KEDUDUKAN HUKUM BANK YANG MENJALANKAN FUNGSI SEBAGAI *PAYMENT GATEWAY* DALAM TRANSAKSI ELEKTRONIK DI INDONESIA

(The Legal Position of Banks That Functions as a Payment Gateway in Electronic Transactions in Indonesia)

Abdul Halim Barkatullah
Fakultas Hukum Universitas Lambung Mangkurat
Jalan Brigjen H. Hasan Basry Banjarmasin Kalsel 70123 Indonesia
Telp/Fax: +62-81348439997 E-mail: halim.ulmbjm@gmail.com

Abstract

Technology's sophisticated continuous improvement has embraced the blooming of electronic transaction. Its reputation gains from multiple methods it offers which benefitted each party. Card payments are getting more popular across Indonesia since it provides convenience. However, security is the main concern to ensure safety transactions and avoid fraudulent threats. Adopting bank as the payment gateway might encounter security issues in an electronic transaction. The application of Certification Authority, which combined three-party payment system and firewall will enhance the security system and prevent illegal access to bank networking. The legal position between merchant and bank as a payment gateway towards cardholders become significant to recognize. This relationship is a special authorization with payment. Therefore, bank as the endorsee should not exercise its power beyond its authorization.

Keywords: Legal Position, Electronic Transactions, Payment Gateway.

Abstrak

Perkembangan transaksi elektronik ini sangatlah pesat didukung dengan sistem teknologi yang semakin canggih. Para pelaku transaksi diuntungkan dengan beragam metode transaksi elektronik ini. Dalam melakukan transaksi elektronik yang menggunakan sistem pembayaran online, haruslah memiliki sistem pembayaran yang benar-benar aman. Pada metode pembayaran dengan menggunakan kartu kredit, merchant di Indonesia sebaiknya menarik bank sebagai *payment gateway* untuk menjaga kerahasiaan dan menjamin keamanan pembayaran. Dalam pengamanan transaksi bank sebagai *payment gateway* haruslah meggunakan sistem keamanan yang handal, dan adanya *certification authority* dengan mengkombinasikan *three party payment system* serta menggunakah f*irewall* sebagai pagar yang mencegah akses illegal ke jaringan perbankan, yang mengitari sistem. Kedudukan hukum antara *merchant* dengan bank selaku *payment gateway* bagi *cardholder* yang menggunakan kartu kredit. Hubungan ini adalah pemberian kuasa khusus dengan mendapatkan upah, oleh karena itu bank sebagai penerima kuasa kewenangannya hanya terbatas pada hal-hal yang dikuasakan kepadanya.

Kata Kunci: *Kedudukan Hukum, Transaksi Elektronik, Payment Gateway.*

PENDAHULUAN

Media internet atau dalam bahasa populer di Indonesia disebut dunia maya, sudah hampir tidak dapat dilepaskan lagi dari kehidupan masyarakat sehari-hari. Internet mempermudah dan mengefisiensikan hampir seluruh pekerjaan yang pada awalnya memerlukan proses yang lama dan sumber daya yang tidak sedikit.

Globalisasi yang ditandai dengan adanya perapatan dunia *(compression of the world)* telah mengubah peta perekonomian, politik, dan budaya. Pergerakan barang dan jasa terjadi semakin cepat. Modal dari suatu negara beralih ke negara lain dalam hitungan detik akibat pemanfaatan teknologi informasi. Sejalan dengan itu,kegiatan perbankan sebagai urat nadi perekonomian bangsa tidak luput dari dampak globalisasi[1].

Dalam perkembangannya, media internet memungkinkan terjadinya transaksi-transaksi antar konsumen dan distributor / produsen yang bahkan tidak berinteraksi secara fisik di dunia nyata. Perkembangan bisnis online (transaksi elektronik) ini sangatlah pesat didukung dengan sistem teknologi yang semakin hari semakin beragam dan canggih. Para pelaku bisnis online sangat diuntungkan dengan beragam metode transaksi elektronik ini, mereka tidak perlu lagi menjalankan bisnis dengan metode konvensional yang memerlukan banyak modal, misalnya untuk menyewa toko atau melakukan penawaran dari rumah ke rumah *(door to door).* Cukup dengan modal kemahiran sedikit untuk membangun laman web yang bahkan tersedia gratis di internet, para pelaku bisnis sudah dapat menjual barang/jasa yang mereka tawarkan. Para konsumen pun dimudahkan, hanya

[1] Jusuf Anwar, *Aspek-aspek Hukum Keuangan dan Perbankan*, Suatu Tinjauan Praktis, disampaikan pada Lokakarya Pembangunan Hukum Nasional VIII Departemen Hukum dan HAM, Badan Pembinaan Hukum Nasional, Denpasar 14-18 Juli 2009.

mengetikkan item yang diinginkan di mesin pencari, maka bermunculanlah laman-laman web yang menawarkan barang yang dicari.

Transaksi yang dilakukan melalui internet, lazim disebut transaksi elektronik, memunculkan beragam resiko, baik terhadap pihak distributor / produsen maupun terhadap pihak konsumen. Isu utama transaksi elektronik adalah masalah keamanan. Keamanan menjadi perhatian utama semua pihak yang terlibat.

Kepastian akan keamanan terkait erat dengan cyberlaw atau hukum siber suatu negara. *Cyberlaw* adalah hukum yang mengatur penggunaan komputer dan internet[2]. Tingkat keamanan yang rendah berbanding lurus dengan transaksi yang terjadi. Dengan kata lain, keamanan yang rendah akan membuat pihak yang berkepentingan berpikir dua kali untuk melakukan transaksi. Tingkat keamanan bertransaksi sering menjadi acuan untuk menentukan itikad baik pihak yang terlibat. Pasal 17 ayat (2) Undang-undang Republik Indonesia Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, mewajibkan para pihak yang melakukan transaksi elektronik untuk memiliki itikad baik dalam melakukan interaksi dan / atau pertukaran informasi elektronik dan/ atau dokumen elektronik selama transaksi berlangsung. Pengertian transaksi elektronik menurut Undang-undang itu sendiri adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/ atau media elektronik lainnya.

