Dialogia Iuridica
Volume 10 Nomor 1, November 2018, p.001-015
Faculty of Law, Universitas Kristen Maranatha
ISSN: 2085-9945 | e-ISSN: 2579-3520
Nationally Accredited Journal by SINTA

Pertanggungjawaban Lembaga Perbankan terhadap Pencurian Data Nasabah

Lukmanul Hakim

Faculty of Law, Universitas Bandar Lampung

lukman517422@gmail.com

Submitted: 2018-05-30; Reviewed: 2018-09-06; Accepted: 2018-11-22

ABSTRACT

Cyber-crime is basically an impact of technological developments that have changed the habit of the community that was originally conventional into a more modern habits or can be called a high technology society. This change of habit has resulted in a crime with the use of electronic devices as a crime medium. The main factor that resulted in the switching of these habits is the development of information technology combined with communication media and computer technology, which then produces a new device called Internet. The emergence of the Internet has resulted in a new interaction pattern in the life of society, which initially more real (real) changed into patterns of interaction which can be said to be virtual.

Keywords: *Bank; Data Theft; Cyber*.

PENDAHULUAN

Perkembangan Teknologi saat ini khususnya dalam era globalisasi mengakibatkan daya dorong masyarakat untuk terus belajar akan kecanggihan teknologi yang ada. Hadirnya Teknologi ini pada akhirnya memudahkan masyarakat dengan mudah mendapatkan berbagai informasi yang diinginkan dengan cepat tanpa membutuhkan waktu yang lama. Untuk berkomunikasi dengan mudahnya dilakukan walaupun berada dalam tempat yang jauh sekalipun.

Kecanggihan alat informasi dan komunikasi setidaknya dapat mempermudah pekerjaan manusia. Banyak teknologi baru dengan berbagai inovasi bermunculan dengan harga yang semakin murah dan mudah didapatkan masyarakat seperti ponsel pintar, laptop, tablet yang semakin memudahkan masyarakat untuk saling berkomunikasi. Indonesia adalah salah satu negara di dunia yang sedang mengalami perkembangan. Salah satu ciri perkembangan ini adalah dengan banyaknya program

pembangunan di berbagai bidang kehidupan berbangsa, bernegara, dan bermasyarakat. Perkembangan tersebut diatas misalnya dapat dilihat dari perkembangan di bidang ilmu pengetahuan dan teknologi atau yang kita kenal dengan istilah Ilmu Pengetahuan Teknologi, serta perkembangan di bidang informasi dan komunikasi yang sangat pesat dan tidak terbendung, dewasa ini yang sudah tentu berdampak pada seluruh aspek atau seluruh sendi-sendi kehidupan masyarakatnya. Dengan demikian, tidaklah berlebihan apabila dikatakan bahwa perkembangan yang salah satunya dicirikan dengan banyaknya pembangunan senantiasa akan menimbulkan perubahan.[1]

Perkembangan dan kemajuan teknologi komputer dan telekomunikasi berupa media internet sebagai salah satu penyebaran informasi dalam kehidupan sehari-hari membawa dampak buruk berupa penyalahgunaan media internet sebagai salah satu sarana untuk melakukan perbuatan memperoleh data identitas diri seperti *user id* dan *password* dengan menggunakan teknik *Data Theft* atau *Phising*.

Phising atau *Identity theft* adalah tindakan memperoleh informasi pribadi seperti User ID (merupukan tanda pengenal untuk masuk dan mengakses internet), PIN (merupakan angka sandi rahasia antara pengguna dan sistem), nomor rekening, nomor kartu kredit Anda secara tidak sah melalui e-mail palsu kepada seseorang atau suatu perusahaan atau suatu organisasi dengan menyatakan bahwa pengirim adalah suatu entitas bisnis yang sah.[2] Informasi ini kemudian akan dimanfaatkan oleh pihak phiser untuk mengakses rekening, melakukan penipuan kartu kredit atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.

