

# PERLINDUNGAN HUKUM TERHADAP NASABAH BANK KORBAN *CYBER CRIME* DALAM INTERNET *BANKING* BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Meslik Anin

Program Studi Magister Ilmu Hukum  
Universitas Langlangbuana

---

## ABSTRAK

Internet selain memberi manfaat juga menimbulkan eksekusi negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik. Dalam jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkungannya yang luas. Kriminalitas di internet atau *cyber crime* pada dasarnya merupakan suatu tindak pidana yang berkaitan dengan *cyber space*, baik yang menyerang fasilitas umum di dalam *cyber space* ataupun kepemilikan pribadi. Secara garis besar kejahatan-kejahatan yang terjadi terhadap suatu sistem atau jaringan komputer dan yang menggunakan komputer sebagai instrumen *delicti*, juga dapat terjadi di dunia perbankan. Sehubungan dengan hal tersebut di atas ada beberapa permasalahan yang menarik untuk dikaji antara lain bagaimanakah perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet *banking* serta bagaimanakah pembuktian dalam *cyber crime* di bidang perbankan dihubungkan dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ?

Pendekatan pembahasan tesis ini penulis menggunakan metode penelitian yuridis normatif yang bertujuan untuk mencari asas-asas dan dasar-dasar falsafah hukum positif, serta menemukan hukum secara *in-concreto*. Spesifikasi penelitian ini deskriptif analitis, yaitu tidak hanya menggambarkan permasalahan saja, melainkan juga menganalisis melalui peraturan yang berlaku dalam hukum pidana. Teknik pengumpulan data dilakukan melalui studi kepustakaan serta penelitian lapangan untuk mengumpulkan data primer dan sekunder.

Hasil penelitian menyimpulkan Perlindungan hukum bagi nasabah pengguna layanan internet *banking* mutlak diperlukan seperti halnya perlindungan yang diberikan kepada nasabah penyimpan dana lainnya. Perlindungan hukum bagi nasabah ada yang berdasarkan ketentuan administratif dan berdasarkan jaminan asuransi deposito. Jaminan perlindungan bagi nasabah sangat diperlukan untuk memberikan kepastian hukum bagi nasabah dikemudian hari bilamana bank mengalami kegagalan dalam sistem keamanan. Kemudian Informasi elektronik dan

Dokumen Elektronik dapat dijadikan sebagai alat bukti yang sah menurut undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah sebagaimana dimaksud Pasal 184 ayat (1) KUHAP. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik<sup>12</sup> sesuai ketentuan yang diatur dalam UU ITE.

## PENDAHULUAN

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi

informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input, process, output, storage*, dan *communication*. Sehubungan dengan itu, dalam ilmu hukum sebenarnya sudah sejak lama

memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana.

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan e-commerce antara lain dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang dibuat di atas kertas.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disingkat dengan UU ITE) merupakan wujud dari tanggung jawab yang harus diemban oleh negara yang memberikan perlindungan maksimal pada seluruh aktivitas pemanfaatan

teknologi informasi dan komunikasi dalam kehidupan berbangsa dan bernegara. Kepastian hukum yang kuat akan membuat seluruh aktivitas pemanfaatan teknologi informasi dan komunikasi di dalam negeri terlindungi dengan baik dari potensi kejahatan dan penyalahgunaan teknologi.

Hukum baru dalam khazanah peraturan perundang-undangan Republik Indonesia, yaitu UU ITE yang terdiri dari 13 Bab dan 54 Pasal menganut asas yurisdiksi ekstra teritorial, asas kebebasan memilih teknologi atau netral teknologi, dengan cakupan materi antara lain pengakuan informasi dan/atau dokumen elektronik sebagai alat bukti hukum yang sah, pengakuan atas tanda tangan elektronik, penyelenggaraan sertifikasi elektronik dan sistem elektronik, nama domain, hak kekayaan intelektual dan perlindungan hak pribadi, perbuatan yang dilarang serta ketentuan pidananya.

Teknologi dalam dunia perbankan pada saat ini telah berkembang pesat sejalan dengan perkembangan teknologi informasi dan telekomunikasi. Perkembangan teknologi informasi telah membawa banyak perubahan dalam peradaban manusia, salah satu bentuk teknologi informasi yang dapat berguna bagi kemajuan industri perbankan adalah internet. Internet merupakan

jaringan komputer global di dunia yang saat ini digunakan oleh jutaan orang di seluruh penjuru dunia. Melalui internet seseorang dapat memperoleh berbagai macam informasi yang dibutuhkan dan bahkan dapat melakukan perdagangan dengan pihak yang berada di belahan dunia lain dengan aman, cepat, dan murah.<sup>1)</sup> *Electronic Fund Transfer* (EFT) merupakan salah satu contoh inovasi dari penggunaan teknologi internet yang mendasar dalam Teknologi Sistem Informasi (TSI) di bidang perbankan.