Ancaman yang ada dalam transaksi elektronik tidak hanya datang dari para pihak yang melakukan transaksi. Ancaman besar lainnya justru datang dari pihak luar yang mencoba mengambil keuntungan dengan melakukan tindakan-tindakan yang sekiranya dapat menguntungkan meski merugikan pihak lain. Komputer yang terhubung ke jaringan (baca: Internet) dapat membuka peluang terjadinya kejahatan bahkan

[2] Gerald R Ferrera, Stephen D Lichstein, Margo E.K Reder, Ray August, Willian T Schiano, *Technology and Cyberlaw, Text and Cases*, South Western College Publishing, United States, 2011, Hlm. 3.

memfasilitasi kejahatan tersebut[3].

Toko online dan Katalog Online adalah dua usaha yang selalu melakukan transaksi elektronik, sesuai dengan jenisnya sebagai penjual online. Perbedaan mendasar dari kedua usaha online tersebut adalah penggunaan bank dalam proses pembayaran yang dilakukan konsumen. Pada Katalog online, baik melalui laman maupun forum online, proses pembayaran dilakukan secara manual. Manual disini berarti konsumen setelah memilih barang/jasa yang diinginkan, diharuskan untuk mentransfer sejumlah uang pembayaran ke rekening bank penjual. Efisiensi yang dihajatkan oleh media internet menjadi tidak tercapai karena proses untuk tercapainya transaksi memakan banyak waktu dan sumber daya. Berbeda dengan Toko Online, dimana konsumen dapat memilih metode pembayaran elektronik dengan mengsgunakan bank sebagai pemberi layanan *payment gateway*, gerbang pembayaran. Nasabah bank manapun dapat memilih metode ini tanpa harus menjadi nasabah bank yang menjadi *payment gateway* tersebut. Metode pembayaran seperti ini dikenal populer sebagai metode pembayaran dengan menggunakan kartu kredit.

Pelayanan Payment Gateway dapat dibedakan dengan online banking. Jika online banking adalah aktivitas perbankan yang hanya dapat dilakukan pada situs perbankan terkait, maka pelayanan payment gateway dapat diaplikasikan pada laman web merchant (penjual) mana saja yang memiliki Toko Online *(Online Store)*. Pada Online Banking, pembelian atau transaksi terbatas pada apa yang ditawarkan oleh bank itu saja, dan dimungkinkan untuk memeriksa neraca *(balance)* rekening yang bersangkutan. Sedangkan *Payment Gateway* memungkinkan semua pemegang kartu kredit bank apa saja untuk melakukan transaksi selama kartu kredit bank tersebut memiliki lisensi yang ditentukan oleh bank acquirer (contoh lisensi dari Visa dan Mastercard), serta karena sifatnya yang kredit (dalam artian bank memberi pinjaman) maka tentu tidak

[3] David I Bainbridge, Ceng,MBCS, MICE, *Introduction to Computer Law*, Pitman Publishing, London 1993, Hlm. 153.

ada neraca rekening yang tercatat. Tidak ada saldo atau simpanan pada bank tersebut.

Transaksi elektronik pada dasarnya adalah merupakan suatu kontrak transaksi perdagangan antara penjual dan pembeli dengan menggunakan media internet. transaksi elektronik membantu pelaksanaan perdagangan tradisional melalui cara baru dalam mentransfer dan memproses informasi, karena informasi menjadi jantung dari segala aktifitas perdagangan. Informasi secara elektronik ditransfer dari komputer ke komputer secara otomatis. Kenyataannya hal ini telah mentransformasikan cara organisasi beroperasi[4].

Dilihat dari jenisnya transaksinya, transaksi elektronik dikelompokan menjadi dua segmen, yaitu*; business to business (B2B) dan business to consumer (B2C). B2B* adalah transaksi perdagangan melalui internet, yang dilakukan oleh dua atau lebih perusahaan. Transaksi ini biasanya dilakukan untuk pembelian bahan baku atau komponen pendukung kegiatan produksi atau perdagangan. Dalam dunia bisnis, transaksi dagang tersebut sering disebut sebagai *Enterprise Resource Planning* (ERP)ataupun *supplay chain management*, sedangkan *B2C* merupakan transaksi jual beli melalui internet antara penjual barang konsumsi dengan cardholder *(end user)*[5].

Perkembangan transaksi elektronik membawa banyak perubahan terhadap sektor aktivitas bisnis yang selama ini dijalankan di dunia *real*. Perubahan tersebut ditandai dengan adanya sejumlah upaya dari sektor aktivitas bisnis yang semula berbasis di dunia *real*, kemudian mengembangkannya ke dunia *virtual*. Salah satu sektor bisnis itu adalah berkaitan dengan sektor perbankan yang dikenal dengan istilah *E-Banking*.

[4] Kamlesh K Bajaj & Debjani Bag, *C-commerce The Cutting Edge of Business*, diterjemahkan oleh Imam Mawardi, Surabaya, PT. Akana Press Offset, 2010, hlm. 3.

[5] Muhammad Aulia Adnan, *Aspek Hukum Protokol Pembayaran Visa/Mastercard Secure Electronic Transaction (SET)*, Fakultas Hukum Universitas Indonesia, 2010, hlm. 6.