Menurut Johanes Gunawan, perlindungan hukum atau tanggung jawab bank terhadap nasabah selaku konsumen dapat dilakukan pada saat sebelum terjadinya transaksi (*pre purchase*) atau sesudah terjadinya transaksi (*post purchase*).[3] 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 di bawah meja kasir. Pelaku mengambil data-data korbannya dengan cara menggesekkan kartu pada *card skimmer* sesaat setelah dilakukan transaksi pada mesin *Electronic Data Capture* (*EDC*)[4]. Namun di sisi lain, mengingat perbankan adalah lembaga yang mengelola dana masyarakat dan memiliki

[1] Kristian dan Yopi Gunawan, *Sekelumit tentang Penyadapan Dalam Hukum Positif di Indonesia*, Bandung: Nuansa Aulia, 2013. hlm.1.
[2] Sutan Remy Syahdeini, *Kejahatan & Tindak Pidana Komputer*, Jakarta: Grafiti, 2009 hlm. 63-64.
[3] Johanes Gunawan, *Hukum Perlindungan Konsumen*, Bandung: Universitas Katolik Parahyangan, 1999, hlm. 3.
[4] 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.

fungsi strategis dalam peningkatan perekonomian masyarakat, maka pemerintah mewajibkan perbankan untuk patuh dan taat dalam menjalankan setiap kebijakan pemerintah.[5]

Perbankan adalah segala sesuatu yang menyangkut tentang bank mencakup kelembagaan ,kepemilikan usaha,serta kegiatan usaha baik konvensional dan prinsip syariah. Sedangkan dalam kasus Data theft, Phisisng ataupun skiming termasuk kedalam *Cyber-crime* adalah tindakan pidana kriminal yang dilakukan pada teknologi internet (*cyber space*), baik yang menyerang fasilitas umum didalam cyber space ataupun kepemilikan pribadi.

Metode Penelitian yang digunakan dalam penelitian ini adalah yuridis normatif dengan jenis penelitian hukum yang mengambil data kepustakaan dan didukung oleh data yang diperoleh di lapangan. Data yang digunakan dalam penelitian ini adalah data sekunder, yang terdiri atas bahan hukum primer, sekunder dan tersier.

PEMBAHASAN

Kejahatan Siber Terhadap sistem Bank Di Indonesia

Bank memiliki fungsi dan peran yang strategis dalam peningkatan ekonomi masyarakat. Hal ini dapat dilihat dari kedudukan bank sebagai lembaga intermediasi, yang menghimpun dana dan menyalurkannya kembali kepada masyarakat dalam bentuk-bentuk lainnya. Peran dan fungsi intermediasi dari bank telah menghidupkan perputaran uang dari pihak yang kelebihan dana kepada pihak yang kekurangan dana. Dana yang dihimpun oleh bank merupakan dana masyarakat yang wajib dikelola dengan baik, serta dilindungi keberadaanya, sehingga tidak menimbulkan kerugian bagi para pihak, maupun bagi bank itu sendiri, yang pada akhirnya secara sistemik akan berdampak pada perekonomian negara.[6]

Besarnya dampak yang ditimbulkan akibat pengelolaan bank yang tidak profesional, telah mendorong pemerintah melakukan tindakan preventif maupun represif melalui pengaturan bisnis perbankan. Secara normatif, pengaturan aktivitas perbankan tertuang dalam Undang- Undang Nomor 10 Tahun 1998 *juncto* Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, dan peraturan perundang-undangan lainnya. Berdasarkan pengaturan tersebut, bank wajib melaksanakan kepatuhan terhadap pelbagai peraturan perundang-undangan dan menerapkan prinsip kehati-hatian.[7] Disisi lain dengan adanya kejahatan dalam dunia siber pun melihat kejahatan yang terjadi pada bank tersebut ke dalam Undang-Undang Nomor 19 Tahun 2016

[5] Johannes Ibrahim, "Pertanggungjawaban Pidana Bank dalam Pelanggaran Kegiatan Operasional didasarkan pada Undang-Undang Nomor 10 Tahun 1998", *Dialogia Iuridica*, Vol 7 No 2 April 2016, hlm. 44.
[6] *Ibid*, hlm 46
[7] *Ibid*, hlm 46

tentang Informasi dan Transaksi Elektronik karena adanya pencurian data tetapi dalam hal ini ada dalam dunia siber.

