Mimbar Keadilan, Jurnal Ilmu Hukum
Juli – November 2015, Hal. 135 – 149

KENDALA PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU PENCURIAN UANG DI BANK MELALUI INTERNET BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Agus Setiawahyudi[1]

Abstrak

Perkembangan pesat di bidang teknologi komputer yang dilengkapi fasilitas internet telah menyebabkan, mempengaruhi, dan membentuk tingkah laku masyarakat yang tidak bisa dikontrol dalam batas-batas wilayah dan waktu, sehingga dengan perkembangan itu juga menimbulkan kejahatan baru *cybercrime*. Salah satu bentuk kejahatan baru yaitu pencurian uang di bank melaui internet. Dalam penegakan hukum pada kejahatan bentuk baru yang sudah ada peraturan perundang-undangannya di Indonesia, tentu ada kesulitan dari penegak hukum dalam penerapannya. Penelitian ini ingin mengetahui kendala yuridis yang dihadapi penegak hukum dalam menanggulangi *cybercrime,* mengingat peraturan perundang-undangan yang berlaku seperti Undang-undang Informasi dan Transaksi Elektronik belum diketahui efektifitasnya dalam mengatur tindak pidana pencurian di bank melalui internet. Peneliti menggunakan pendekatan yuridis normatif yaitu pendekatan terhadap hubungan antara faktor-faktor yuridis (hukum positif) dengan faktor-faktor normatif (asas-asas hukum), dengan cara inventarisasi terhadap peraturan perundang-undangan yang berkaitan dengan *cybercrime* dan hal-hal lain yang menjadi kendala dalam menanggulangi tindak pidana *cybercrime*. Berdasarkan hasil analisis ditemukan 2 (dua) kendala pokok dalam pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melalui internet yaitu penerapan pasal-pasalnya, dan kendala yang kedua terletak di keterbatasan sumber daya manusia (SDM) dalam pembuktian.
Kata kunci: tindak pidana, pencucian uang, *cybercrime*, penegak hukum.

PENDAHULUAN

Globalisasi dan modernisasi yang telah memasuki bangsa ini membuat internet atau teknologi informasi hampir digunakan dalam setiap aspek kehidupan sehari-hari, khususnya dalam bidang perbankan. Sejumlah bank di Indonesia saat ini memanfaatkan teknologi informasi untuk meningkatkan layanan kepada para nasabahnya, sehingga dari kemajuan teknologi informasi itu muncullah banyak fasilitas layanan terhadap nasabahnya, misalnya ATM (*Automated Teller Machine)* atau mesin ATM (Anjungan Tunai Mandiri), mobile banking atau M-banking, dan layanan lainnya yaitu internet banking. Dengan menggunakan koneksi internet, para nasabah bisa melakukan aktivitas perbankan melalui komputer. Transaksi internet banking yang bisa dilakukan berupa memeriksa saldo, mentransfer uang, melakukan deposito, melihat laporan transaksi.

Perkembangan yang terjadi dalam kemajuan layanan perbankan yang menggunakan internet juga mempengaruhi dan membentuk tingkah laku masyarakat yang tidak bisa dibatasi dengan batas-batas wilayah dan waktu, sehingga dengan perkembangan itu juga menimbulkan kejahatan baru yang canggih yang disebut *cybercrime* (Kejahatan Dunia Maya). "*Cybercrime* adalah kejahatan yang dilakukan oleh seseorang atau sekelompok orang atau korporasi dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer."[2]

[1] Peneliti adalah staf di salah satu kantor advokat terkemuka di Surabaya.

[2] Widodo. 2009. *Sistem Pemidanaan dalam Cyber Crime.* Aswaja Pressindo, Yogyakarta, h. iii.

Kejahatan yang berhubungan dengan komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer. Kejahatan tersebut dibedakan menjadi 2 kategori, yakni *cybercrime* dalam pengertian sempit dan dalam pengertian luas. *Cybercrime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan *cybercrime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.[3]

Kejahatan perbankan seperti pencurian melalui ATM, pencurian data elektronik untuk transaksi keuangan elektronik dan masih banyak lagi. Bila kejahatan perbankan seperti ini terus terjadi, maka yang dirugikan sangat banyak tidak hanya dari nasabah yang rugi, namun juga bank yang mengalami penurunan kepercayaan. Pada nasabah, dana yang tersimpan di tabungan bisa berkurang tanpa ada transaksi yang dilakukan oleh pemilik, sementara data transaksi tercatat dengan lengkap, sehingga nasabah melakukan keluhan kepada bank atas transaksi tersebut.