Contoh dari produk-produk EFT antara lain meliputi Anjungan Tunai Mandiri (ATM), *electronic home banking* (biasa disebut sebagai internet *banking*), dan *money transfer network*.<sup>2)</sup> Kejahatan internet *banking* juga merupakan salah satu bentuk kejahatan di dalam dunia maya atau disebut sebagai *cyber crime* di bidang perbankan.

Internet *banking* merupakan salah satu pelayanan perbankan tanpa cabang, yaitu berupa fasilitas yang akan memudahkan nasabah untuk melakukan transaksi perbankan tanpa perlu datang ke kantor cabang. Layanan yang diberikan internet *banking* kepada

nasabah berupa transaksi pembayaran tagihan, informasi rekening, pemindahbukuan antar rekening, informasi terbaru mengenai suku bunga dan nilai tukar valuta asing, administrasi mengenai perubahan *Personal Identification Number* (PIN), alamat rekening atau kartu, data pribadi dan lain-lain, terkecuali pengambilan uang atau penyetoran uang. Karena untuk pengambilan uang masih memerlukan layanan ATM dan penyetoran uang masih memerlukan bantuan bank cabang.<sup>3)</sup>

Di samping itu, penggunaan Teknologi Sistem Informasi (TSI) terdapat resiko yang bersifat teknis dan khusus, yang berbeda dengan penggunaan sistem manual. Resiko yang dimaksud antara lain resiko kekeliruan pada tahap pengoperasian, resiko akses oleh pihak yang tidak berwenang, resiko kehilangan atau kerusakan data.<sup>5)</sup>

Dalam praktek internet *banking* terdapat berbagai macam serangan atau ancaman bagi pihak pengguna dan penyedia layanan internet *banking*. Contohnya serangan seperti *man in the middle attack* dan *trojan horses* dapat mengganggu keamanan layanan.

---

<sup>1)</sup> Barno Sudarwanto, *Implikasi Penggunaan Teknologi Dalam Dunia Perbankan*, Majalah Bank & Manajemen, edisi November-Desember 1998, hlm.69.

<sup>2)</sup> <http://www.fdic.gov.html/>, diakses pada tanggal 10 Maret 2015

---

<sup>3)</sup> Onno W. Purbo dan Aang Arif Wahyudi, *Mengenal E-Commerce*, Elex Media Komputindo, Jakarta, 2001, hlm.85.

<sup>5)</sup> <http://www.theage.com.au/>, diakses pada tanggal 15 Maret 2015

Gambaran umum dari aktifitas yang sering disebut *man in the middle attack* yaitu penyerang membuat sebuah *website* dan membuat nasabah pengguna layanan internet *banking* atau *user* masuk ke *website* tersebut. Agar berhasil mengelabui *user*, *website* tersebut harus dibuat semirip mungkin dengan *website* bank yang sebenarnya. Kemudian *user* memasukkan *password*-nya, dan penyerang kemudian menggunakan informasi ini untuk mengakses *website* bank yang sebenarnya. Untuk mengecoh token, penyerang dapat mengirimkan *challenge-response* kepada *user* sebelum melakukan transaksi ilegal. Sedangkan, *trojan horses* adalah program palsu dengan tujuan jahat, yang disusupkan kepada sebuah program yang umum dipakai. Di sini para penyerang meng-*install trojan* kepada komputer *user*. Ketika *user* mulai *login* ke *website* banknya, penyerang menumpang sesi tersebut melalui *trojan* untuk melakukan transaksi yang diinginkannya.<sup>6)</sup>

Informasi merupakan hal yang sangat berharga bagi bank, mengingat bahwa bank merupakan lembaga kepercayaan. Oleh karena itu, pengamanan terhadap informasi tersebut baik dari penyalahgunaan yang disengaja ataupun pengungkapan informasi yang