Kejahatan *cyber* atau *cyber crime* yang pada dasarnya merupakan imbas dari perkembangan teknologi yang telah mengubah kebiasaan masayarakat yang pada awalnya bersifat konvensional menjadi sebuah kebiasaan yang lebih bersifat modern atau dapat disebut dengan *high technology society*. Perubahan kebiasaan ini telah menghasilkan suatu kejahatan dengan penggunaan alat elektronik sebagai media kejahatan. Faktor utama yang mengakibatkan peralihan kebiasaan tersebut adalah adanya perkembangan teknologi informasi yang berpadu dengan media komunikasi dan teknologi komputer, yang kemudian menghasilkan suatu piranti baru yangdisebut dengan internet. Kemunculan internet telah menghasilkan suatu pola interaksi baru dalam kehidupan bermasyarakat, yang pada awalnya lebih bersifat nyata *(real)* berubah menjadi pola interaksi masayakat yang dapat dikatakan bersifat v*irtual (cybernetics)*[8]

Dalam Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik yang berbunyi setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pengertian *Cyber law* adalah merupakan seperangkat aturan yang dibuat oleh suatu Negara tertentu, dan peraturan yang dibuat itu hanya berlaku kepada masyarakat Negara tertentu. *Cyber Law* dapat pula diartikan sebagai hukum yang digunakan di dunia *cyber* (dunia maya), yang umumnya diasosiasikan dengan internet. Pengertian *Cyber-crime* adalah tidak *criminal* yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. *Cyber-crime* merupakan kejahatan yang memanfaatkan perkembangan teknologi computer khusunya internet dan seperti halnya pencurian data yang akhir-akhir ini semakin marak terjadi pada lembaga perbankan terutama dalam sistem informasi.

Dalam perkembangan kejahatan di bidang perbankan di Indonesia saat ini sangat kompleks mengingat kehadiran bank saat ini yang sangat berkembang pesat, sehingga makin maraknya kejahatan yang terjadi di bidang perbankan khususnya dalam pencurian data nasabah.

Perlindungan Terhadap Dana Nasabah oleh Lembaga Penjamin Simpanan

Dikeluarkan Undang-undang Nomor 24 Tahun 2004 tentang Lembaga Penjamin Simpanan, yang kemudian telah diubah dengan Undang-undang Nomor 7 Tahun 2009 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 3 Tahun

[8] Akbar Kurnia Putra, "Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (*Cybercrime*) berdasarkan Convention on Cybercrime", *Jurnal Ilmu Hukum*, Vol.7. No.1, Maret 2016 hlm.26.

2008 tentang Perubahan Atas Undang-Undang Nomor 24 Tahun 2004 tentang Lembaga Penjamin Simpanan Menjadi Undang-Undang (Undang-Undang LPS), mengatur adanya skim penjaminan simpanan nasabah yang bersifat terbatas dan resolusi bank oleh Lembaga Penjamin Simpanan (LPS) sebagai suatu lembaga yang independen. Secara khusus tujuan pembentukan LPS adalah :

a. melindungi simpanan nasabah kecil;
b. mengurangi *moral hazard* dan mendorong tumbuhnya disiplin pasar;
c. membatasi beban keuangan negara;
d. menciptakan mekanisme yang transparan dalam penyelesaian bank gagal dan likuidasi bank.

Selain itu, perlindungan hukum bagi nasabah juga dilakukan oleh Lembaga Penjamin Simpanan yang biasa dikenal dengan sebutan LPS terjadi dalam hal bank gagal, dimana LPS menggantikan kedudukan nasabah (subrogasi) sehingga berhak atas pembayaran yang berasal dari penjualan aset bank gagal tersebut. Dalam hal ini, perlu ditegaskan bahwa nasabah penyimpan memiliki kedudukan utama terhadap aset bank gagal tersebut sehingga LPS akan memperoleh kedudukan pemegang hak utama.

Berdasarkan program penjaminan simpanan LPS, nasabah penyimpan pada bank yang telah dicabutan izin usahanya, memiliki hak untuk mengajukan klaim penjaminan atas dana simpanannya kepada LPS melalui bank pembayaran yang ditunjuk oleh LPS. LPS mempunyai kewajiban untuk membayar klaim penjaminan kepada nasabah penyimpan dan menentukan simapanan layak dibayar, setelah melakukan rekonsiliasi dan verifikasi atas data nasabah selambatlambatnya 90 (sembilan puluh) hari kerja terhitung sejak izin usaha bank dicabut.