Implikasi dari pengembangan ini memiliki sisi positif dan negatif. Aspek positifnya bahwa dengan pengembangan kegiatan perbankan di internet melalui jaringan *online*, telah meningkatkan peranan dan fungsi perbankan itu sendiri sebagai lembaga intermediari sekaligus memberikan kemudahan dan efesiensi bagi para pengguna jasa *e-banking*. Aspek negatif dari pengembangan ini adalah berkaitan dengan persoalan keamanan dalam bertransaksi dengan menggunakan media ebanking dan secara yuridis terkait pula dengan jaminan kepastian hukum *(legal certainty*[6]*).*

Dalam transaksi elektronik di Indonesia yang kepercayaan *cardholder* baik dalam negeri maupun luar negeri dirasakan masih sangat kurang, hal ini akan berdampak negatif pada perkembangan transaksi elektronik di Indonesia. Keraguan *cardholder* untuk bertransaksi dengan *merchant* di Indonesia disebabkan dari aspek hukum dan perlindungan keamanan dalam bertransaksi di Indonesia tergolong lemah. Fenomena ini merupakan indikasi buruk dalam transaksi elektronik untuk mengatasi hal ini beberapa *merchant* sudah mencoba mencari pihak ketiga yang dapat dipercaya baik oleh penjual maupun *cardholder* sehingga transaksi dapat berjalan dengan lancar, dalam prakteknya *merchant* menggunakan Bank sebagai *Payment Gateway* dalam transaksi pembayaran yang menggunakan kartu kredit.

METODE

Beranjak dari permasalahan dan tujuan yang ingin dicapai, maka jenis penelitian ini adalah penelitian hukum normatif *(legal research)* atau penelitian hukum secara kepustakaan secara kepustakaan. Yang mana penelitian ini berupaya memecahkan permasalahan berkenaan dengan keabsahan perjanjian jual beli online yang ditelaah menggunakan bahan hukum dari aturan-aturan hukum yang ada dalam KUHPerdata dengan aturan-aturan hukum yang ada dalam Undang-undang Nomor 11 tahun

[6] Budi Agus Riswandi, *Hukum dan Internet di Indonesia*, UII Press, Jakarta, 2013, Hlm. 3.

2008 tentang Informasi dan Transaksi elektronik. Dalam hal ini berarti peneliti melakukan telaah terhadap peraturan hukum yang terkait dengan permasalahan ini dengan analisa berdasarkan data-data sekunder yang berupa bahan hukum primer maupun bahan hukum sekunder.

Penelitian ini merupakan penelitian hukum normatif dengan tipe penelitian berupa inventarisir aturan perundng-undangan. Artinya penelitian ini berupaya menyelesaikan permasalahan yang ada dngan cara melakukan identifikasi terhadap aturan hukum menurut KUHPerdata Indonesia dan aturan yang diatur dalam UU No. 11 Tahun 2008 tentang ITE, dalam kaitannya pula dengan dalam pelaksanaan hubungan jual beli secara *online* ini.

Sesuai dengan jenisnya, maka bahan-bahan hukum yang digunakan dalam penelitian ini diperoleh melalui studi kepustakaan, utamanya yang terkait dengan permasalahan transaksi elektronik yang menggunakan bank sebagai *payment gateway*. Inventarisasi terhadap peraturan perundang-undangan yang berlaku dilakukan untuk mengumpulkan bahan hukum primer, sedangkan pengumpulan bahan hukum sekunder dilakukan dengan teknik pengelompokkan bahan hukum secara studi kepustakaan, termasuk penelitian-penelitian terdahulu yang terkait dengan permasalahan yang diteliti dalam penelitian ini untuk mengetahui sampai ke mana ilmu yang berhubungan dengan penelitian telah berkembang, sampai ke mana terdapat kesimpulan dan degeneralisasi yang pernah dibuat.

Pengolahan bahan hukum dilakukan dengan mengadakan sistematisasi terhadap bahan-bahan hukum tertulis, yakni dengan membuat klasifikasi terhadap bahan-bahan hukum tertulis tersebut untuk memudahkan pekerjaan analisis dan konstruksi. Penelitian ini merupakan kajian hukum normatif yang pemecahan masalahnya dilakukan secara deskriptif-analitikal. Asas-asas hukum akan ditarik terlebih dahulu untuk kemudian dilakukan penelaahan serta pengkajian terhadap peraturan perundang-undangan yang

terkait dengan penelitian ini. Permasalahan kemudian akan diuraikan kembali untuk dianalisis secara kualitatif berdasarkan data sekunder untuk kemudian ditarik kesimpulan.

HASIL DAN PEMBAHASAN

A. Hukum Transaksi Elektronik

Internet merupakan suatu media informasi dan komunikasi yang membawa permasalahan hukum baru yang lebih kompleks bagi masyarakat. Internet menciptakan berbagai sistim perhubungan baru yang memerlukan keamanan mutakhir dalam prosesnya dan telah menjadi aspek penting dalam bisnis dan kehidupan sosial. Internet telah menjadi suatu kekuatan baru yang menopang pertumbuhan dan kekuatan bisnis di seluruh dunia. Saat ini suatu perusahaan tidak dapat tumbuh berkembang tanpa ditopang oleh kekuatan dan keamanan telekomunikasi kerana pada dasarnya internet digunakan untuk meningkatkan dan mempercepat proses serta memperlebar jaringan bisnis. Internet sudah menjadi alat yang paling diandalkan baik untuk keperluan pribadi maupun keperluan bisnis.

Transaksi elektronik *(electronic transaction)* di Indonesia sebenarnya sudah dilakukan semenjak internet mulai masuk pada tahun 1994 dan dimanfaatkan oleh sebagian kalangan, utamanya kalangan pelajar dan menengah, termasuk para pebisnis. Transaksi elektronik kerap dicampuradukkan dengan perdagangan elektronik *(electronic commerce)* atau e-dagang. E-dagang *(transaksi elektronik)* mengandung cakupan yang lebih luas yang mana juga meliputi transaksi elektronik. E-dagang atau transaksi elektronik merupakan bagian dari e-business, dimana cakupannya lebih luas yakni termasuk pengkolaborasian mitra bisnis, pelayanan nasabah, netiket dan lain-lain.