Indonesia adalah negara hukum, hal ini tercantum dalam pasal 1 ayat 3 UUD 1945, sehingga aparat penegak hukum dalam menjalankan tugasnya harus mentaati hukum yang berlaku di Indonesia. Tidak lepas dari indonesia adalah negara hukum, penegak hukum juga dalam menangkap dan menegakkan hukum harus mempunyai dasar hukum yang kuat ini didasari dengan indonesia yang menganut asas legalitas yang dituangkan di dalam pasal 1 ayat 1 KUHP (Kitab Undang-undang Hukum Pidana), yaitu: "suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada".

KUHP sudah mengatur tentang pencurian, dimana tercantum dalam pasal 362, yaitu "Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian, kepunyaan orang lain dengan maksud untuk dimiliki secara melawan hukum, diancam, karena pencurian, dengan pidana penjara paling lama lima tahun atau denda paling banyak sembilan ratus rupiah". Peraturan itu mengatur tentang pencurian yang umum dilakukan oleh para pencuri biasa, akan tetapi sekarang sudah ada Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang mengatur juga tentang c*ybercrime,* walaupun sudah diatur dalam undang-undang ITE ini akan tetapi dalam pelaksanaannya undang-undang ini banyak menemui kendala.

Perkembangan teknologi informasi termasuk internet di dalamnya juga memberikan tantangan tersendiri bagi perkembangan hukum di Indonesia. Hukum di Indonesia dituntut untuk dapat menyesuaikan dengan perubahan sosial yang terjadi. Perubahan-perubahan sosial dan perubahan hukum atau sebaliknya tidak selalu berlangsung bersama-sama. Artinya pada keadaan tertentu perkembangan hukum mungkin tertinggal oleh perkembangan unsur-unsur lainnya dari masyarakat serta kebudayaannya atau mungkin hal yang sebaliknya.

---

[3] *Ibid,* hal. 24[3] Widodo. 2009. S*Istem Pemidanaan dalam Cyber Crime.* Aswaja Pressindo, Yogyakarta, h. iii.

[3] *Ibid,* h. 24.

Kendala dalam undang-undang ITE ini salah satunya dalam hal pembuktian terhadap pelaku, dimana untuk hal pembuktian memerlukan alat bukti sah yang tertuang dalam pasal 44 undang-undang ITE ini yang menyatakan:

> "Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut:
> a. alat bukti sebagaimana dimaksud dalam ketentuan perundang-undang; dan
> b. alat bukti lain berupa Inforasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)."

Dalam hukum acara pidana, Informasi dan/atau Dokumen elektronik dan/atau hasil cetaknya merupakan perluasan alat bukti lain selain yang telah diatur dalam Pasal 184 KUHAP. Hal ini juga ditegaskan dalam Pasal 44 huruf b Undang-undang ITE. Dengan kata lain, maksudnya adalah upaya untuk menghadirkan bukti Informasi Elektronik dalam memenuhi kategorisasi sebagai alat bukti yang dikenal dalam Pasal 184 KUHAP. Untuk itu, Informasi dan/atau Dokumen Elektronik pelaku pencurian di Bank melalui Internet itu biasanya terletak atau tersimpan di *harddisck*, sehingga pelaku bisa menghapus atau mengganti *harddisk* komputernya untuk menghilangkan jejak sehingga menyulitkan penyidik, atau dalam hal menjalankan aksinya dalam mencuri uang nasabah Bank di luar wilayah Indonesia, pelaku menggunakan komputer yang sering kali bersifat sewa jasa di Warung Internet (Warnet). Dalam Hal pelaku menggunakan komputer di Warnet dan melakukan pencurian uang pada nasabah Bank, apalagi yang dicuri uangnya adalah nasabah Bank di luar wilayah Indonesia, maka penegak hukum akan kesulitan mendapatkan alat bukti yang diperlukan.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi oleh penegak hukum, mengingat sulitnya penerapan hukum serta sulitnya melakukan pembuktian-pembuktian terhadap tindak kejahatan tersebut. Walaupun sulit untuk dibuktikan, akan tetapi pelaku harus tetap bertanggung jawab secara hukum.