LPS berhak memperoleh data nasabah penyimpan dan informasi lain yang diperlukan per tanggal pencabutan izin usaha dari LPP dan/atau bank dalam rangka penghitungan dan pembayaran klaim penjaminan LPS berperan sebagai penjamin terhadap simpanan nasabah bank. Dengan adanya hubungan antara LPS dan nasabah, maka LPS dapat melindungi dana nasabah pada bank-bank peserta penjaminan agar tetap aman dan memberikan jaminan atas simpanannya apabila bank-bank tersebut mengalami kesulitan usaha, kemudian dicabut izin usahanya dan dilikuidasi, maka kedudukan nasabah tetap terjamin. Dengan kata lain, LPS merupakan bentuk nyata dari adanya penjaminan dan perlindungan terhadap dana simpanan masyarakat.

PertanggungJawaban Lembaga Perbankan Terhadap Nasabah Bank yang mengalami Pencurian Data

Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara. Setiap negara harus menghadapi kenyataan bahwa informasi dunia saat ini dibangun

berdasarkan suatu jaringan yang ditawarkaan oleh kemajuan bidang teknologi. Salah satu cara berpikir yang produktif adalah mendirikan usaha untuk menyediakan suatu infra struktur informasi yang baik di dalam negeri, yang kemudian dihubungkan dengan jaringan informasi global.

Keberadaan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik ini sebenarnya dapat meningkatkan keamanan dan kenyamanan nasabah saat melakukan kegiatan perbankan melalui sistem elektronik yang disediakan bank. Ada beberapa alasannya. Pertama, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik menegaskan bahwa bank, sebagai pihak yang menyelenggarakan sistem elektronik dalam memfasilitasi pelayanan jasa bank via Internet (*e-banking*), bertanggung jawab secara hukum terhadap kerugian yang dialami nasabah berkaitan dengan pemanfaatan layanan yang disediakannya. Namun, jika kerugian disebabkan oleh force majeur atau kesalahan dan kelalaian nasabah, maka bank tidak dapat dimintai pertanggungjawaban.

Kedua, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik mengharuskan bank untuk menyelenggarakan sistem elektronik yang andal dan aman, serta bertanggung jawab terhadap operasional sistem elektroniknya. Bank juga wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagaimana diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik.

Ketiga, dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik ada pengakuan terhadap kontrak elektronik, yaitu perjanjian yang dibuat melalui sistem elektronik. Laporan transaksi perbankan via e-mail, yang menunjukkan adanya penawaran dan persetujuan yang melibatkan nasabah, dapat juga dianggap sebagai kontrak elektronik.

Keempat, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik menegaskan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Jika nasabah menggunakan e-banking untuk transaksi perbankannya, maka laporan mutasi rekening miliknya pada sistem elektronik yang disediakan bank dan hasil cetaknya dapat menjadi alat bukti yang sah.

Kelima, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik mengatur lebih jelas mengenai kejahatan terhadap system informasi, sehingga memudahkan aparat penegak hukum untuk menindaklanjutinya. Selain itu, terdapat pula sanksi berat bagi orang yang mengganggu atau menerobos sistem pengamanan elektronik secara ilegal. Dengan demikian, siapa pun akan berpikir panjang untuk melakukan kejahatan terhadap e-banking. Namun demikian, beberapa ketentuan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik masih perlu pengaturan lebih lanjut melalui peraturan pemerintah. Salah satunya

mengenai persyaratan minimum yang harus dipenuhi suatu system elektronik. Peraturan pemerintah itu menjadi penting karena informasi/dokumen elektronik dinyatakan sah jika menggunakan sistem elektronik yang sesuai dengan ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik.

Dalam perlindungan hukum nasabah bank yang mengalami pencurian data Sebelum memberikan perlindungan hukum terhadap nasabah, bank harus terlebih dahulu melakukan berbagai upaya sebagai berikut :

1. Bank harus mengetahui identitas yang akan atau sedang menggunakan jasa perbankan.
2. Manajemen bank harus menjamin bahwa transaksi yang dilakukan telah sesuai dengan kode etik dan peraturan atau ketentuan peraturan yang berkaitan dengan transaksi tersebut (Undang-undang Nomor 10 Tahun 1998 tentang Perbankan).
3. Dalam kaitannya dengan pelaksanaan ketentuan rahasia bank, bank harus bekerja sama dengan aparat penegak hukum sesuai dengan ketentuan yang berlaku (*bank secrecy*).