> *Transaction is a term used to describe the data exchange and data changes which occur as the result of an interaction*[7].

Transaksi adalah istilah yang digunakan untuk menggambarkan

[7] Francis Botto, *Dictionary of Multimedia and Internet Applications*, John Willey and sons, UK, 1999, hlm 313.

pertukaran data yang terjadi kerana adanya interaksi. Apabila mendapat tambahan kata elektronik menjadi "transaksi elektronik" maka menjadi transaksi yang bersifat elektronik dan digital. Akan tetapi definisi yang tepat apabila berkenaan dengan istilah perundangan adalah segala pertukaran data, informasi, atau catatan yang dihasilkan oleh alat elektronik (misalnya komputer) yang berkaitan dengan dua orang atau lebih yang memiliki dampak hukum.

Transaksi elektronik dalam prakteknya haruslah memiliki sistem pembayaran yang benar-benar aman sehingga konsumen dapat melakukan transaksi dengan aman dan nyaman tanpa merasa was-was. Di Indonesia pemerintah telah mengundangkan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang setidaknya telah menjadi payung hukum terhadap aktifitas dunia maya yang salah satu diantaranya mencakup tentang transaksi elektronik. Pasal 1 angka 2 undang-undang ini memberikan definisi atas transaksi elektronik sebagai perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.

UU ITE secara substantif pengaturan mengenai keabsahan dari informasi elektronik, dokumen dan tanda tangan elektronik tersebut telah diatur secara tegas tentang hal tersebut, yang mana dalam Pasal 5 ditentukan:

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah;
(2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia;
(3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini;

(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
   a. Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
   b. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notarial atau akta yang dibuat oleh pejabat pembuat akta.

Pasal 11 UU ITE menyebutkan, bahwa:

(1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:
   a. Data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
   b. Data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
   c. Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
   d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
   e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan
   f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap

Informasi Elektronik yang terkait.

(2) Ketentuan lebih lanjut tentang Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 12 UU ITE menyatakan bahwa:

(1) Setiap Orang yang melakukan pelanggaran ketentuan yang terkait dengan Tanda Tangan Elektronik, bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul;

(2) Pengamanan Tanda Tangan Elekronik sebagaimana dimaksud pada ayat (1) sekurang-kurangnya:

a. Sistem tidak dapat diakses oleh orang lain yang tidak berhak;

b. Penanda Tanganan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;

c. Penanda Tanganan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh Penyelenggara Tanda Tangan Elektronik atau pun cara lain yang layak dan sepantasnya harus segera memberitahukan kepada seseorang yang Penanda Tangan Elektronik dianggap mempercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:

1. Penanda tangan mengetahui bahwa data pembuat Tanda Tangan

Elektronik telah dibobol, atau;

2. Keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan resiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik, dan;

d. Dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

(2) Setiap orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat (1), bertanggungjawab atas segala kerugian dan konsekuensi hukum yang timbul.

Ada beberapa transaksi elektronik yang perlu sistem keamanan yang tinggi, diantaranya adalah transaksi e-dagang, transaksi keuangan, surat elektronik (e-mail), pertukaran file[8], tandatangan suatu kontrak bisnis, dan informasi suatu perusahaan agar tidak dapat diubah oleh orang lain, terutama informasi terkait rahasia perusahaan. Transaksi-transaksi yang dilakukan melalui jaringan internet sangat tergantung pada kepercayaan di antara para pihak yang terlibat. Hal ini terjadi karena transaksi melalui jaringan adalah transaksi dimana para pihak tidak berinteraksi secara fisik.

Unsur-unsur transaksi elektronik adalah :

1. Adanya sebuah transaksi;
2. Setiap transaksi itu dibuat melalui media elektronik;
3. Kehadiran pihak-pihak yang melakukan transaksi secara fisik tidak mutlak;

[8] David I. Bainbridge, *Introduction To Computer Law*, Pitman Publishing, UK, 1993, Hlm 198.

4. transaksi menggunakan system jaringan umum;
5. Sistem terbuka;
6. Transaksi tersebut dilakukan tanpa batas apapun;

Secara hukum, keamanan transaksi elektronik dapat dicapai dengan cara:

1. Memberikan sertifikasi kepada sistem, yang menunjukan bahwa sistem yang dipergunakan untuk transaksi elektronik tersebut dapat diandalkan keamanannya;
2. Mengimplementasikan sistem yang telah terbukti keamanannya (misalnya sudah terbukti sulit untuk ditembus hacker).

Dalam industri perbankan banyak sekali pihak-pihak yang terkait, di antaranya; direksi bank, nasabah, karyawan. Untuk pemanfaatan *internet* sebagai jaringan *online* bagi kegiatan di sektor perbankan pihak nasabah merupakan salah satu pihak yang perlu mendapatkan perhatian dan perlindungan hukum dalam transaksi pembayaran *e-banking*.

Hal ini sangat diperlukan mengingat transaksi pembayaran *e-banking* sangat berbeda dengan sistem yang dilakukan di sektor perbankan biasa. Dalam pelaksanaannya transaksi pembayaran *e-banking* seluruh dokumen umumnya sifatnya elektronik, penandatanganan juga bersifat elektronik *(digital signature)* dan proses transaksi itu sendiri bersifat *online*. Artinya pihak yang bertransaksi tidak bertemu secara langsung[9].