---

<sup>6)</sup> <http://www.ristek.go.id/kebijakan-dalam/internet-banking.htm>, diakses pada tanggal 23 Maret 2015

tidak bertanggung jawab serta bentuk-bentuk kecurangan lainnya sangat diperlukan. Dalam rangka perkembangan internet *banking*, pihak Bank Indonesia mengeluarkan regulasinya pada tahun 1995. Regulasi itu dituangkan dalam Surat Keputusan Direksi Bank Indonesia No. 27/164/KEP/DIR dan Surat Edaran Bank Indonesia No. 27/9/UPPB Tentang Penggunaan Teknologi Sistem Informasi Perbankan keduanya tanggal 31 Maret 1995. Bersamaan dengan itu, Bank Indonesia juga mengeluarkan buku panduan Pengamanan Penggunaan Teknologi Sistem Informasi Oleh Bank sebagai lampiran dari SKDBI dan SEBI tersebut, juga dikeluarkannya PBI No. 9/15/PBI/2007 tentang Penerapan Manajemen risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum, Pedoman Penyelesaian Pengaduan Nasabah.

Kasus lainnya yaitu penipuan menggunakan rekening fiktif dan meminta sejumlah uang untuk ditransfer melalui pesan singkat atau SMS. Kejahatan perbankan berikutnya yakni pembobolan PIN nasabah melalui *skimming EDC (Electronic Data Capture)*. Saat ini nasabah cenderung lebih gemar melakukan pembayaran via *skimming EDC* daripada di ATM. kasus berikutnya yang sering terjadi yakni penipuan melalui *e-banking* dengan modus nasabah dinyatakan menang undian dan kemudian nasabah tanpa

sadar diminta registrasi mobile banking melalui mesin ATM.

Saat ini penanganan *cyber crime* di Indonesia masih minim, padahal Indonesia termasuk negara dengan kasus *cyber crime* tertinggi di bawah Ukraina. Penanganan kasus kejahatan jenis ini memang membutuhkan kemampuan khusus dari para penegak hukum. Dari kasus-kasus yang terungkap selama ini, pelaku diketahui memiliki tingkat kepandaian di atas rata-rata. Selain karena motif ekonomi, sebagian *hacker* melakukan tindakan merusak website orang lain hanya sekedar untuk pamer kemampuan.

*Cyber crime* menimpa beberapa bank. Bank-bank besar yang memiliki teknologi informasi canggih, berikut adalah sembilan kasus perbankan pada kuartal pertama yang dihimpun oleh Strategic Indonesia melalui Badan Reserse Kriminal Mabes Polri.

#### **A. Perlindungan hukum terhadap nasabah bank yang mengalami cyber crime dalam internet banking**

Upaya perlindungan hukum terhadap pemberi jasa atau pengguna internet telah melahirkan suatu produk hukum dalam bentuk UU ITE, namun dengan lahirnya UU ITE belum semua permasalahan menyangkut masalah ITE dapat tertangani. Dengan lahirnya UU ITE tidak semata-mata undang-undang

ini bisa diketahui oleh masyarakat pengguna teknologi informasi dan praktisi hukum. Kemudian berbagai bentuk perkembangan teknologi yang menimbulkan penyelenggaraan dan jasa baru harus dapat diidentifikasi dalam rangka antisipasi terhadap pemecahan berbagai persoalan teknis yang dianggap baru sehingga dapat dijadikan bahan untuk penyusunan berbagai Peraturan Pelaksanaan. Pengayaan akan bidang-bidang hukum yang sifatnya sektoral (rejim hukum baru) akan makin menambah semarak dinamika hukum yang akan menjadi bagian sistem hukum nasional.

Jaminan perlindungan bagi nasabah sangat diperlukan untuk memberikan kepastian hukum bagi nasabah dikemudian hari bilamana bank mengalami kegagalan dalam sistem keamanan sehingga menyebabkan uang nasabah yang disimpan dalam bank tersebut dicuri oleh para pelaku *cyber crime*.

Satu langkah yang dianggap penting untuk menanggulangi keamanan sistem informasi adalah telah diwujudkannya rambu-rambu hukum yang tertuang dalam UU ITE. Hal yang mendasar dari UU ITE ini sesungguhnya merupakan upaya mengakselerasikan manfaat dan fungsi hukum (peraturan) dalam kerangka kepastian hukum. Penegakan hukum pidana dalam *cyber crime* dapat

dilakukan oleh penyidik yang terdiri dari Kepolisian Republik Indonesia dan Penyidik Pegawai Negeri Sipil. Penyidikan dilakukan berdasarkan KUHP dan UU ITE. Kewenangan Penyidik Pegawai Negeri Sipil dalam rangka memberikan perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet *banking* tercantum dalam Pasal 43 UU ITE.

Perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet *banking* dihubungkan dengan UU ITE terdapat dalam Pasal 45, Pasal 46, Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51 UU ITE. Namun menurut hemat penulis, ketentuan-ketentuan yang terdapat di dalam UU ITE masih memerlukan penjabaran yang relevan, misalnya ketentuan yang diatur dalam Bab VII Pasal 27 sampai dengan Pasal 37 UU ITE mengenai perbuatan yang dilarang, semua pasal tersebut menggunakan kalimat setiap orang. Padahal perbuatan yang dilarang, seperti *spam*, penipuan, *cracking*, virus, dan *flooding* sebagian besar akan dilakukan oleh mesin oleh program bukan langsung oleh manusia.

Menurut sistem perbankan Indonesia, perlindungan terhadap nasabah dapat dilakukan melalui dua metode, yaitu perlindungan secara eksplisit (*explicit deposit protection*) yaitu perlindungan

yang diperoleh melalui pembentukan lembaga yang menjamin simpanan masyarakat, sebagaimana diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum. Sehingga apabila bank mengalami kegagalan, maka lembaga tersebut akan mengganti dan masyarakat yang disimpan dalam bank yang gagal tersebut. Hal ini diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum, sebelum diberlakukannya asuransi deposito.

Perlindungan secara implisit (*implicit deposit protection*) yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank secara efektif. Maksudnya agar dapat menghindari terjadinya kebangkrutan bank yang diawasi. Perlindungan semacam ini dapat diperoleh melalui peraturan perundang-undangan di bidang ITE dan perbankan. Perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif, yang dilakukan oleh Bank Indonesia.

Pemerintah melalui Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Pembayaran Bank Umum, menjamin bahwa kewajiban pembayaran bank umum kepada para pemilik simpanan dan krediturnya akan

dipenuhi. Dengan ketentuan Bank Umum yang dijamin adalah bank umum yang didirikan berdasarkan hukum Indonesia; kewajiban pembayaran yang dijamin pemerintah meliputi kewajiban dalam mata uang rupiah maupun mata uang asing, jaminan atas kewajiban dalam mata uang asing diberikan dengan mata uang rupiah berdasarkan nilai tukar pasar pada hari pembayaran.

Pelaksanaan penjaminan tersebut dilakukan oleh BPPN yang dibentuk berdasarkan Keputusan Presiden No. 27 Tahun 1998 dan Keputusan Presiden No. 34 Tahun 1998. Sedangkan teknis pelaksanaan serta ketentuan lebih lanjut dari penjaminan tersebut diatur dalam Keputusan Menteri Keuangan No. 26/KMK.017/1998 tentang Syarat dan Tata Cara Pelaksanaan Jaminan Pemerintah Terhadap Kewajiban Pembayaran Bank Umum, serta Surat Keputusan Bersama Direksi Bank Indonesia dan Ketua Badan Penyehatan Perbankan Nasional No. 30/270/KEP/DIR dan No. 1/BPPN/1998 tentang Petunjuk Pelaksanaan Pemberian Jaminan Pemerintah Terhadap Kewajiban Pembayaran Bank Umum. Lembaga Penjamin Simpanan (LPS) diatur dalam Pasal 37 B Undang-undang No.7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang No. 10 Tahun 1998.

Tujuannya adalah melindungi kepentingan nasabah dan sekaligus meningkatkan kepercayaan masyarakat kepada bank. Lembaga ini dibentuk untuk menggantikan fungsi BPPN setelah masa penjaminan pemerintah sebagaimana yang ditentukan dalam Keputusan Presiden No. 26 Tahun 1998 berakhir. Dalam tenggang waktu antara berakhirnya penjaminan pemerintah dan berlakunya LPS akan diadakan suatu masa transisi, sehingga nasabah dapat menyesuaikan diri. Adapun LPS tersebut, menurut penjelasan Pasal 37 B ayat 2 Undang-undang No.7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-undang No.10 Tahun 1998 dapat berbentuk Skim dana bersama, Skim asuransi, di antaranya yang sudah melakukan ketentuan mengenai skim asuransi ini, dapat dilakukan pembagian yaitu yang melakukan secara resmi oleh pemerintah.