Kemudian perlindungan yang dapat diberikan pada nasabah bank dapat melalui dua cara, yaitu :

1. Perlindungan secara implisit (*implicit deposit protection*), yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif yang dapat menghindarkan terjadinya kebangkrutan bank. Perlindungan ini dapat diperoleh melalui :
    a) Peraturan perundang-undangan di bidang perbankan.
    b) Perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif yang dilakukan oleh Bank Indonesia.
    c) Upaya menjaga kelangsungan usaha bank sebagai lembaga pada khususnya dan perlindungan terhadap sistem perbankan pada umumnya.
    d) Memelihara tingkat kesehatan bank.
    e) Melakukan usaha bank dengan menggunakan prinsip kehati-hatian.
    f) Menyediakan informasi risiko pada bank.

2. Perlindungan secara eksplisit (*explicit deposit protection*), yaitu perlindungan melalui pembentukan suatu lembaga yang menjamin simpanan masyarakat, sehingga apabila bank mengalami kegagalan, lembaga tersebut yang akan mengganti dana masyarakat. Selanjutnya dalam rangka memberikan perlindungan hukum kepada nasabah Bank biasanya melakukan hal sebagai berikut :

a. Bank dengan menggunakan teknologi Secure Socket Layer (SSL) 128 bit yang akan melindungi komunikasi antara komputer nasabah dengan server Bank . Untuk menambah keamanan digunakan metode time out, maksudnya adalah setiap 10 (sepuluh) menit tanpa aktivitas nasabah, akses dari komputer nasabah ke server Bank secara otomatis tertutup.
b. Bank akan menjaga kerahasiaan data pengguna internet banking dan hanya orang tertentu yang berhak untuk mengakses informasi tersebut untuk digunakan sebagaimana mestinya (dalam hal ini Bank selalu mengingatkan pegawai Bank akan pentingnya menjaga kerahasiaan data nasabah). Bank tidak akan memperlihatkan atau menjual data tersebut kepada pihak ke tiga.
c. Bank juga tidak secara otomatis mengumpulkan informasi data pengunjung internet banking .
d. Informasi umum yang dikumpulkan dan digunakan antara lain :
    1) Domain yang akan digunakan oleh nasabah untuk mengakses internet;
    2) Internet banking yang digunakan untuk mengakses website Bank;
    3) Browser;
    4) Hari, tanggal, dan waktu;
    5) Pilihan yang ditentukan oleh nasabah untuk memberikan informasi kepada bank antara lain jenis rekening ;
e. Untuk dapat mengakses internet banking , nasabah harus memasukkan terlebih dahulu user ID dan PIN untuk keamanan nasabah diharuskan memasukkan kembali PIN untuk transaksi bersifat *financial*.
f. Saat ini Bank menyediakan sarana internet banking yang lebih cocok di akses dengan menggunakan netscape communitor 4.7 atau Microsoft internet explorer 5.01 (yang menggabungkan navigator, klien e-mail, editor halaman website, dan aplikasi lainnya).

Dari sini dapat dilihat bahwa sebenarnya sudah ada upaya melindungi para nasabah dalam layanan perbankan yang terdiri dari perlindungan data atas data yang dikumpulkan, dimanfaatkan atau digunakan untuk keperluan transaksi dari nasbahnya. Tidak hanya itu perlindungan atas data pribadi nasabah pengguna fasilitas internet banking pun diperketat lagi dengan adanya persyaratan-persyaratan tertentu dalam penggunaan untuk bertransaksi dengan menggunakan layanan internet banking. Namun dengan adanya upaya untuk melindungi nasabah bank masih saja tidak luput dari ancaman kejahatan *cyber crime*.

Bank akan bertanggung jawab terhadap kerugian yang dialami nasabah pengguna fasilitas internet banking jika kesalahan teknis atau bocornya data nasabah bank terjadi

karena kelalaian dari pihak Bank, Bank juga akan memberikan perlindungan hukum terhadap nasabah Bank yang mengalami kerugian dikarenakan oleh pihak Bank sesuai aturan hukum yang mengatur, yaitu :

1. Undang-undang Nomor 10 Tahun 1998 tentang Perbankan, Pasal 42 ayat (1) dan Pasal 47.
   Pasal 42 ayat (1), dikatakan bahwa :
   " Untuk kepentingan dalam perkara pidana Menteri dapat member izin kepada polisi, jaksa, atau hakim untuk memperoleh keterangan dari bank tentang keadaan keuangan tersangka / terdakwa pada bank. "