B. Bank Sebagai Payment Gateway

Bank sebagai lembaga pendukung dalam melakukan transaksi perdagangan, tentunya akan menjangkau media internet ini dengan alasan efisiensi dan kemudahan. Tetapi alasan ini nyatanya masih perlu dijawab dengan teknologi yang tersedia mengenai masalah internet. Faktanya menunjukan bahwa dengan berkembangnya *transaksi elektronik* juga memicu percobaan-percobaan

[9] Budi Agus Riswandi, *Hukum dan Internet di Indonesia*, UII Press, Jakarta, 2003, Hlm 5

kejahatan penipuan, terutama perdagangan yang bertransaksi melalui internet. Menurut sumber *National Consumer League,* tujuh persen dari pemakai internet mengalami penipuan kartu kredit. Tujuh persen tersebut senilai enam juta pemakai[10].

Bank dalam menjalankan fungsinya sebagai lembaga keuangan antara *(financial intermediary)* memberikan berbagai macam jasa, antara lain adalah jasa pembayaran *(payment).* Jasa pembayaran pada saat ini berkembang pesat kearah *electronic/internet payment system*. *Internet Payment system* menimbulkan berbagai permasalahan dari teknis maupun dari segi hukum. Permasalahan ini meliputi kerahasiaan, keutuhan pesan *(integrity),* identitas para pihak dan hukum yang mengatur transaksi tersebut. Permasalahan-permasalahan tersebut kemudian melalui penggembangan teknologi internet dikembangkanlah teknik kriptografi *(cryptography).*

Kriptografi dapat memenuhi kebutuhan umum suatu transaksi;

1. Kerahasiaan *(confidentiality)* dijamin dengan melakukan enkripsi (penyandian);
2. Keutuhan *(integrity)* atas data-data pembayaran dilakukan dengan has satu arah;
3. Jaminan atas identitas dan keabsahan *(authenticity)* pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan *password* atau sertifikat digital
4. *Non repudation* (tidak dapat disangkal), pengirim pesan tidak dapat menyangkal bahwa ia tidak pernah mengirim pesan tersebut.[11]

Ada dua katagori *encryption types* yang secara umum digunakan secara umum untuk sistem pembayaran. Metode pertama, menggunakan *symmetric-key*, yakni kunci untuk membuat pesan yang disandikan sama dengan kunci untuk

[10] Burton S. Kaliski Jr, A Layman's Guide to a Subset of ASN. 1, BER, and DER, dalam Arif *Priharsanta, Implementasi PrototipeProses Otorisasi Kartu Pembayaran Antara Merchant dan Payment Gateway Pada Protokol Secure Electronic Transaction*, Fakultas Ilmu Komputer Universitas Indonesia, Depok, 1991, hlm. 10.

[11] Abdul Halim Barkatullah, *Transaksi Konsumen dalam Bisnis e-Commerce*, Nusa Media, Bandung, 2009, hlm. 120.

membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimannya harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut-termasuk pihak-pihak yang tidak diinginkan– dapat membuat dan membongkar rahasia *ciphertext*-nya, melainkan masalah bagaimana menyampaikan kunci simetris tersebut kepada pihak yang diinginkan. Contoh alogritma kunci simetris yang terkenal adalah DES *(Data Encryption Standard)* dan RC-4.

Kedua, Kunci *Asimetris/public key*, yakni pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk deskripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu-dalam hal ini kunci privat- untuk melakukan pembongkaran terhadap sendi yang dikirim untuknya.

Globalisasi sistem keuangan telah diikuti oleh kecenderungan yang paralel, internasionalisasi perbankan *(internationalization of banking)* yang mengarah kepada konsolidasi globalisasi dari industri keuangan secara keseluruhan. (Jordi Canal, 1997: 242) Dibalik gencarnya fenomena internasional perbankan, Model-model jasa perbankan mengalami perkembangan yang sangat pesat seiring dengan proses globalisasi dan liberalisasi perdagangan. Aspek yang menarik untuk dicermati saat ini menyangkut pada sistem pembayaran di dunia perbankan.

Sistem pembayaran adalah instrumen sistem dan peraturan di mana agen mempertemukan pihak yang membayar dan menerima pembayaran. Bank yang mempunyai fungsi intermediari merupakan pelaku yang sangat penting dalam sistem pembayaran karena bank sebagai sumber hukum langsung yang memfasilitasi transfer dana antar agen. Seandainya sistem pembayaran diperluas dan disilang batas nasionalnya, maka akan menjadi perhatian global. Dengan membentuk peraturan pokok perbankan sebagai agen penegas

tidak hanya untuk individu, tetapi juga untuk bank-bank kecil.

Dalam sistem pembayaran ini sendiri dikenal minimal tujuh pihak yang terkait. Tujuh pihak itu di antaranya:

1. *Cardholder,* adalah orang yang menggunakan kartu pembayaran yang dikeluarkan oleh sebuah *issuer*;
2. *Issuer,* adalah suatu institusi ekonomi (bank) yang membuat rekening dan mengeluarkan kartu pembayaran bagi *cardholder.* Contoh *issuer* adalah bank-bank yang mengeluarkan kartu kredit seperti Bank Lippo, Bank BCA, BANK dan lain sebagainya;
3. *Merchant,* adalah orang yang menyediakan barang atau jasa untuk dipertukarkan dengan pembayaran, dalam hal ini pembayaran dilakukan melalui internet;
4. *Acquirer,* adalah suatu institusi ekonomi yang membuat rekening bagi *merchant* dan melakukan proses otorisasi kartu pembayaran yang diterima oleh *merchant* dari *cardholder.* Contoh *acquirer* adalah bank-bank yang menyediakan layanan otorisasi bagi toko-toko yang menerima pembayaran dengan kartu kredit seperti Bank Mandiri, BCA, CitiBank, dan lain sebagainya;
5. *Payment Gateway,* adalah suatu perangkat yang dioperasikan oleh *aquirer* atau pihak ketiga untuk memproses pesan pembayaran termasuk instruksi pembayaran dari *cardholder;*
6. Pemegang Merek, adalah suatu badan usaha yang mengambangkan sistem kartu pembayaran, yang melindungi, mempromosikan dan menciptakan aturan-aturan penggunaannya. Ada beberapa pemegang merek yang merupakan institusi ekonomi dan berperan sebagai issuer maupun *acquirer.* Contohnya pemegang merek yaitu Visa, MasterCard, Amex, dan sebagainya;
7. Pihak Ketiga, terkadang *acquirer* maupun issuer memilih pihak ketiga untuk menjalankan *payment gateway;*