Undang No.10 Tahun 1998, mengatur perlindungan nasabah secara implisit dan eksplisit. Implisit berarti adanya perlindungan yang dihasilkan melalui pembinaan dan pengawasan. Ini dilakukan oleh Bank Indonesia seperti yang tertera dalam Pasal 29 ayat (1) Undang-Undang Perbankan. Sedangkan eksplisit adalah perlindungan yang didapat melalui pembentukan lembaga yang menjamin simpanan dana nasabah seperti yang

diatur dalam Pasal 37 B Undang-Undang Perbankan.

Salah satu upaya untuk tetap mempertahankan kepercayaan masyarakat terhadap lembaga perbankan, yaitu melalui asuransi deposito yang dalam pengertian Undang-undang No. 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang No.10 Tahun 1998. Berarti Pasal 37 B Undang-undang

## KESIMPULAN DAN SARAN

### A. Kesimpulan

1. Perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet *banking* dihubungkan dengan UU ITE terdapat dalam Pasal 45, Pasal 46, Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51 UU ITE. Perlindungan hukum bagi nasabah pengguna layanan internet *banking* mutlak diperlukan seperti halnya perlindungan yang diberikan kepada nasabah penyimpan dana lainnya. Perlindungan hukum bagi nasabah ada yang berdasarkan ketentuan administratif dan berdasarkan jaminan asuransi deposito. Jaminan perlindungan bagi nasabah sangat diperlukan untuk memberikan kepastian hukum bagi nasabah dikemudian hari bilamana bank

mengalami kegagalan dalam sistem keamanan sehingga menyebabkan uang nasabah yang disimpan dalam bank tersebut dicuri oleh para pelaku *cyber crime*.

2. Informasi Elektronik dan Dokumen Elektronik dapat dijadikan sebagai alat bukti yang sah menurut undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah sebagaimana dimaksud Pasal 184 ayat (1) KUHP. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik<sup>12</sup> sesuai ketentuan yang diatur dalam UU ITE.

### B. Saran

1. Menurut sistem perbankan Indonesia, perlindungan terhadap nasabah dapat dilakukan melalui dua metode, yang pertama merupakan perlindungan secara eksplisit yang diperoleh melalui pembentukan lembaga yang menjamin simpanan masyarakat, yang kedua perlindungan secara implisit yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank secara efektif, maksudnya agar dapat menghindari terjadinya kebangkrutan bank yang diawasi.

2. Aplikasi yang sangat banyak dipakai dari kegiatan *cyber* adalah transaksi-transaksi elektronik, sehingga transaksi secara *online* saat ini menjadi isu yang paling aktual. Sebenarnya hal ini menjadi persoalan hukum semenjak transaksi elektronik mulai diperkenalkan, di samping persoalan pengamanan dalam sistem informasi itu sendiri. Tanpa pengamanan yang ketat dan canggih, perkembangan teknologi informasi tidak memberikan manfaat yang maksimal kepada masyarakat. Teknologi digital memungkinkan penyalahgunaan informasi secara mudah, sehingga masalah keamanan sistem informasi menjadi sangat penting. Satu langkah yang dianggap penting untuk menanggulangi keamanan sistem informasi adalah telah diwujudkannya rambu-rambu hukum yang tertuang dalam UU ITE. Hal yang mendasar dari UU ITE ini sesungguhnya merupakan upaya mengakselerasikan manfaat dan fungsi hukum (peraturan) dalam kerangka kepastian hukum. Penegakan hukum pidana dalam *cyber crime* dapat dilakukan oleh penyidik yang terdiri dari Kepolisian Republik Indonesia dan Penyidik Pegawai Negeri Sipil. Penyidikan dilakukan berdasarkan KUHP dan UU ITE.

## DAFTAR PUSTAKA

### A. Buku-buku

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Jakarta, 2005

Ahmad Sanusi, *Prospek Internet Banking di Era Millenium III*, Majalah Bank dan Manajemen, edisi Maret-April, Jakarta, 2000

Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Arikha Media Cipta, Jakarta, 2009

Atmasasmita, Romli, *Pengantar Hukum Kejahatan Bisnis*, Bogor: Kencana, 2003.

Agus Rahardjo, Budi, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: PT. Citra Aditya Bakti, 2002.

Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Perdana Media Group, Jakarta, 2007

Barno Sudarwanto, *Implikasi Penggunaan Teknologi Dalam Dunia Perbankan*, Majalah Bank &

Manajemen, edisi November-Desember 1998,

Budi Agus Rahardjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002

David Whiteley, *E-commerce: Strategy, Technology and Application*, Mc.Graw-Hill, London, 2000

Departemen Komunikasi dan Informatika Republik Indonesia, *Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Menuju Masyarakat Informasi Indonesia*, Jakarta: Depkominfo RI, 2008.