   Pasal 47, dinyatakan bahwa :
   (1) Barang siapa tanpa membawa perintah tertulis dari Menteri kepada bank sebagaimana dimaksud dalam Pasal 41 atau tanpa izin Menteri sebagaimana dimaksud dalam Pasal 42 dengan sengaja memaksa bank atau pihak terafiliasi untuk memberikan keterangan sebagaimana dimaksud dalam Pasal 40, diancam dengan pidana penjara paling lama 3 (tiga) tahun dan denda paling banyak Rp. 3.000.000.000,00 (tiga miliar rupiah).
   (2) Anggota Dewan Komisaris, direksi, pegawai bank, atau pihak terafiliasi lainnya dengan sengaja memberikan keterangan yang wajib dirahasiakan menurut Pasal 40, diancam dengan pidana penjara paling lama 2 (dua) tahun dan denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

2. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 30 dikatakan bahwa :
   (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan / atau Sistem Elektronik milik orang lain dengan cara apapun.
   (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum atau mengakses komputer dan / atau Sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan / atau Dokumen Elektronik.
   (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan / atau Sistem Elektronik dengan caraapapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengaman.

Akan tetapi langkah cerdas telah diambil oleh Bank untuk mengantisipasi risiko atas kelemahan dari segi teknologi dan yuridis dengan membuat suatu kebijakan yang disebut *self-regulatory* banking yang mewajibkan bank menyusun ketentuan internal mengenai pedoman manajemen risiko. *Self- regulatory* pada bank adalah untuk

memperkuat kondisi internal perbankan dalm menghadapi risiko yang semakin kompleks berupaya melindungi kepentingan stake holders dan meningkatkan kepatuhan terhadap peraturan perundang-undangan yang berlaku serta nilai-nilai etika yang berlaku umum pada industri perbankan.Namun jika kejahatan *cyber crime* telah merugikan nasabahnya, Bank akan bersedia memberikan data nasabah guna di persidangan nanti jika hal tersebut mutlak terjadi karena kejahatan *cyber crime*.

Begitu juga sebaliknya ada beberapa kendala dalam memberikan perlindungan nasabah bank sebagai berikut :

1. Memungkinkan terjadinya penyalahgunaan atau kejahatan jasa layanan elektronik oleh pihak yang tidak bertanggung jawab yang mengakibatkan nasabah mengalami kesulitan melakukan klaim kepada bank dan memungkinkan nasabah untuk memperoleh bukti transaksipun tidak ada.
2. Kondisi VSAT (Jaringan Vertikal Satelit) adalah jaringan komunikasi yang sering kali menjadi penghambat, karena teknologi yang canggih yang digunakan bank belum dapat memberikan kenyamanan yang maksimal bagi nasabahnya. Misalnya dari sekian orang nasabah yang mengunakan layanan internet banking belum tentu dapat ditampung oleh koneksi yang tersedia dalam mengakses internet banking tersebut sehingga gagal log-in pun sering dialami nasabah pengguna fasilitas internet banking.
3. Sumber daya manusia yang kurang mendukung, maksudnya adalah tidak semua nasabah mengerti cara penggunaan yang baik dan benar atas layanan yang tersedia di dalam fasilitas internet banking sehingga sering terjadi salah pemahaman dalam penggunaannya seperti kesalahan dalam mentransfer pun kerap terjadi.
4. Kurang berperannya pihak-pihak yang terkait dengan perlindungan terhadap nasabah, masih terbatas pada kegiatan operasional dari suatu bank atau Lembaga Perlindungan Konsumen belum berperan secara aktif dalam memberikan perlindungan kepada nasabah bank, hal ini dikarenakan kurangnya pemahaman yang diberikan dari lembaga tersebut sehingga nasabah bank tidak memiliki informasi yang cukup mengenai keberadaan dari lembaga ini.
5. Jika dilihat dari segi Undang-undang yang mengatur secara khusus mengenai internet banking masih belum ada. Karena mengingat di era digital saat ini mengenai pencurian data nasabah memang sangat marak dilakukan oleh para pihak yang tidak bertanggung jawab maka sebagai pelaku perbankan haruslah dapat menjaga bersama tidak hanya tugas bagi bank saja tapi peran dari pada masyarakat selaku para nasabah kreditur setidaknya ikut menjaga dan terus berhati-hati meskipun telah banyak perlindungan yang diberikan tapi tidak

selamanya menjamin kepastian hukum jika itu terjadi akibat kelalaian dari nasabah.