RUMUSAN MASALAH

Cybercrime merupakan kejahatan baru yang timbul di masyarakat disebabkan oleh kemajuan teknologi informasi, salah satunya yaitu pencurian uang di bank melaui Internet. Seiring dengan timbulnya kejahatan baru tersebut, timbul juga kendala-kendala yang dihadapi oleh penegak hukum. Berdasarkan uraian tersebut, permasalahan yang diangkat oleh peneliti, yaitu: Bagaimanakah kendala pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melaui internet berdasarkan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

METODE PENELITIAN

Metode pendekatan yang dilakukan dalam penelitian ini adalah pendekatan yuridis normatif, yaitu suatu pendekatan yang terhadap hubungan antara faktor-faktor yuridis (hukum positif) dengan faktor-faktor normatif (asas-asas hukum), dengan cara Inventarisasi terhadap peraturan perundang-undangan yang berkaitan dengan *cybercrime* dan hal-hal lain

yang menjadi kendala dalam menanggulangi tindak pidana *cybercrime*. Selanjutnya, menganalisis perundang-undangan dan peraturan-peraturan yang telah diinventarisasi tersebut untuk mengetahui sejauh mana asas-asas dan peraturan perundang-undangan tersebut di atas bisa diterapkan untuk menanggulangi kendala yang ada. Metode pengumpulan bahan hukum yang digunakan oleh peneliti adalah dengan menggunakan metode studi kepustakaan dimana peneliti mengambil bahan hukum dari literatur yang digunakan untuk mencari konsep, teori-teori, pendapat-pendapat, maupun berita-berita yang dimuat di media massa yang berhubungan erat dengan permasalahan yang diteliti oleh peneliti.[4]

PEMBAHASAN

Kecanggihan dunia internet telah mencapai suatu tahap dimana perkembangannya begitu cepat, sehingga tidak mengherankan apabila sekarang di hampir setiap orang terhubung dengan internet. Bahkan, di perkotaan internet sudah menjadi kebutuhan primer bagi beberapa orang. Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan baru bermunculan, kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan internet dalam segala bidang seperti pendidikan, militer, perbankan dan lain-lain.

Globalisasi dan modernisasi yang telah memasuki bangsa ini membuat internet atau teknologi informasi hampir digunakan dalam kehidupan sehari-hari, khususnya dalam bidang perbankan. Sejumlah bank di Indonesia saat ini memanfaatkan teknologi informasi untuk meningkatkan layanan kepada para nasabahnya, sehingga dari kemajuan teknologi informasi itu muncullah banyak fasilitas layanan terhadap nasabahnya, misalnya: ATM (*Automated Teller Machine)* atau orang Indonesia biasa menyebutnya mesin ATM (Anjungan Tunai Mandiri), *mobile banking* atau M-banking, dan layanan lainnya yaitu internet banking. Dengan menggunakan koneksi internet, para nasabah bisa melakukan aktivitas perbankan melalui komputer. Transaksi internet banking yang bisa dilakukan berupa memeriksa saldo, mentransfer uang, melakukan deposito, melihat laporan transaksi.

Perkembangan yang terjadi dalam kemajuan layanan perbankan yang menggunakan internet juga mempengaruhi dan membentuk tingkah laku masyarakat yang tidak bisa dibatasi dengan batas-batas wilayah dan waktu, sehingga dengan perkembangan itu juga menimbulkan kejahatan baru yang canggih yang disebut *cybercrime* (Kejahatan Dunia Maya). *Cybercrime* yang terjadi pada layanan perbankan bermacam-macam bentuknya, salah satunya adalah menyalahgunakan data dalam pemanfaatan anjungan tunai mandiri (ATM), kejahatan ini telah membuat nasabah resah, uang nasabah diambil habis tanpa sepengetahuan si pemilik tabungan. Peristiwa seperti ini marak terjadi, seperti di Jakarta dan Bali. Bentuk lain dari pencurian uang nasabah di Bank yaitu melalui internet banking, pelaku pencurian membeli sesuatu barang secara online dengan menggunakan uang nasabah lain. Kenyamanan menggunakan mesin ATM pun kini masih melemah. Padahal, penggunaan transaksi dengan cara seperti ini tujuannya adalah memudahkan nasabah,

[4] Soerjono soekanto. 2010. *Pengantar Penelitian Hukum.* UI Press, Jakarta, h. 55.

dengan memberi rasa aman, praktis dan efisien tanpa harus nasabah mengambil uang di bank.

Kasus *cybercrime* yang paling banyak terjadi di Indonesia adalah berupa kejahatan internet untuk memesan barang dari perusahaan asing di luar negeri dengan menggunakan kartu kredit yang dipalsukan. Salah satu contoh kasus *cybercrime* yaitu seseorang yang bernama Buyung alias Sam, mahasiswa berusia 25 tahun asal bandung ini menggunakan kartu kredit orang lain untuk transaksi melalui internet, nilainya mencapai USD 15.000, aksi ini dilakukan melalui warnet selama satu tahun, kasus ini diserahkan Polda Jabar ke Mabes Polri, pertimbangannya karena kejahatan yang dilakukan tersangka berdampak ke berbagai negara, sehingga pengusutannya membutuhkan keterlibatan pihak Interpol. Terbongkarnya kejahatan Sam sendiri berawal dari laporan Interpol kepada Polda Jabar, pihak Interpol melaporkan adanya suatu pencurian melalui internet yang diduga melibatkan seorang warga negara Indonesia yang bertindak sebagai pemesan barang bernama Sam. Berdasarkan informasi tersebut, pihak Kepolisian segera melakukan pelacakan dan pencarian terhadap Sam, akhirnya melalui mengejaran yang terorganisir, Sam ditangkap dirumahnya di Bandung tanpa perlawanan. Belum jelas bagaimana kasus ini ditindaklanjuti sebab pihak kepolisian juga kurang terbuka kepada masyarakat, kabar yang beredar Sam dilepas setelah diberi semacam bimbingan oleh sejumlah praktisi TI (Teknologi Informasi) dan pihak Kepolisian untuk tidak mengulangi perbuatannya, Sam juga didesak agar memberi pesan moral kepada *carder* yang lain supaya menghentikan aksinya.

Ada juga kasus lain dalam pencurian uang di bank melalui internet, yaitu Pencurian dana nasabah bank yang terjadi di Jakarta. Nasabah *Internet banking* Bank Negara Indonesia (BNI) kehilangan uangnya sebesar Rp 9 juta oleh seseorang dengan menggunakan fasilitas internet. Korban sebelumnya mendapatkan *e-mail* yang mengatasnamakan BNI. *E-mail* tersebut di dalamnya terdapat sebuah *link* dengan alamat https://ibank.bni.co.id/directRetail/ibank, untuk konfirmasi identitas pelanggan BNI Internet Banking. *Link* tersebut membawa korban ke sebuah halaman situs *verifikasi login* ke BNI *Internet Banking* yang sama persis dengan halaman *login* milik BNI. pelaku memakai uang hasil curiannya untuk berbelanja melalui *shopping online* dan sebagian uangnya lagi di *transfer* ke rekening tabungannya.

Dalam kasus seperti di atas, banyak orang menyebutnya sebagai *carding database, carding database* adalah pencurian data nasabah berupa nomor rekening dan identitas nasabah melalui *database* bank tersebut, sehingga pelaku akan mendapatkan informasi tentang nasabah yang terkait untuk dijadikan target pencurian. Dalam kasus *carding database* pihak-pihak yang terkait, yaitu:

1. *Carder*

"Carder adalah pelaku dari *carding database* adalah yang memanfaatkan data kartu kredit orang lain untuk kepentingan sendiri. *Carder* menggunakan *e-mail*, *banner* atau *pop-up window* untuk menipu *netter* ke suatu situs *web* palsu, dimana *netter* diminta untuk memberikan informasi pribadinya".[5] Teknik umum yang sering digunakan oleh para *carder* dalam aksi pencurian adalah membuat situs atau *e-mail* palsu atau disebut juga *phising* dengan tujuan memperoleh informasi nasabah seperti nomor rekening, PIN (*Personal Identification Number)*,

[5] *Hacker, Cracker, & Carder.* http://diazadhika.blogdetik.com**.** diunduh pada tanggal 10 Januari 2013, Jam 09.30 WIB.

atau *password*. Pelaku kemudian melakukan konfigurasi PIN atau *password* setelah memperoleh informasi dari nasabah, sehingga dapat mengambil dana dari nasabah tersebut. Target *carder* yaitu pengguna layanan *internet banking atau* situs-situs iklan, jejaring sosial, *online shopping* dan sejenisnya yang ceroboh dan tidak teliti dalam melakukan transaksi secara *online* melalui situs internet. *Carder* mengirimkan sejumlah *email* ke target sasaran dengan tujuan untuk meng *up-date* atau mengubah *user ID* dan PIN nasabah melalui internet. *E-mail* tersebut terlihat seperti dikirim dari pihak resmi, sehingga nasabah sering kali tidak menyadari kalau sebenarnya sedang ditipu. Pelaku *carding database* mempergunakan fasilitas internet dalam mengembangkan teknologi informasi tersebut dengan tujuan yaitu menimbulkan rusaknya lalulintas mayantara demi terwujudnya tujuan tertentu antara lain keuntungan pelaku dengan merugikan orang lain disamping yang membuat, atau pun menerima informasi tersebut.

2. *Netter*

Netter adalah pengguna internet, dalam hal ini adalah penerima *email* (nasabah sebuah bank) yang dikirimkan oleh para *carder*.

3. *Cracker*

Cracker adalah sebutan untuk orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang dimasuki seperti pencurian data, penghapusan, penipuan, dan banyak yang lainnya.[6]

4. Bank

Bank adalah badan usaha yang melakukan kegiatan di bidang keuangan dengan menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan/atau bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak.[7]

Kejahatan-kejahatan yang dilakukan di dunia maya sudah diatur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Namun demikian, ada kejahatan yang tidak diatur secara khusus seperti pencurian uang di bank melalui internet.

Berkaitan dengan Pasal 32 Undang-undang ITE tersebut, peneliti akan menguraikan terlebih dahulu tentang Informasi Elektronik, Dokumen Elektronik, dan Sistem Elektronik. Menurut ketentuan Pasal 1 ayat (1) Undang-undang ITE, Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (*EDI*), surat elektronik, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Kemudian pengertian Dokumen Elektronik, menurut ketentuan Pasal 1 ayat (4) Undang-undang ITE, yang dimaksud dengan Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas

[6] *Pengertian Cracker.,* http://roniamardi.wordpress.com, diunduh pada tanggal 10 Januari 2013.

[7] Sunaryo, *loc.cit,* h. 10.

pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Dan yang terakhir adalah pengertian Sistem Elektronik, menurut ketentuan Pasal 1 ayat (5) Undang-undang ITE, yang dimaksud dengan Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Pertukaran informasi bisnis pada saat ini umumnya dilakukan dengan cara yang konvensional, yaitu menggunakan media kertas. Seiring dengan meningkatnya transaksi bisnis suatu perusahaan tentu akan meningkat pula penggunaan kertas. Hal ini dapat menimbulkan banyak masalah seperti keterlambatan dalam pertukaran informasi, kebutuhan akan bertambah jumlah personil yang sekaligus juga berarti menambah beban keuangan dalam perusahaan. Fakta-fakta ini telah menyebabkan ketidakefisienan dalam bisnis, khususnya yang berkaitan dengan pertukaran informasi bisnis. Persoalan di atas tentu harus kita cari jalan keluarnya agar efisiensi dalam transaksi bisnis dapat ditingkatkan. Kehadiran internet menjadi sebuah jawaban untuk mengatasi berbagai problema di atas. Namun, jaminan keamanan dalam transaksi melalui internet telah menimbulkan kekhawatiran orang untuk bertransaksi melalui media maya ini. Kehadiran Electronic Data Interchange (EDI) telah menjadi salah satu solusi untuk membuat keefisienan dalam transaksi bisnis di Internet dan sekaligus memberikan jaminan keamanan dalam bertransaksi tersebut. EDI adalah pertukaran data komputer antar aplikasi melintasi batas-batas organisasi, sehingga intervensi manusia atau interpretasi atas data tersebut oleh manusia dapat ditekan seminimum mungkin. Akibatnya data dalam EDI tentunya harus dalam format terstruktur yang bisa dipahami oleh masing-masing komputer. EDI *(Electronic Data Interchange)* merupakan suatu sistem yang memungkinkan data bisnis seperti dokumen pesanan pembelian dari suatu perusahaan yang telah memiliki sistem informasi dikirimkan ke perusahaan lain yang telah memiliki sistem informasi.

Dalam kasus pencurian pencurian uang di bank melaui internet yang mengunakan modus memalsukan kartu kredit orang lain untuk mencuri uangnya dan dibelanjakan secara online pada situs luar negeri. