PERLINDUNGAN TRANSAKSI ELECTRONIC COMMERCE MELALUI LEMBAGA ASURANSI

Oleh: Elisatris Gultom, S.H., M.H.[1]

Abstrak

Era Globalisasi yang ditandai dengan meningkatnya perkembangan teknologi komunikasi dan informasi, telah memberikan pengaruh positif pada seluruh aktivitas manusia, tidak terkecuali di sektor perekonomian. Salah satu pengaruh teknologi komunikasi dan informasi di sektor perekonomian adalah mulai dipergunakannya electronic commerce. Sekalipun banyak keuntungan yang diperoleh melalui electronic commerce, khususnya ditinjau dari aspek jarak, dan waktu, namun tidak berarti e. commerce bebas dari terjadinya risiko-risiko yang dapat merugikan para pihak, utamanya pihak konsumen, sehingga diperlukan adanya suatu sistem keamanan yang baik. Sistem pengamanan transaksi yang banyak dipakai adalah teknologi kriptografi (cryptography) dan Secure Electronic Transction (SET). Namun sistem keamanan ini pun tidak luput dari kelemahan, karena masih dimungkinkan seseorang menembus sistem tersebut. Jika pihak-pihak dalam e-commerce bermaksud mengurangi risiko akibat masuknya pihak lain ke dalam sistem jaringan keamanan, mereka harus mencari cara untuk mengatasinya. Hasil penelitian menunjukkan bahwa perjanjian asuransi dapat digunakan untuk mengurangi risiko yang dapat terjadi akibat masuknya pihak lain ke dalam sistem keamanan e. commerce, sepanjang perjanjian tersebut tidak menyalahi prinsip-prinsip asuransi sebagaimana diatur dalam Kitab Undang-Undang Hukum Dagang. Mengingat perjanjian asuransi yang dibuat termasuk golongan asuransi kerugian maka pembuktiannya dapat mengacu kepada ketentuan Pasal 257 dan 258 Kitab Undang-Undang Hukum dagang.

A. Latar Belakang

Teknologi informasi atau *information technology* (IT) telah mengubah paradima dalam beraktivitas, telah menciptakan jenis-jenis dan peluang-peluang bisnis yang baru, serta menciptakan jenis pekerjaan dan karier baru dalam

---

[1] *Staf pengajar Fakultas Hukum Universitas Padjadjaran Bandung.*

pekerjaan manusia.[2] Gambaran ini hanyalah sebagian kecil dampak positif dari berkembangnya teknologi informasi.

Salah satu bagian yang paling berkembang pesat dari bidang teknologi informasi adalah internet (*interconnection networking*), yang semula hanya diperuntukkan sebagai media penyebaran informasi, namun pada beberapa dasawarsa terakhir ini telah merambah ke bidang lain, salah satunya di bidang ekonomi, sehingga kemudian muncul istilah seperti *electronic commerce (e-commerce)*

Keuntungan dari *e-commerce* adalah memberikan kenyamanan bagi konsumen dalam bertransaksi karena konsumen tidak harus bertemu secara fisik. Kosumen dapat bertransaksi diberbagai macam toko *(online store)* selama 24 jam sehari dan tujuh hari seminggu, dengan akses yang sangat cepat sehingga memudahkan pembeli (konsumen) untuk membandingkan harga dan melakukan pembelian, tanpa harus meninggalkan rumah atau kantor. Dalam hitungan detik, konsumen pun dapat dengan cepat memperoleh barang atau jasa yang mereka inginkan, seperti *e-book*, musik, atau piranti lunak komputer.

Bagi penjual, *e-commerce* menawarkan jalan untuk memotong biaya pengeluaran dan kemudahan dalam mengembangkan jaringan toko mereka. Penjual tidak harus mendirikan sebuah gedung, merekrut pegawai, atau mengatur dan merawat toko. Pemesanan dan pencatatan keuangan dilakukan dengan menerapkan sistem tertentu sehingga dapat memangkas biaya tambahan.

Sekalipun internet terbukti telah memberikan berbagai kemudahan bagi para pelaku bisnis, utamanya bagi konsumen, namun dalam praktiknya tidak luput dari risiko yang merugikan. Sistem keamanan yang melingkupi jaringan internet ternyata potensial untuk dimasuki oleh pihak-pihak yang tidak bertanggung jawab. Hal ini mendorong pemikiran untuk dibangunnya suatu sistem yang dapat mengamankan transaksi *e-commerce*. Salah satunya dengan menggunakan teknologi kriptografi (*cryptography*). Beberapa penyedia jasa *e-commerce* pun mengembangkan teknologi mereka masing-masing, salah satunya adalah *secure electronic transaction* (SET) yang dikembangkan oleh Visa dan Master Card.

Teknologi *secure electronic transaction* adalah protokol pengaman transaksi yang dikembangkan oleh Visa dan Mastercard khususnya untuk mengamankan transaksi kartu kredit melalui internet. SET adalah sistem yang

---

[2] Sutan Remy Sjahdeini, *Hukum Siber Sistem Pengamanan E-commerce*, makalah dalam seminar tentang Peran Penegak Hukum Dalam Kaitannya Dengan Transaksi Perbankan" yang diselenggarakan oleh Bank Mandiri pada hari Kamis, 18 Januari 2001 di Mandiri Club Jakarta, hlm. 1.

paling umum dipakai sebagai sistem keamanan, sistem ini diharapkan menjadi standar internasional dalam pembentukan sistem pengamanan dalam *e-commerce*. Namun sebenarnya risiko pencurian dan manipulasi dapat juga terjadi pada sistem ini.

Untuk mengatasi risiko kerugian akibat ditembusnya sistem pengamanan dalam *e-commerce,* para pihak berupaya menemukan cara mengatasinya, salah satunya melalui lembaga asuransi. Melalui asuransi, risiko yang sejatinya diderita oleh para pihak yang bertransaksi dialihkan kepada pihak lain yaitu perusahaan asuransi.

B. Permasalahan

1. Bagaimana eksistensi perjanjian asuransi dalam transaksi *electronic commerce* ditinjau dari Kitab Undang-Undang Hukum Dagang?
2. Bagaimana pembuktian adanya perjanjian asuransi dalam transaksi *e-commerce* dihubungkan dengan ketentuan Kitab Undang-Undang Hukum Dagang?