Pada sistem pembayaran dengan sistem keamanan seperti

SSL, Algotitma Simetris, Kunci Publik Algoritma *merchant* tetap mendapatkan seluruh informasi kartu kredit *cardholder*. Kalau *cardholder* sering menggunakan kartu kreditnya di Internet, rasanya tidak aman kalau membiarkan informasi kartu kredit miliknya diketahui semua *merchant* yang pernah didatanginya. Oleh karena itu, pada perkembangan berikutnya di Internet muncul skenario pembayaran *"three-party"*.

Dalam skenario ini ada pihak ketiga yang dipercaya menjadi *payment gateway* (gerbang pembayaran), seolah-olah menjadi 'kasir' atau POS *virtual*. Tergantung pada merek dagangnya, kadang-kadang disebut pula sebagai *payment server*, *commerce service provider*, atau *authentication server*. Institusi yang menjadi *payment gateway* harus merupakan pihak yang dipercaya, dan sering kali *acquirer* bertindak sebagai *payment gateway*.

Cardholder memang memberikan informasi kartu kreditnya kepada *payment gateway*, tetapi *merchant* tidak akan pernah tahu informasi kartu kredit tersebut. Jadi pembayarannya malah lebih aman ketimbang dari transaksi kartu kredit yang tidak dilakukan di Internet. *Payment gateway*lah yang akan berhubungan dengan jaringan kartu kredit untuk melakukan proses otorisasi *on-line. Merchant* akan menyerahkan barang dagangannya kepada *cardholder*, kalau informasi kartu kredit *cardholder* sudah berhasil diotorisasi oleh *payment gateway*.

Contoh skenario transaksi yang '*three-party'* ini antara lain *CyberCash, Open Market* dan *Visa/Mastercard Secure Electronic Transaction (SET).* Yang diluncurkan pada tanggal 1 Februari 1996. Visa/Mastercard mempublikasikan bahwa mereka sudah mempelopori pengembangan sebuah standar teknis untuk menjamin keamanan transaksi kartu kredit melalui internet yang dikenal dengan nama *Secure Electronic Transaction* (SET).

Dalam melakukan transaksi online, dikenal 3 (tiga) metode pembayaran, yakni COD, transfer bank dan pembayaran dengan kartu kredit:

1. COD *(Cash on delivery)*

Pada metode ini, pihak konsumen dan pihak merchant bertemu secara langsung dan melakukan transaksi meskipun penawaran dan persetujuan penawaran dilakukan secara online. Metode ini memberikan rasa aman pada kedua belah pihak karena kemungkinan terjadinya kesalahpahaman ataupun penipuan sangatlah kecil. Kekurangannya adalah pihak konsumen dan merchant harus berada di dalam satu wilayah dan memakan waktu serta biaya yang lebih besar dibandingkan dengan metode lain. Metode ini tidak melibatkan bank sebagai pihak ketiga;

2. Transfer bank

   Metode transfer bank dilakukan dengan cara pihak konsumen mentransfer sejumlah uang ke rekening bank merchant, setelah transfer diterima, pihak merchant akan segera mengirimkan barang/melakukan jasa yang telah dibayar oleh pihak konsumen. Pada metode ini, bank hanya berperan sebagai perantara pengiriman uang. Kelemahan dari metode ini adalah pihak konsumen harus melakukan langkah-langkah untuk mentransfer uang, seperti misalnya ke bank atau melakukan phone-banking. Dari segi kepraktisan dirasa kurang karena bisa saja pada saat itu saldo tersimpan tidak mencukupi atau konsumen sedang berada di satu tempat yang tidak memungkinkan ia untuk melakukan transfer;

3. Pembayaran dengan kartu kredit

   Pembayaran dengan kartu kredit untuk saat ini adalah metode pembayaran yang paling praktis selama merchant bekerjasama dengan pihak yang menyediakan layanan tersebut. Pihak konsumen hanya perlu memasukkan kode kartu kreditnya dalam melakukan transaksi.

Dalam sistem pembayaran COD dan Transfer bank menurut penulis hal itu tidak menjadi permasalahan, sama dengan jual beli secara umum tetapi dalam sistem pembayaran yang menggunakan *credit card* yang perlu mendapat perhatian, mengenai keamanan pembayarannya agar konsumen tidak merasa takut atau khawatir terjadinya kejahatan kartu kredit. Berikut adalah contoh pembayaran dengan menggunakan kartu kredit di salah satu merchant online.

Dalam sistem pembayaran ini sistem keamanan pembayaran kartu kredit yang menggunakan bank sebagai *payment geteway* (gerbang pembayaran).Dalam skenario transaksi ini, *cardholder* tetap memilih barang-barang yang dibelinya dari *website* penjual. Setelah terkumpul semua, penjual membuatkan slip pembelian. Kemudian, penjual meneruskan slip pembelian dengan teknik enkripsi sederhana ke *payment gateway* yang bertindak sebagai kasir. Pada saat masuk ke *payment gateway* inilah, dibuat saluran komunikasi aman, seperti SSL antara *payment gateway* dengan *cardholder*. *Cardholder* akan memberikan informasi kartu kreditnya kepada *payment gateway* dalam 'slip pembayaran'. *Payment gateway*lah yang kemudian akan memberitahukan kepada penjual apakah suatu transaksi sudah berhasil diotorisasi atau belum. Jadi penjual tidak penah membaca informasi nomor kartu kredit *cardholder*. Salah satu ciri skenario perdagangan ini yang nampak pada *browser* yang dipakai *cardholder* adalah URL yang dipergunakan oleh *payment gateway* (saat memasukkan informasi kartu kredit) berbeda dengan URL *website merchant*.

