>19</sup>

1. Data pembuatan tanda tangan elektronik terkait hanya kepada penanda tangan.
2. Data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa penanda tangan.
3. Segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui.
4. Segala perubahan terhadap informasi elektronik tersebut setelah waktu penandatanganan dapat diketahui.
5. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangnya.
6. Terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap informasi elektronik terkait.

Penerapan tanda tangan digital pada *internet banking* diterapkan pada saat nasabah melakukan proses registrasi. Sebelum nasabah melakukan registrasi maka terlebih dahulu nasabah memasukkan nomor PIN. Nomor PIN itulah yang merupakan bentuk tanda tangan elektronik yang berfungsi sebagai ciri atau otentifikasi yang menunjukkan bahwa si penanda tangan menyetujui terhadap isi atas suatu akta atau dokumen. Selanjutnya pada saat transaksi menggunakan *internet banking* yang digunakan sebagai tanda tangan elektronik yaitu nomor PIN dan *M-*

---

<sup>19</sup> Pasal 11 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

*token*. Dengan adanya tanda tangan berupa tanda tangan elektronik pada saat melakukan transaksi dengan menggunakan sarana *internet banking* menunjukkan bahwa transaksi yang dilakukan yaitu sah menurut hukum.