C. Metode Penelitian

Penelitian ini menggunakan metode pendekatan yuridis normatif, yaitu penelitian terhadap asas-asas hukum[3] yang dilakukan dengan menitikberatkan pada penelitian kepustakaan *(library research)* untuk mendapatkan data sekunder, sedangkan spesifikasi penelitian bersifat deskriptif analitis yaitu berupa penggambaran terkait perjanjian asuransi dalam transaksi e.commerce dengan menggunakan kunci-kunci kriptografi dan *secure electronic transaction* (SET). Selanjutnya, hasil penggambaran tersebut dianalisis sehingga dapat digunakan untuk membantu dalam menjawab berbagai permasalahan yang ada.

D. Tinjauan Pustaka

E-commerce pada dasarnya sama dengan jual beli konvensional, pembeli dan penjual bertemu untuk mempertukarkan barang atau jasa dengan uang. Namun berbeda dengan jual beli konvensional, dalam *e-commerce* pembeli dan penjual melakukan transaksi bisnis dengan menggunakan jaringan komputer.

---

[3] Soetandyo Wignjosoebroto, penelitian tipe ini disebut dengan istilah "studi dogmatik" atau Penelitian doktrinal (lihat tulisannya "Penelitian Hukum: Sebuah Tipologi" pada Majalah Masyarakat Indonesia, Tahun ke-I No. 2, 1974, hlm. 92-94).

Sutan Remy Sjahdeini[4] mendefinisikan *e-commerce* yaitu: *kegiatan bisnis yang menyangkut konsumen (consumers), manufaktur (manufactures), service providers, dan pedagang perantara (intermediaters) dengan menggunakan jaringan-jaringan komputer (computer networks) yaitu internet.*

Secara umum, pihak-pihak yang terlibat dalam *e-commerce* antara lain Pembeli atau *cardholder*; Penjual atau *merchant; Issuer* atau lembaga penerbitkan kartu pembayaran; *Acquirer* adalah lembaga keuangan penjual dan yang memproses otorisasi kartu pembayaran dan pembayaran-pembayaran; *Payment Gateway,* yaitu sarana yang dioperasikan oleh acquirer atau pihak ketiga yang ditunjuk untuk memperoses pesan pembayaran penjual, termasuk perintah pembayaran; jasa pengiriman; dan lembaga otoritas sertifikat atau *certification authorities*, yaitu lembaga yang dipercaya untuk mengeluarkan sertifikat digital guna mengamankan transaksi.

Jenis-jenis kegiatan *e-commerce* antara lain:

1. Transaksi Barang
   Sebuah toko maya atau *Cybershop* biasanya memiliki katalog elektronik yang menjelaskan dan memperlihatkan produk yang akan dijual. Konsumen dapat mencari barang tertentu atau secara acak mencari di katalog elektronik yang dapat memuat lebih banyak produk dibanding katalog cetak biasa.
2. Transaksi jasa
   Bentuk bisnis *e-commerce* lain adalah menjual jasa. Jasa pembiayaan mewakili sebagian besar usaha *e-commerce*. Transaksi jasa lainnya adalah penjualan tiket, konsultasi kesehatan, hukum, dan sebagainya.
3. Lelang
   Beberapa situs *e-commerce* mengkhususkan diri untuk mempertemukan pembeli dan penjual, tidak hanya untuk menjual barang milik mereka sendiri tetapi juga milik orang lain melalui sistem lelang.
4. Transaksi *Bussines-to-Business*
   Transaksi *Bussines-to-Business* atau B-to-B merupakan salah satu bagian dari *e-commerce* yang berkembang pesat. Dalam transaksi ini pelaku umumnya dari kalangan pebisnis yang menggunakan barang yang dibelinya bukan untuk digunakan sendiri.

[4] Sutan Remy Sjahdeini, *op. cit*

Sebagaimana telah dikemukakan pada bagian awal bahwa *e-commerce* telah berkembang sangat pesat, jutaan dolar tiap harinya telah berpindah tangan melalui cara ini. Untuk menjadikan hal tersebut lebih berkembang, maka perlu ada system yang menjamin konsumen memperoleh perlindungan dalam bertransaksi. Kebutuhan perlindungan yang demikian ini menjadi sangat tinggi apabila menyangkut pesan elektronik yang sangat rahasia.[5]

Pada prinsipnya, sistem pengamanan terhadap komunikasi elektronik harus dapat memberikan perlindungan terhadap hal-hal sebagai berikut:[6]

1. Pengubahan, penambahan atau perusakan oleh pihak yang tidak bertanggung jawab terhadap data dan informasi, baik selama dalam penyimpanan maupun selama proses transmisi oleh pengirim kepada penerima; dan
2. Perbuatan yang tidak bertanggung jawab yang berusaha untuk dapat memperoleh informasi yang dirahasiakan, baik diperoleh langsung dari penyimpanannya maupun ketika ditransmisikan oleh pengirim kepada penerima (upaya penyadapan).

Menurut Budi Rahardjo, sistem pengamanan komunikasi elektronik harus dapat mengakomodasi kebutuhan pengamanan yang berkaitan dengan aspek-aspek:[7]

1. *Confidentiality*
   Menyangkut kerahasiaan dari data atau informasi, dan perlindungan bagi informasi tersebut dari pihak yang tidak berwenang. Untuk melindungi kerahasiaan maka dilakukan dengan cara membuat informasi itu "tidak dapat dipahami" (*unintelligible*), isi dari informasi itu harus ditransformasikan sedemikian rupa sehingga tidak dapat dipahami (*undecipherable*) oleh siapapun yang tidak mengetahui prosedur dari proses transformasi itu.
2. *Integrity*
   Integrity menyangkut perlindungan data terhadap usaha membuat modifikasi data itu oleh pihak-pihak yang tidak bertanggung jawab, baik selama data itu disimpan maupun selama data itu dikirimkan kepada pihak lain.

---

[5] Kamlesh K Bajaj dan Debjani Nag, *E-Commerce: Cutting Edge of Business*, New Dehli: Tat Mc Graw-Hill Publishing Limited, 2000, hlm. 427.
[6] Sutan Remy Sjahdeini, *op. cit.*
[7] Budi Rahardjo, *Keamanan Sistem Informasi Berbasis Internet*, PT . Insan Komunikasi, Bandung, 2000, hlm.11.

3. *Authorization*
   Authorization menyangkut pengawasan terhadap akses kepada infomasi tertentu.
4. *Availability*
   Informasi yang disimpan atau ditransmisikan melalui jaringan komunikasi harus dapat tersedia sewaktu-waktu apabila diperlukan.
5. *Authenticity*
   Authenticity atau *authentication* menyangkut kemampuan seseorang, organisasi, atau komputer untuk membuktikan identitas dari pemilik yang sesungguhnya dari informasi tersebut.
6. *Non-repudiability of Origin* atau *Non-repudiation*
   Non-repudiability of Origin atau *Non-repudiation* menyangkut perlindungan terhadap suatu pihak yang terlibat dalam suatu transaksi atau kegiatan komunikasi yang di belakang hari pihak tersebut menyanggah bahwa transaksi atau kegiatan tersebut benar telah terjadi.
7. *Auditability*
   Data harus dicatat sedemikian rupa, bahwa data tesebut telah memenuhi semua syarat *confidentiality* dan *integrity* yang diperlukan, yaitu bahwa pengiriman data tersebut telah dienkripsi[8] (*encrypted*) oleh pengirimnya dan telah didekripsi (*decrypted*) oleh penerimannya sebagaimana mestinya.

Dalam pengamanan *e-commerce*, data enkripsi memerankan 4 fungsi penting yaitu:

1. Autentikasi secara digital memungkinkan para pihak, pembeli dan penjual, yakin mereka bertransaksi dengan orang yang benar.
2. Memberikan jaminan kepastian bahwa data yang diterima tidak mengalami perubahan oleh pihak ketiga.
3. Menghindari tindakan penyangkalan, pembeli maupun penjual, bahwa mereka tidak pernah menerima atau mengirim informasi atau pesanan.
4. Bila terjadi gangguan oleh pihak ketiga, enkripsi menjamin hak privasi dari campur tangan pihak ketiga yang ingin membaca dan atau menggunakan informasi milik konsumen untuk kepentingan mereka sendiri.

Atas dasar kebutuhan akan pengamanan, *e-commerce* membutuhkan enkripsi sebagai sistem pengaman untuk melindungi pihak-pihak yang bertransaksi.

---

[8] Enkripsi adalah proses menyalin ulang pesan atau data ke dalam bentuk yang tidak dapat dibaca tanpa proses *decrypting* terhadap pesan atau data yang dienkripsi.

Ada 2 metode enkripsi yang dikembangkan dan digunakan *e-commerce* yaitu:[9]

1. *Private-key encryption* (*secret-key* atau *symmetric encryption*) dimana pemakainya berbagi kunci yang umum. Didasarkan pada *Single Secret Key* yang digunakan oleh kedua belah pihak yang terlibat dalam suatu hubungan komunikasi. Dengan kata lain, kunci yang sama sama untuk melakukan dekripsi (*decryption*).

2. *Public-Key Encryption*, yang juga dikenal sebagai *Asymmetric Encryption*, di sini digunakan 2 kunci yang berbeda untuk melakukan enkripsi dan dekripsi. Ke 2 kunci yang berpasangan itu adalah *Private Key* dan *Public Key*.

Secure Electronic Transaction (SET) merupakan sistem keamanan jaringan yang akan menjadi standar sistem keamanan dimasa mendatang. Para pihak yang terlibat dalam *secure electronic transaction* antara lain:[10]

a. Pembeli atau *cardholder*, dalam *e-commerce* pembeli umumnya berhubungan dengan penjual menggunakan komputer pribadi atau *personal computer*. Dalam transaksi tersebut pembeli menggunakan kartu yang dikeluarkan oleh *Issuer*. Disinilah peran SET menjamin agar jalannya transaksi berjalan lancar.
b. *Issuer* atau lembaga keuangan dimana pembeli menjadi nasabah, dan menerbitkan kartu pembayaran. *Issuer* menjamin pembayaran atas transaksi yang menggunakan kartu pembayaran yang dikeluarkannya.
c. Penjual atau *merchant* adalah pihak yang menawarkan barang atau jasa kepada pembeli. Dalam SET, Penjual dapat menyarankan kepada pembeli untuk melakukan transaksi yang aman.
d. *Acquirer* adalah lembaga keuangan dimana penjual menjadi nasabahnya dan memproses autorisasi kartu pembayaran dan pembayaran-pembayaran.
e. *Payment Gateway,* adalah sarana yang dioperasikan oleh a*cquirer* atau pihak ketiga yang ditunjuk untuk memperoses pesan-pesan pembayaran penjual, termasuk intruksi pembayaran.
f. Otoritas sertifikat atau *Certification Authorities*, yaitu lembaga yang dipercaya, dan mengeluarkan sertifikat-sertifikat dan ditandatangani olehnya.

---

[9] Sutan Remy Sjahdeini, *op. cit.*

[10] Arrianto Mukti Wibowo, *Kerangka Hukum Digital Signature Dalam Electronic Commerce,* makalah dipresentasikan di hadapan Masyarakat Telekomunikasi Indonesia pada bulan Juni 1999 di Pusat Ilmu Komputer Universitas Indonesia , Depok, Jawa Barat.

g. Jasa Pengiriman, yaitu pihak yang bergerak dibidang jasa pengiriman barang, seperti truk, kapal ataupun pesawat, dalam hal ini ia bertugas mengirimkan barang dari penjual kepada pembeli.

Dalam alur *secure electronic transaction* pembeli dianggap telah memiliki *browser* yang mendukung SET, seperti Netscape atau Microsoft's Internet Explorer, sementara penyedia transaksi, seperti bank, toko, dan lain-lain menggunakan atau mendukung sebagai "SET *Server*", maka alur transaksi yang terjadi adalah sebagai berikut:

a. Pembeli membuka *account* kartu kredit dari *issuer*, umumnya Bank.
b. Pembeli menerima sertifikat digital atau *digital certificate.* Data elektronik ini berfungsi sebagai kartu kredit dalam pembelian *online* atau transaksi lainnya.
c. Pihak penjual juga menerima sertifikat dari bank. Sertifikat ini sudah termasuk kunci publik milik penjual dan milik bank.
d. Pembeli memesan barang atau jasa melalui *web page*, telephone, atau cara lainnya.
e. *Browser* milik pembeli menerima dan mendapat pemberitahuan dari sertifikat milik penjual bahwa penjual adalah pihak yang sah.
f. *Browser* mengirimkan informasi pemesanan.
g. Penjual memeriksa pembelinya dengan melihat terlebih dahulu tandatangan digital milik pembeli yang sah dalam sertifikat milik pembeli.
h. Penjual mengirim pesan pemesanan ke bank. Di dalamnya termasuk kunci publik milik bank, informasi pembayaran dari pembeli yang mana penjual tidak dapat men-*decode*-nya, dan sertifikat milik penjual.
i. Bank memeriksa penjual dan pesan yang dikirimkannya. Kemudian bank menggunakan tandatangan digital yang tertera dalam sertifikat dengan pesan dan memeriksa bagian pembayaran yang terdapat pada pesan tersebut.
j. Bank menandatangani secara digital dan mengirim otorisasi kepada penjual.
k. Penjual memenuhi pesanan barang atau jasa dengan mengirimkan barang melalui jasa pengangkutan.

Dengan memperhatikan gambaran di atas, lembaga otoritas sertifikat akan berkedudukan sebagai pihak ketiga yang menjamin keamanan identitas para pihak yang bertransaksi. Informasi yang terdapat dalam sertifikat yang diterbitkan lembaga otoritas sertifikat dapat berupa:

a. Identitas lembaga otoritas sertifikat yang menerbitkannya.
b. Pemegang atau pemilik atau *subscriber* dari sertifikat tersebut.
c. Batas waktu berlaku sertifikat tersebut.
d. Kunci publik dari pemilik sertifikat.

Pembobolan atas sistem *secure electronic transaction* mungkin saja terjadi, tergantung pada panjangnya kunci-kunci yang dipakai. Semakin panjang kunci maka semakin lama pula untuk ditembus.

Beberapa ancaman dan serangan yang dapat terjadi pada sistem keamanan jaringan komputer, adalah:[11]

1. Ancaman keamanan:
   a. *Leakage* (Kebocoran), pengambilan informasi oleh penerima yang tidak berhak.
   b. *Tampering*, pengubahan informasi yang tidak legal.
   c. *Vandalism* (perusakan), gangguan operasi sistem tertentu. Pelaku tidak mengharap keuntungan apapun.
2. Serangan pada sistem terdistribusi tergantung pada akses ke saluran komunikasi yang ada atau membuat saluran baru yang menyamarkan (*masquerade*) sebagai koneksi legal.
3. Penyerangan pasif, hanya mengamati komunikasi atau data.
4. Penyerangan aktif, secara aktif memodifikasi komunikasi atau data, seperti Pemalsuan atau pengubahan *e-mail* dan *IP Spoofing*.

Setelah menguraikan gambaran sistem pengamanan dalam *e-commerce*, selanjutnya akan dibahas tentang pengaturan asuransi di Indonesia sebagai lembaga yang diharapkan mampu mengalihkan risiko jika terjadi kerugian akibat masuknya pihak lain dalam sistem keamanan *e-commerce*.

Eksistensi asuransi di Indonesia diatur secara tersebar dalam beberapa perundang-undangan di antaranya: Kitab Undang-Undang Hukum Perdata (KUHPerdata), Kitab Undang-Undang Hukum Dagang (KUHD), Undang-Undang Republik Indonesia Nomor 2 Tahun 1992 Tentang Usaha Perasuransian.

Pengertian asuransi (kerugian) diatur secara jelas di dalam Pasal 246 Kitab Undang-Undang Hukum Dagang (KUHD) yang menyatakan:

> *"Asuransi atau pertanggungan adalah suatu perjanjian, dengan mana seorang penanggung mengikatkan diri kepada seorang tertanggung, dengan menerima suatu premi, untuk memberikan*

[11] Budi Susanto, *Modul No.12: Keamanan Jaringan*, hlm.1 (tanpa tahun).

penggantian kepadanya karena suatu kerugian kerusakan atau kehilangan keuntungan yang diharapkan, yang mungkin akan dideritanya karena suatu peristiwa yang tak tertentu.

Sedangkan Pasal 1 ayat (1) Undang-Undang Republik Indonesia No. 2 Tahun 1992 tentang Usaha Perasuransian menyebutkan bahwa:

"Asuransi atau pertanggungan adalah perjanjian antara dua pihak atau lebih dengan mana pihak penanggung mengikatkan diri kepada tertanggung, dengan menerima premi asuransi, untuk memberikan pergantian kepada tertanggung karena kerugian, kerusakan atau kehilangan keuntungan yang diharapkan, atau tanggung-jawab kepada pihak ketiga yang mungkin akan diderita tertanggung, yang timbul dari suatu peristiwa yang tidak pasti, atau untuk pembayaran yang didasarkan atas meninggal atau hidupnya seseorang yang dipertanggung jawabkan"

Dari definisi di atas tergambar adanya beberapa unsur dari asuransi, yaitu:

1. Merupakan suatu perjanjian;
2. Adanya premi;
3. Adanya kewajiban penanggung untuk memberikan penggantian kepada tertanggung; dan
4. Adanya suatu peristiwa yang belum tentu pasti terjadi.

Agar suatu perjanjian asuransi menjadi sah dan memiliki kekuatan mengikat, maka tertanggung harus mempunyai kepentingan terhadap objek yang diasuransikannya. Hal ini dengan tegas dinyatakan dalam Pasal 250 KUHD yang menyebutkan:

"apabila seseorang yang telah mengadakan suatu perjanjian asuransi untuk diri sendiri, atau apabila seseorang yang untuknya telah diadakan suatu asuransi, pada saat diadakannya asuransi itu tidak mempunyai suatu kepentingan terhadap barang yang diasuransikan, maka penanggung tidak diwajibkan memberikan ganti kerugian."

Kepentingan yang dapat diasuransikan tentunya berkaitan dengan objek asuransi itu sendiri. Objek asuransi dalam perjanjian asuransi tercantum dalam ketentuan Pasal 268 KUHD yaitu:

> "*suatu pertanggungan dapat mengenai segala kepentingan yang dapat dinilai dengan uang, dapat diancam oleh suatu bahaya, dan tidak dikecualikan oleh undang-undang*"

Sedangkan Pasal 1 ayat (2) Undang-Undang Nomor 2 Tahun 1992 Tentang Usaha Perasuransian, menyebutkan:

> "*Objek asuransi adalah benda atau jasa jiwa dan raga, kesehatan manusia, tanggung jawab hukum, serta kepentingan lainnya yang dapat hilang , rusak, rugi, dan atau berkurang nilainya.*"

Terkait dengan pembentukan perjanjian asuransi, Pasal 255 KUHD menyebutkan bahwa suatu asuransi harus dibuat secara tertulis dalam suatu akta yang dinamakan polis. Namun, polis bukanlah syarat mutlak untuk perjanjian asuransi, tetapi hanya sekedar berfungsi sebagai alat bukti.

Sesuai dengan ketentuan Pasal 256 KUHD bahwa setiap polis kecuali menyangkut suatu asuransi jiwa, harus menyatakan:

1. hari ditutupnya asuransi;
2. nama orang yang menutup asuransi atas tanggungan sendiri atau atas tanggungan orang ketiga;
3. suatu uraian yang cukup jelas mengenai barang yang dipertanggungkan;
4. jumlah uang untuk berapa diadakan asuransi;
5. bahaya-bahaya yang ditanggung oleh penanggung;
6. saat pada mana bahaya mulai berlaku untuk tanggungan penanggung dan saat berakhirnya itu;
7. premi asuransi tersebut; dan
8. pada umumnya, semua keadaan yang kiranya penting bagi penanggung untuk diketahuinya dan segala syarat yang diperjanjikan antara para pihak.

Apabila suatu peristiwa yang diperjanjikan *(evenement)* dalam asuransi telah terjadi, maka pihak tertanggung dapat mengajukan klaim dengan mengajukan berbagai alat bukti pendukung. Terkait alat bukti, Pasal 257 KUHD menyebutkan:

"perjanjian pertanggungan diterbitkan seketika setelah ia ditutup; hak-hak dan kewajiban-kewajiban bertimbal-balik dari penanggung dan tertanggung mulai semenjak saat itu, bahkan sebelum polisnya tandatangani", sedangkan Pasal 258 KUHD menyebutkan: *"Untuk membuktikan hal ditutupnya perjanjian tersebut, diperlukan pembuktian dengan tulisan; namun demikian bolehlah lain-lain alat pembuktian dipergunakan juga, mana kala sudah ada suatu permulaan pembuktian dengan tulisan."*

Dari 2 Pasal di atas, dapat disimpulkan bahwa pembuktian perjanjian asuransi dapat dilakukan dengan:

1. polis, bila dalam perjanjian asuransi tersebut di buat polis;
2. alat bukti lain, asal sudah ada permulaan pembuktian dengan tulisan, apabila polis belum dibuat;
3. sumpah pemutus, apabila polis dan permulaan pembuktian dengan tulisan tidak ada.

E. Pembahasan

1. Perjanjian Asuransi dalam Transaksi *E-commerce* Menurut Kitab Undang-Undang Hukum Dagang (KUHD)

Kegiatan *e-commerce* dengan menggunakan kunci-kunci kriptografi dan *secure electronic transaction* berpotensi menimbulkan kerugian bagi para pihak apabila sistem keamanan dapat ditembus secara illegal oleh pihak lain. Bagi pembeli atau pemilik kartu, mereka akan kehilangan uang mereka, sedangkan bagi penjual, *issuer*, *acquirer*, *gateway*, dan lembaga otoritas sertifikat, akan kehilangan kepercayaan dari konsumen sehingga konsumen akan meninggalkannya. Pada dasarnya, tanpa adanya upaya menembus kunci kriptografi milik konsumen secara aktif, yaitu pelaku mencoba berbagai kemungkinan hingga akhirnya ia menemukan kunci yang cocok, sertifikat digital sulit untuk ditembus.

Dalam upaya mengalihkan risiko yang akan terjadi akibat pengamanan ditembus secara illegal oleh pihak lain, maka pihak lembaga otoritas sertifikat membutuhkan sebuah perjanjian asuransi dengan perusahaan asuransi yang dapat melindungi kepentingan pihak-pihak yang telibat dalam transaksi *e-commerce*, khususnya yang menggunakan *secure electronic transaction*. Lembaga otoritas sertifikat dianggap sebagai pihak yang tepat untuk menutup asuransi, ini berkaitan dengan prinsip kepentingan yang dapat diasuransikan.

Di bawah ini akan dianalisis perjanjian asuransi antara lembaga otoritas sertifikat dengan perusahaan asuransi dihubungkan dengan ketentuan Kitab Undang-Undang Hukum Dagang, khususnya dengan mengacu pada Pasal 256 KUHD.

1. Hari ditutupnya asuransi
   Hari ditutupnya asuransi penting untuk menentukan saat terbentuknya perjanjian asuransi sehingga dapat diketahui saat mulai berjalan hak dan kewajiban para pihak.
2. Nama orang yang menutup asuransi atas tanggungan sendiri atau atas tanggungan orang ketiga.
   Dalam asuransi pihak-pihak yang dikenal adalah penanggung dan tertanggung Sebagaimana yang disebutkan dalam Pasal 246 KUHD bahwa tertanggung adalah pihak yang mengalami suatu kerugian kerusakan atau kehilangan keuntungan yang diharapkan akibat suatu peristiwa tak tertentu. Sementara yang dimaksud dengan pihak penanggung adalah pihak yang mengikatkan diri kepada tertanggung untuk memberikan penggantian atas kerugian yang diderita tertanggung dengan menerima bayaran atau premi dari tertanggung. Pihak-pihak yang terlibat dalam alur transaksi menggunakan *secure electronic transaction* antara lain pembeli, penjual, *issuer*, *acquirer*, *gateway*, dan lembaga otoritas sertifikat. Pihak yang menjadi penanggung adalah perusahaan asuransi, sementara untuk mengetahui siapa yang merupakan pihak tertanggung perlu dilihat siapa saja yang mempunyai risiko kerugian.
   Bila terjadi pencurian atau penggunaan kunci secara illegal, pihak penjual, acquirer dan *gateway* tidak akan mengalami dampak langsung kerugian seperti pihak pembeli, *issuer,* dan lembaga otoritas sertifikat. Walaupun begitu tidak berarti bahwa pembeli lebih besar kepentingannya dibandingkan penjual. Namun yang menjadi tertanggung tidak boleh lebih dari satu pihak (pembeli, *issuer,* dan otoritas sertifikat), karena akan terjadi tumpang tindih kepentingan dan melanggar prinsip *indemnity*. Maka penulis berpendapat bahwa pihak yang tepat sebagai tertanggung adalah lembaga otoritas sertifikat. Ini sesuai dengan syarat-syarat yang harus dimiliki setiap Lembaga Otoritas Sertifikat yang salah satunya adalah asuransi.[12]

---

[12] Danrivanto Budhijanto, *Cyber Law: Suatu Pengantar; Aspek Hukum "Digital Signature" dan "Certification Authorities" dalam Transaksi E-commerce*, Elips, Bandung, 2002, hlm. 71.

3. suatu uraian yang cukup jelas mengenai benda yang dipertanggungkan. Penanggung harus mempunyai pengetahuan tentang objek yang ditanggungnya guna memahami berapa besar risiko yang akan ditanggungnya. Tertanggung pun harus memberikan keterangan yang benar dan beritikad baik.
4. jumlah uang untuk berapa diadakan asuransi;
   Bahwa asuransi ini ditutup untuk harga yang penuh (*volle verzekering*) atau untuk di bawah harga sepenuhnya (*onder verzekering*). Dengan menyebutkan jumlah uang untuk berapa diadakan asuransi, besarnya ganti kerugian dapat diketahui ketika peristiwa yang diasuransikan terjadi.
5. bahaya-bahaya yang ditanggung oleh penanggung;
   Hal ini berkaitan dengan prinsip sebab akibat (kausalitas) dalam hukum asuransi. Apabila bahaya yang terjadi tidak disebutkan, maka penanggung tidak mempunyai kewajiban untuk mengganti kerugian.

Sekalipun *e-commerce* sarat dengan keterlibatan sistem pengamanan yang berbasis teknologi informasi, namun hal tersebut tidak berarti *e-commerce* bebas dari potensi terjadinya kerugian yang disebabkan adanya gangguan. Justru sebaliknya, teknologi ini sangat peka terhadap gangguan seperti:
Inosentius Samsul, Perlindungan Konsumen, Kemungkinan Penerapan Tanggungjawab Mutlak, Universitas Indonesia, Fakultas Hukum, Pascasarjana, 2004.

a. Gangguan tegangan listrik (Power surges/ Stoppages);
b. Hacking;
c. Virus dan sejenisnya; dan
d. Denial of Services Attacks ("DoS").

Salah satu cara yang dapat ditempuh untuk mengamankan data dan informasi dari berbagai gangguan tersebut adalah menggunakan teknologi kunci kriptografi *(cryptography).* Secure electronic transaction (SET) sebagai salah satu sistem keamanan dalam *e-commerce* yang menggunakan kunci-kunci kriptografi sangat dibutuhkan untuk memberikan jaminan perlindungan terhadap konsumen dalam bertransaksi. Namun demikian, SET bukanlah sebuah sistem yang sempurna, karena masih tetap potensial mengalami gangguan.

Terjadinya gangguan terhadap SET tentunya akan berpengaruh terhadap transaksi yang dilakukan oleh para pihak, sehingga akan merugikan para pihak, misalnya data yang dikirim tidak sampai kepada pihak yang dituju atau nilai transaksi tidak sesuai dengan nilai yang disepakati.

Dalam *secure electronic transaction*, bahaya yang akan terjadi terkait dengan penggunaan kunci kriptografi, berupa:

a. Gagal mencegah pencurian data.
b. Akses tanpa izin, yang bertujuan menggunakan atau merusak data atau sistem.
c. Gagal mencegah pihak lain selain tertanggung memasukkan *malicious code* ke dalam data atau sistem;
d. Ketidakmampuan pihak ketiga, yang berkepentingan, untuk melakukan akses kecuali ketidakmampuan itu disebabkan oleh kesalahan mekanis, telekomunikasi, atau gangguan listrik.

6. Saat bahaya mulai berlaku atas tanggungan penanggung dan saat berakhirnya bahaya dimaksud.
7. Premi asuransi.
   Jumlah premi asuransi tergantung pada objek yang diasuransikan, idealnya sebuah perjanjian asuransi dilaksanakan terhadap suatu objek yang memiliki kemungkinan risiko kerugian yang besar namun probabilitasnya rendah. Dalam kaitannya dengan kunci kriptografi dan *secure electronic transaction*, penggunaan kunci kriptografi dapat menimbulkan kerugian yang besar bagi tertanggung namun kemungkinan kunci kriptografi tersebut dicuri relatif kecil.
8. pada umumnya, semua keadaan yang kiranya penting bagi penanggung untuk diketahuinya dan segala syarat yang diperjanjikan antara para pihak. Penanggung berhak mengetahui segala sesuatu yang berkaitan dengan apa yang ditanggungnya. Untuk itu diperlukan kejujuran dan itikad baik dari pihak tertanggung untuk menginformasikan segala sesuatu terkait obyek pertanggungan dan tidak menyembunyikan suatu hal yang sepatutnya diberitahukan pada penanggung. Misalnya, apabila terjadi perubahan sistem pengamanan setelah perjanjian asuransi ditutup yang dapat mempengaruhi kualitas pengamanan, maka tertanggung harus segera memberitahukannya kepada pihak penanggung, baik diminta maupun tidak.

2. Pembuktian Adanya Perjanjian Asuransi dalam Asuransi *E-commerce*

Sebagaimana disebutkan di atas, pembuktian adanya perjanjian asuransi diatur dalam Pasal 255, 257, dan 258 KUHD. Pasal 255 KUHD menyebutkan bahwa asuransi harus dibuat secara tertulis dalam suatu akta yang dinamakan polis. Namun jika memperhatikan Pasal 257 dan 258 KUHD terkesan munculnya kontradiktif.

Berdasarkan Pasal 255, polis terkesan sebagai satu-satunya alat bukti dalam perjanjian asuransi padahal berdasarkan Pasal 257 dan Pasal 258 tidak menyatakan demikian. Pasal 257 KUHD menyebutkan:

> *"perjanjian pertanggungan diterbitkan seketika setelah ia ditutup; hak-hak dan kewajiban-kewajiban bertimbal-balik dari penanggung dan tertanggung mulai semenjak saat itu, bahkan sebelum polisnya tandatangani"*

Pasal 258 KUHD menegaskan pula bahwa:

> *"Untuk membuktikan hal ditutupnya perjanjian tersebut, diperlukan pembuktian dengan tulisan; namun demikian bolehlah lain-lain alat pembuktian dipergunakan juga, manakala sudah ada suatu permulaan pembuktian dengan tulisan."*

Dari 2 pasal di atas, dapat dikatakan bahwa polis bukanlah syarat mutlak untuk perjanjian asuransi, tetapi hanya berfungsi sebagai alat bukti untuk kepentingan penanggung. Namun, bukan berarti polis tidak perlu, menurut Emmy Pangaribuan Simanjuntak[13] polis merupakan bukti yang sempurna mengenai perjanjian yang bersangkutan dan ketiadaan polis kemungkinan dapat mempersulit pembuktian, karena di dalamnya memuat isi perjanjian berikut hak dan kewajiban para pihak.

Dari uraian di atas dapat disimpulkan bahwa pembuktian perjanjian asuransi dapat dilakukan dengan:

1. polis, ketika dalam perjanjian asuransi tersebut di buat polis;
2. alat bukti lain, asal sudah ada permulaan pembuktian dengan tulisan, bila polis belum dibuat;
3. sumpah pemutus, ketika polis dan permulaan pembuktian dengan tulisan tidak ada.

Ada kalanya peristiwa yang menimbulkan kerugian *(evenement)* dapat terjadi sebelum dikeluarkannya polis oleh perusahaan asuransi, namun peristiwanya terjadi setelah para pihak sepakat untuk membuat perjanjian asuransi. Bila polis belum dibuat maka untuk membuktikan adanya perjanjian asuransi, dapat dipergunakan alat bukti lain selain polis yang dapat dipergunakan sebagai permulaan pembuktian seperti: korespondensi antara para pihak,

---

[13] Emmy Pangaribuan Simanjuntak, *Hukum Pertanggungan*, Seksi Hukum Dagang Fakultas Hukum UGM, yogyakarta,1980 hlm. 20.

catatan agen asuransi, nota penutupan, dan sebagainya. Hal yang sama dapat digunakan untuk membuktikan telah terjadinya perjanjian asuransi *e-commerce*

Permasalahan lain terkait pembuktian adalah obyek (benda) asuransi yang mengalami kerugian. Pada beberapa kasus, pengadilan mengganggap data bukanlah benda yang berwujud, sehingga kriteria "*direct physical loss*" atau kerugian fisik yang harus ditunjukkan sebagai bukti kerugian sebagaimana yang tertera dalam polis konvensional tidak terpenuhi. Lebih lanjut kerusakan atau kerugian dari aset yang tidak wujud (dalam *e-commerce*) jarang disebabkan oleh sebab fisik seperti api atau banjir, melainkan oleh virus komputer dan *hacker*.

Masalah di atas tergambar dengan jelas dalam kasus yang terjadi antara America Online, inc. v. St. Paul Mercury Insurance Co. Penggugat, American Online, Inc. (AOL), melakukan klaim terhadap St. Paul Mercury Insurance Co (St. Paul) berdasarkan keluhan beberapa konsumen AOL akibat penggunaan program AOL's Internet access software versi 5 (AOL 5.0) yang menyebabkan "rusak"-nya komputer, data, piranti lunak, dan sistem.

St. Paul Mercury Insurance Co menolak klaim AOL dengan alasan bahwa peristiwa yang terjadi tidak memenuhi apa yang dimaksudkan dengan kerusakan fisik yang tertera dalam polis asuransi yaitu *commercial general liability policy* yang ditutup oleh AOL. Pengadilan sependapat dengan St. Paul bahwa kerusakan fisik tersebut tidak termasuk data komputer, dan piranti lunak tidak dapat menyebabkan kerusakan fisik, karena ia bukan termasuk benda yang wujud.

Dari kasus di atas, permasalahan yang timbul terkait objek asuransi. Jika permasalahan obyek/benda yang diasuransikan sebagaimana diuraikan di atas dilihat dari KUHD, maka pembahasan tidak dapat dilepaskan dari ketentuan tentang objek asuransi di Indonesia, sebagaimana diatur dalam Pasal 268 KUHD, yang menyatakan bahwa:

> "*Suatu pertanggungan dapat mengenai segala kepentingan yang dapat dinilai dengan uang, dapat diancam suatu bahaya, dan tidak dikecualikan oleh undang-undang*"

Pasal 1 ayat (2) Undang-Undang Nomor 2 Tahun 1992 Tentang Usaha Perasuransian, menyebutkan bahwa:

> *"objek dari asuransi adalah benda dan jasa, jiwa dan raga, kesehatan manusia, tanggung jawab hukum, serta semua kepentingan lainnya yang dapat hilang, rusak, rugi dan atau berkurang nilainya."*

Melihat kedua definisi tersebut, maka kerugian yang dialami perusahaan di atas sejatinya dapat dijadikan objek asuransi. Objek mengenai kepentingan tersebut dapat dinilai dengan uang dan diancam suatu bahaya. Pada kasus AOL, objek asuransi adalah tanggung jawab hukum pihak AOL sebagai penyedia jasa, mengingat KUHD tidak menjelaskan bahwa kerusakan yang terjadi merupakan kerusakan fisik atas benda yang dapat disentuh atau tidak.

Terkait dengan penggunaan kunci-kunci kriptografis dalam sistem pengamanan *e-commerce*, apakah layak untuk dijadikan sebagai objek asuransi atau tidak, kiranya dapat dilihat dari syarat-syarat sebagai berikut:[14]

1. Massal dan Homogen
   Massal dan homogen berarti kunci-kunci kriptografis yang akan diasuransikan haruslah banyak, perusahaan asuransi tentunya tidak mungkin hanya menanggung satu tertanggung. Dalam transaksi SET pihak yang berkepentingan dan dapat mengasuransikan kepentingannya itu lebih dari satu.
2. Kerugian tertentu
   Kerugian yang akan terjadi terhadap kunci-kunci kriptografis adalah dicurinya kunci tersebut yang akan merugikan beberapa pihak. Perusahaan asuransi akan berjanji membayar kerugian tertentu, yang disebabkan hal yang tertentu pada waktu tertentu. Dapat menjadi patokan jangka waktu asuransi ini adalah jangka waktu daluwarsa dari sertifikat yang dikeluarkan otoritas sertifikat.
3. Kerugian yang terjadi bersifat kebetulan
   Kerugian yang terjadi tidaklah boleh akibat kesengajaan dari pihak yang berkepentingan. Tertanggung dalam hal pemakaian kunci kriptografis tidak boleh memiliki kontrol atau pengaruh terhadap kejadian yang ingin diasuransikannya.
4. Kelayakan ekonomis
   Idealnya suatu objek diasuransikan adalah adanya kemungkinan kerugian yang besar namun kemungkinan terjadinya kecil. Nilai kerugian yang akan dialami lembaga otoritas sertifikat akibat pencurian kunci kriptografi ataupun gagal dalam menyelenggarakan jasanya sangat besar, namun kemungkinan untuk dicuri juga kecil tergantung panjang kunci yang diterbitkan.
5. Probabilitas dapat diperhitungkan
   Probabilitas dalam *e-commerce* dapat diperhitungkan melalui panjang pendeknya kunci yang digunakan tentunya juga dengan mempertimbangkan serta mengkaji perkembangan teknologi.

---

[14] Arrianto Mukti Wibowo, *op.cit.*, hlm. 36.

Memperhatikan uraian di atas, maka kunci kriptografi dapat dijadikan sebagai objek asuransi.

F. Kesimpulan

1. Perjanjian asuransi antara lembaga otoritas sertifikat dengan perusahaan asuransi merupakan jenis asuransi kerugian, sehingga terhadap perjanjian tersebut harus memenuhi prinsip-prinsip asuransi kerugian sebagaimana diatur dalam Kitab Undang-Undang Hukum Dagang.
2. Perjanjian asuransi antara lembaga otoritas sertifikat dengan perusahaan asuransi termasuk golongan asuransi kerugian maka pembuktiannya harus mengacu kepada ketentuan Pasal 257 dan 258 Kitab Undang-Undang Hukum Dagang. Dalam pembuktian adanya perjanjian asuransi *e-commerce* polis bukan merupakan syarat esensial dalam perjanjian asuransi, tapi hanya berfungsi sebagai salah satu alat bukti.

G. Saran

1. Mengingat dalam beberapa hal, ketentuan dalam KUHD sukar untuk diterapkan dalam perjanjian asuransi *e-commerce*, maka disarankan agar dilakukan beberapa perubahan (revisi) terhadap KUHD, khususnya mengenai pengaturan obyek atau benda yang dapat diasuransikan, dan pembuktian.
2. Mengingat asuransi *e-commerce* sangat penting guna memberikan perlindungan bagi para pihak yang terlibat di dalamnya, utamanya pihak konsumen, maka disarankan asuransi ini mulai diwajibkan penerapannya, sehingga masyarakat dapat terlindungi dalam bertransaksi.

DAFTAR PUSTAKA

A. Buku

Budi Raharjo, *Keamanan Sistem Informasi Berbasis Internet*, PT. Insan Komunika, Bandung, 2000.

Budi Susanto, *Keamanan Jaringan*, Modul no.12, (tanpa tahun).

Bickelhaup, David L, *General Insurance*, Richard D. Irwin, Inc. Homewood, Illinois, 1974.

Danrivanto Budhijanto, *Cyber Law: Suatu Pengantar; Aspek Hukum "Digital Signature" dan "Certification Authorities" dalam Transaksi E-commerce*, Elips Bandung, 2002.

Emmy Pangaribuan Simanjuntak, *Hukum Pertanggungan*, Seksi Hukum Dagang Fakultas Hukum Universitas Gajah Mada, Yogyakarta, 1980.

Gunanto, *Hukum Asuransi Kebakaran di Indonesia* , PT. Tira Pustaka, Jakarta, 1984.

Man Suparman Sastrawidjaja, *Aspek-Aspek Hukum Asuransi dan Surat Berharga*, PT. Alumni, Bandung, 1997.

_____, *Cyberlaw: Suatu Pengantar- Perjanjian. Baku Dalam Aktivitas Dunia Maya*, ELIPS II, Bandung, 2002.

Mehr, Robert I and Emerson Cammack, *Principles of Insurance*, Richard D. Irwin, Inc. Homewood, Illinois,1972.

Sri Rejeki Hartono, *Hukum Asuransi dan perusahaan Asuransi*, PT. Sinar Grafika, Jakarta, 1997.

B. Artikel/ Jurnal/ Makalah

Arianto Mukti Wibowo, *makalah: Kerangka Hukum Digital Signature Dalam Electronic Commerce*, dipresentasikan di hadapan Masyarakat Telekomunikasi Indonesia, pada bulan Juni 1999 di Pusat Ilmu Komputer Universitas Indonesia , Depok, Jawa Barat.

Heru Soepraptomo, *Makalah: Kejahatan Komputer dan Siber Serta Antisipasi Pengaturan Pencegahannya di Indonesia*, diberikan pada perkuliahan Hukum dan Komputer, 2004.

Sutan Remy Sjahdeini, *Hukum Siber Sistem Pengamanan E-commerce*, makalah dalam seminar tentang Peran Penegak Hukum Dalam Kaitannya Dengan Transaksi Perbankan" yang diselenggarakan oleh Bank Mandiri pada hari Kamis, 18 Januari 2001 di Mandiri Club Jakarta.

_____, *E-commerce Tinjauan Dari Perspektif Hukum*, makalah ini merupakan perbaikan dari makalah yang di sajikan pada seminar tentang "*E-commerce* dan Mekanisme Penyelesaian Masalahnya melalui Arbitrase/Alternatif Penyelesaian Sengketa" diselenggarakan di Hotel Mulia Senayan, Jakarta, tanggal 3 Oktober 2000.

C. Perundang-undangan

Kitab Undang-Undang Hukum Dagang.

Kitab Undang-Undang Hukum Perdata.

Undang-Undang Nomor 2 Tahun 1992 tentang Usaha Perasuransian.