Djumhana, M., *Hukum Perbankan di Indonesia*, Cet. 3, Bandung: Citra Aditya Bakti, 2001.

Ermansjah Djaja, *Penyelesaian Sengketa Hukum Teknologi Informasi Dan Transaksi Elektronika*, Pustaka Timur, Yogyakarta, 2010

Fuady, Munir, *Hukum Perbankan Modern*, Cet.1, Bandung: Citra Aditya Bakti, 2001.

Lamintang, P.A.F., *Dasar-Dasar Hukum Pidana Indonesia*, Bandung: PT. Citra Aditya Bakti, 1997.

Makarim, Edmon, *Kompilasi Hukum Telematika*, Jakarta: Rajawali Press, 2003.

Marpaung, Leden, *Pemberantasan dan Pencegahan Tindak Pidana terhadap Perbankan*, Jakarta: Djembatan, 2005.

Nawawi Arif, Barda, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*, Jakarta: PT Rajagrafindo Persada, 2007.

Onno W. Purbo dan Aang Arif Wahyudi, *Mengenal E-Commerce*, Elex Media Komputindo, Jakarta, 2001

Philipus M. Hardjon dalam Budi Agus Riswandi, *Aspek Hukum Internet Banking*, PT. Raja grafindo Persada, Jogjakarta, 2005

Purbo, Onno W., dan Aang Arif Wahyudi, *Mengenal E-Commerce*, Jakarta: Elex Media Komputindo, 2001.

Rahardjo, Satjipto, *Biarkan Hukum Mengalir, Catatan Kritis Tentang Pergulatan Manusia dan Hukum*, Jakarta: Kompas, 2007.

Ramli, Ahmad, *Penulisan Karya Ilmiah Tentang Perlindungan HaKI dan Cyber Law*, Jakarta: BPHN, Departemen

Hukum dan Hak Asasi Manusia Republik Indonesia, 2005.

Riswandi, Budi Agus. *Aspek Hukum Internet Banking*. Jogjakarta: PT.Rajagrafindo Persada, 2005.

S., Yulius, dkk, *Kamus Baru Bahasa Indonesia*, Surabaya: Usaha Nasional, 1984.

Saifullah, *Refleksi Sosiologi Hukum*, Bandung: PT. Refika Aditama, 2007.

Salman, Otje, dan Anthon F. Susanto, *Teori Hukum*, Bandung: PT. Refika Aditama, 2007.

Sumadi Suryabrata, *Metodologi Penelitian*, Yogyakarta, 1993

Sjahdeni, Sutan Remy, *Kebebasan Berkontrak dan Perlindungan Yang Sumbang Bagi Para Pihak Dalam Perjanjian Kredit Bank Indonesia*, Jakarta: Institut Bank Indonesia, 1993.

Usman, Rachmad, *Aspek-aspek Hukum Perbankan di Indonesia*, Cet. 1, Jakarta: Gramedia Pustaka Utama, 2001.

Whiteley, David, *E-commerce: Strategy, Technology and Application*, London: Mc.Graw-Hill, 2000.

Widjanarto, *Hukum dan Ketentuan Perbankan di Indonesia*, Jakarta: Pustaka Utama Grafiti, 2003.

## **B. Peraturan Perundang-undangan**

Undang-Undang Nomor 8 Tahun 1981 Tentang Kitab Undang-Undang Hukum Acara Pidana

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-undang No. 10 Tahun 1998 mengenai Perubahan Undang-undang Nomor 7 Tahun 1992 tentang Perbankan

Surat Edaran Bank Indonesia No. 27/9/UPPB Tahun 1995 tentang *Penggunaan Teknologi Sistem Informasi oleh Bank*.

## **C. Internet**

<http://www.fdic.gov.html/>, diakses pada tanggal 10 Maret 2015

<http://www.theage.com.au/>, diakses pada tanggal 15 Maret 2015

<http://www.ristek.go.id/kebijakan-dalam/internet-banking.htm>, diakses pada tanggal 23 Maret 2015

<http://www.cbcindonesia.com/>, diakses pada tanggal 15 Maret 2015

<http://www.Tempo.co.>, diakses pada Senin 19 Januari 2015

<http://www.BeritaUtama.hukum.dan.kriminal.com/>, diakses pada tanggal 15 Maret 2015