Penerapan Sanksi Hukum terhadap Pelaku Pencurian Data Nasabah

Usaha Perbankan Indonesia berasaskan demokrasi ekonomi dengan berdasarkan Pancasila dan UUD 1945 serta menggunakan prinsip kehati-hatian (*prudent banking principle*) yaitu dalam menjalankan usahanya, bank wajib bersikap hati-hati (*prudent*) untuk melindungi dana masyarakat yang dipercayakan pada bank. Selain itu terdapat asas kepercayaan (*Fiduciary Principle*), dimana bank dilandasi atas hubungan kepercayaan antara bank dengan nasabah dan asas kerahasiaan (*Confidential Principle*) yaitu kewajiban bank untuk merahasiakan semua hal yang berkaitan dengan keuangan nasabah dan menurut aturan perbankan wajib untuk dirahasiakan.

Keberadaan Kitab Undang-undang Hukum Pidana dianggap mampu mencakup seluruh kejahatan yang terjadi di masyarakat, namun dalam Pasal 362 mengenai pencurian ini tidak disebutkan apakah dilakukan secara langsung atau melalui media lain. Pada awalnya KUHP mampu juga dikenai terhadap pelaku kejahatan pencurian melalui media elektronik ini, namun dengan seiring perkembangan zaman semakin tingginya tingkat kejahatan siber melalui media elektronik ini menuntut agar adanya perkembangan dalam sistem hukum yang dinilai tidak mampu memenuhi unsur-unsur kejahatan yang berkembang mengikuti era globalisasi diantaranya adalah terhadap pencurian data nasabah di lingkungan bank.

Adapun Tindak pidana perbankan dan tindak pidana di bidang perbankan dapat dibedakan sebagai berikut, yaitu :

a. Tindak pidana perbankan adalah semua perbuatan yang melanggar ketentuan yang diatur dalam Undang- Undang Perbankan, atau tindak pidana yang dilakukan dalam kegiatan menjalankan fungsi dan usaha sebagai bank berdasarkan Undang-Undang Perbankan.
b. Tindak pidana di bidang perbankan adalah semua jenis perbuatan melanggar hukum yang berhubungan dengan kegiatan dalam menjalankan usaha bank, baik bank sebagai sasaran maupun sebagai sarana, atau tindak pidana yang bukan hanya mencakup pelanggaran Undang- Undang Perbankan saja, namun juga mencakup tindak pidana umum lainnya selama berkaitan dengan lembaga perbankan.

Dalam hukum pidana, sanksi hukum disebut hukuman adalah “Suatu perasaan tidak enak (sengsara) yang dijatuhkan oleh hakim dengan vonis kepada orang yang telah melanggar undang-undang hukum pidana”. Berdasarkan prinsip utama dalam transaksi perbankan di Indonesia masih lebih mengedepankan aspek kepercayaan atau “trust” terhadap penjual maupun pembeli. Prinsip keamanan infrastruktur transaksi

secara online seperti jaminan atas kebenaran identitas penjual/pembeli, jaminan keamanan jalur pembayaran (*payment gateway*), jaminan keamanan dan keandalan website electronic commerce belum menjadi perhatian utama bagi penjual maupun pembeli, Salah satu indikasinya adalah banyaknya laporan pengaduan tentang penipuan melalui media internet maupun media telekomunikasi lainnya yang diterima oleh kepolisian.

Dengan kondisi demikian, ada baiknya kita lebih selektif lagi dalam melakukan transaksi secara online dan mengedepankan aspek keamanan transaksi dan kehati-hatian sebagai pertimbangan utama dalam melakukan transaksi jual beli. Peraturan hukum Indonesia, belum ada pengaturan yang khusus dan jelas mengenai internet banking. Namun, perbincangan tentang perlunya aturan aturan yang jelas mengatur masalah internet banking sudah marak dikaji dan dibahas. Undang -Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik kini cukup mampu mengatur permasalahan-permasalahn hukum dari sistem internet banking sebagai salah satu layanan perbankan yang merupakan wujud perkembangan teknologi informasi.

Penerapan sanksi hukum terhadap pelaku pencurian data nasabah yaitu terdapat pada Pasal 30, Pasal 32, Pasal 33 dan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Ketentuan Pidana terdapat pada Pasal 46, Pasal 48, Pasal 49, Pasal 51 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Dapat dijabarkan mengenai penerapan sanksi diatas adalah sebagai berikut :

> Setiap perbuatan melawan hukum dengan mengakses sistem elektronik yang bertujuan untuk memperoleh Informasi/Dokumen Elektronik dengan cara melanggar sistem pengamanan dianggap sebagai tindak pidana sesuai Pasal 46 jo Pasal 30 UU ITE. Perbuatan ini diancam dengan sanksi pidana penjara paling lama 6 sampai 8 tahun dan/atau denda paling banyak Rp600.000.000,00 sampai Rp800.000.000,00.
>
> Pasal 30 UU ITE selengkapnya berbunyi:
> (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
> (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
> (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Sedangkan Pasal 46UU ITEberbunyi:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Terkait perlindungan data pribadi dalam bentuk Dokumen Elektronik atau Informasi Elektronik, Pasal 32 UU ITE mengatur tentang larangan bagi setiap Orang untuk melakukan interferensi (mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan) terhadap bentuk Dokumen Elektronik atau Informasi Elektronik tanpa hak dan dengan cara melawan hukum. Ancaman hukuman atas perbuatan tersebut diatur dalam Pasal 48 UU ITE.

Pasal 32 UU ITE selengkapnya berbunyi:

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa punmengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Sedangkan Pasal 48 UU ITE berbunyi:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

KESIMPULAN

Berdasarkan uraian pembahasan di atas, maka dapat disimpulkan hal-hal sebagai berikut:

1. Maraknya kejahatan dunia cyber saat ini menjadi permasalahan bersama antara nasabah dan lembaga perbankan
2. 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 protection*) yaitu perlindungan melalui pembentukan suatu lembaga yang menjamin simpanan masyarakat, sehingga apabila bank mengalami kegagalan, lembaga tersebut yang akan mengganti dana masyarakat.
3. Dengan adanya LPS diharapkan dapat memberikan perlindungan bagi nasabah yang telah mempercayakan dana nya kepada lembaga perbankan sehingga kepercayaan masyarakat akan tetap tumbuh.
4. Penerapan sanksi hukum terhadap pelaku pencurian data nasabah yaitu terdapat pada Pasal 30, Pasal 32, Pasal 33 dan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Ketentuan Pidana terdapat pada Pasal 46, Pasal 48, Pasal 49, Pasal 51 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Dalam penelitian ini, penulis juga menyarankan:

1. Perlu pengawasan yang optimal dari Stakeholder, masyarakat selaku nasabah dan lembaga perbankan tentunya terhadap pengelolaan sistem perbankan, mengingat tindak pidana kejahatan maupun pelanggaran dalam bisnis perbankan terutama terhadap pencurian data nasabah cukup meresahkan masyarakat, serta perlu adanya penguatan substansi untuk menjangkau modus baru tindak pidana yang saat ini tidak terjangkau oleh Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, seperti misalnya jual beli data nasabah.
2. Perlu adanya peran serta pemerintah selaku pembuat kebijakan dan regulasi terkait penjatuhan sanksi pidana bagi oknum yang melakukan tindak pidana

khususnya dalam hal ini yang merugikan nasabah yang menimbulkan kerugian yang serius.

DAFTAR PUSTAKA

Buku

Johanes Gunawan, *Hukum Perlindungan Konsumen*, Bandung: Universitas Katolik Parahyangan, 1999.

Kristian dan Yopi Gunawan,Penyadapan Dalam Hukum Positif di Indonesia, Bandung, 2013.

Sutan Remy Syahdeini, *Kejahatan & Tindak Pidana Komputer*, Grafiti, Jakarta, 2009.

Jurnal

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.

Johannes Ibrahim, "Pertanggungjawaban Pidana Bank dalam Pelanggaran Kegiatan Operasional didasarkan pada Undang-Undang Nomor 10 Tahun 1998", *Dialogia Iuridica*, Vol 7 No 2 April 2016.

Akbar Kurnia Putra, analisis *hukum yurisdiksi tindak kejahatan siber (Cybercrime) berdasarkan convention on Cybercrime*, Jurnal Ilmu Hukum, Vol.7. No.1, Maret 2016.

Peraturan dan Perundang-Undangan

Undang-Undang Nomor 7 Tahun 1992 jo Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaski Elektronik.