Perintah melalui kartu kredit *(credit card orders),* cardholder yang menggunakan web dengan perintah pengisian informasi cardholder dan menunjukan nomor kartu kredit mereka. SSL sebagai teknologi yang melindungi nomor kartu.

Waktu tersebut dibutuhkan dengan menggunakan 120 komputer jalan paralel, tapi yang harus diperhatikan dalam menilai keamanan adalah teknologi yang selalu berkembang dari waktu-kewaktu karenanya dalam sistem

keamanan harus memperhatikan perkembangan teknologi dan selalu disesuaikan dengan keadaan pada saat itu, dalam pengamanannya bank juga menggunakah *Firewall* sebagai pagar yang mencegah akses illegal ke jaringan perbankan, yang mengitari sistem. Dalam pengamanannya bank menggunakan *Veri Sign* sebagai *Certification Authority* yang merupakan *Certification Authority* yang dapat dipercaya dan www.jatis.com yang menyediakan jasa sistem internet yang menghubungkan *merchant* dan bank dalam transaksi yang menggunakan kartu kredit.

Oleh karena itu *merchant* hendaknya bekerjasama dengan perbankan sebagai gerbang pembayaran yang telah memiliki sistem keamanan yang handal. Dalam kaitannya dengan tanggung jawab pelaku usaha tersebut, UU ITE telah mengaturnya secara tegas, yang dalam Pasal 9 ditentukan: Pelaku usaha yang menawar produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen dan produk yang ditawarkan. Lalu, dalam penjelasannya dijelaskan bahwa: Yang dimaksud dengan "informasi yang lengkap dan benar" meliputi:

1. Informasi yang memuat identitas serta status subjek hukum dan kompetensinya, baik sebagai produsen, pemasok, penyelenggara maupun perantara;
2. Informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.

Pasal 10 UU ITE menyebutkan:

(1) Setiap pelaku usaha yang menyelenggarakan transaksi elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.

(2) Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan tersebut akan diatur dengan Peraturan Pemerintah (PP).

Atas dasar isi ketentuan Pasal 9 dan Pasal 10 beserta penjelasannya dapat dikemukakan bahwa pelaku usaha bertanggung jawab atas segala data dan dokumen yang telah diinformasikan melalui jaringan informasi elektronik secara lengkap dan benar serta patut dipercaya keakuratan dan kehandalanya.

Jadi dalam sistem keamanan yang disediakan bank sebagai *Payment Gateway* dalam transaksi elektronik dapat penulis katakan bank seharusnya penyediakan sistem yang aman, dan yang harus diperhatikan adalah teknologi yang digunakan harus selalu diperbaharui dengan mengikuti berkembang teknologi yang selalu berkembang.

Sebagai lembaga keuangan, bank harus mendapatkan kepercayaan dari masyarakat, dan kepercayaan masyarakat itu akan lahir apabila semua data *cardholder* pada bank dapat tersimpan secara tertutup, rapi dan dirahasiakan. Hal ini membawa konsekuensi kepada bank, yaitu bank memikul kewajiban untuk menjaga rahasia *cardholder*, sebagai timbal balik dari kepercayaan yang diberikan *cardholder* kepada bank selaku lembaga keuangan yang menjadi gerbang pembayaran.

Bank sebagai *payment gateway* berkewajiban untuk menjaga kerahasian data kartu kredit *cardholder*, apabila bank tidak menjaga kerahasiaan ini maka bank dapat dituntut baik secara perdata maupun pidana.

C. **Hubungan Hukum Antara Para Pihak Dalam Transaksi Elektronik yang Menggunakan Bank Sebagai *Payment Gateway***

Hubungan hukum yang ada dengan menggunakan kartu kredit sebagai alat pembayaran. Pada penggunaan kartu kredit, secara serentak bekerja tiga perjanjian yang satu sama lain saling terpisah, yaitu:

1. Perjanjian antara *merchant* dengan bank sebagai *payment gateway*;
2. Perjanjian antara *merchant* dengan perusahaan penerbit kartu kredit, yang berdasarkan perjanjian itu penjual yang bersangkutan setuju untuk menerima pembayaran yang menggunakan kartu itu;

3. Perjanjian antara perusahaan penerbit kartu kredit dan Bank.

Perjanjian pengadaan pembayaran dengan kartu kredit merupakan perjanjian bisnis ke bisnis (*business to business contract).*

Kedudukan hukum antara *merchant* dengan bank selaku *payment gateway* sebagai gerbang pembayaran bagi *cardholder* yang menggunakan kartu kredit. Hubungan ini adalah pemberian kuasa khusus dengan mendapatkan upah, oleh karena itu bank (*payment gateway)* sebagai si kuasa memberiikan tindakan-tindakan yang dapat dilakukan oleh seseorang penerima kuasa hanya terbatas pada hal-hal yang dikuasakan kepadanya, yakni:

1. Melaksanakan kuasanya (Pasal 1800 KUH Perdata) sebagai kasir yang menerima pembayaran dan melakukan otorisasi *online* dengan jaringan kartu kredit dalam jalur yang aman, Bank juga berkewajiban menjaga kerahasiaan kartu kredit *cardholder*;
2. Bertanggung jawab tentang perbuatan-perbuatan yang dilakukan dengan sengaja, bertanggung jawab tentang kelalaian-kelalaian yang dilakukan dalam menjalankan kuasanya; (Pasal 1801 KUH Perdata);
3. Memberi laporan kepada *merchant* sebagai si pemberi kuasa tentang apa yang telah diperbuatnya;(1802)
4. Tidak bertanggung jawab tentang apa yang telah terjadi diluar batas kuasa itu. (Pasal 1806 KUH Perdata);
5. *Merchant* sebagai Pemberi kuasa berkewajiban sebagai berikut:
    1. Memberi persekot dan biaya-biaya yang telah dikeluarkan bank sebagai si kuasa untuk melaksanakan kuasanya, (Pasal 1808 KUH Perdata) dan *merchant* mempunyai *account* pada Bank untuk menerima pembayaran dari *cardholder*, setelah dikurangi biaya (tanggungan *merchant)* yang disebut *discoun fe;*

2. Membayar upah kuasa yang telah diperjanjikan dengan memberikan komisi dengan bank dalam setiap transaksi yang diatur dalam perjanjian antara mereka; (Pasal 1808 KUH Perdata);
3. Memberi ganti-rugi kepada si kuasa tentang kerugian-kerugian yang diderita sewaktu menjalankan kuasanya; (Pasal 1809 KUH Perdata);
4. Bank sebagai si kuasa berhak menahan segala kepunyaan *merchant* sebagai si pemberi kuasa yang berada ditangannya, sampai dibayar lunas segala hak-hak si kuasa (hak retensi). (Pasal 1812 KUH Perdata).

Pemberian kuasa ini berakhir apabila:

1. Ditarik kembali kuasa bank oleh *merchant* sebagai pemberi kuasa; (Pasal 1813 KUH Perdata);
2. Dengan pemberitahuan penghentian kuasanya oleh bank sebagai si kuasa; (Pasal 1817 KUH Perdata);
3. Pailitnya *merchant* sebagai si pemberi kuasa atau bank sebagai si kuasa.

Pada metode pembayaran dengan menggunakan kartu kredit (*credit card)*, merchant mengambil langkah yang tepat dengan menarik bank sebagai *three party payment*/*payment gateway* sehingga merchant tidak mengetahui nomer kartu kredit konsumen maka konsumen merasa aman dari pencurian kartu kredit dan percaya bahwa dalam bertransaksi dengan merchant adalah aman, keuntungan bagi merchant dia tidak mengurusi masalah pembayaran itu dan tugasnya hanya memeriksa apakah ada transaksi dengan konsumen dan *cross chek* dengan bank yang bersangkutan apakah kartu kredit yang digunakan valid serta bank yang menjamin keamanan transaksi ini, sehingga dia terlepas dari segala resiko dan merchant di percaya oleh konsumen.

PENUTUP

Berpijak dari uraian

sebelumnya dapat dikemukakan beberapa kesimpulan, sebagai berikut:

1. Transaksi elektronik dalam praktiknya haruslah memiliki sistem pembayaran yang benar-benar aman sehingga konsumen dapat melakukan transaksi dengan aman dan nyaman tanpa merasa was-was. Pada metode pembayaran dengan menggunakan kartu kredit (*credit card),* merchant di Indonesia sebaiknya menarik bank sebagai *three party payment*/*payment gateway* untuk menjaga kerahasiaan dan keamanan, karena bank dapat diandalkan sebagai lembaga yang dapat menjaga keamanan dalam sistem pembayaran bertransaksi elektronik;
2. Dalam pengamanan transaksi bank sebagai *payment gateway* haruslah meggunakan sistem keamanan yang handal, dan adanya *certification authority* dengan mengkombinasikan *three party payment system* serta menggunakah *Firewall* sebagai pagar yang mencegah akses illegal ke jaringan perbankan, yang mengitari sistem;
3. Kedudukan hukum antara *merchant* dengan bank selaku *payme9nt gateway* sebagai gerbang pembayaran bagi *cardholder* yang menggunakan kartu kredit. Hubungan ini adalah pemberian kuasa khusus dengan mendapatkan upah, oleh karena itu bank (*payment gateway)* sebagai si kuasa hanya dapat melakukan tindakan-tindakan sebagai penerima kuasa hanya terbatas pada hal-hal yang dikuasakan kepadanya.

DAFTAR PUSTAKA

Adnan, Muhammad Aulia , *Aspek Hukum Protokol Pembayaran Visa/Mastercard Secure Electronic Transaction (SET),* Fakultas Hukum Universitas Indonesia, 2010.

Anwar, Jusuf, *Aspek-aspek Hukum Keuangan dan Perbankan*, Suatu Tinjauan Praktis, disampaikan pada Lokakarya Pembangunan Hukum Nasional VIII Departemen Hukum dan HAM, Badan Pembinaan Hukum Nasional, Denpasar 14-18 Juli 2009.

Bainbridge, David I, *Introduction To Computer Law*, Pitman Publishing, UK, 1993.

Bainbridge, David I, LLB, Ceng,MBCS, MICE, *Introduction to Computer Law*, Pitman Publishing, London 1993.

Bajaj, Kamlesh K, & Debjani Bag, *C-commerce The Cutting Edge of Business*, diterjemahkan oleh Imam Mawardi, Surabaya, PT. Akana Press Offset, 2010.

Barkatullah, Abdul Halim, *Transaksi Konsumen dalam Bisnis e-Commerce*, Nusa Media, Bandung, 2009.

Botto, Francis, *Dictionary of multimedia and internet applications*, John Willey and sons, UK, 1999.

Ferrera, Gerald R, dan Stephen D Lichstein, Margo E.K Reder, Ray August, Willian T Schiano, *Technology and Cyberlaw, Text and Cases*, South Western College Publishing, United States, 2011.

Kaliski Jr, Burton S., A Layman's Guide to a Subset of ASN. 1, BER, and DER, dalam Arif *Priharsanta, Implementasi PrototipeProses Otorisasi Kartu Pembayaran Antara Merchant dan Payment Gateway Pada Protokol Secure Electronic Transaction, Fakultas Ilmu Komputer Universitas Indonesia*, Depok, 1991.

Riswandi, Budi Agus, *Hukum dan Internet di Indonesia*, UII Press, Jakarta, 2013.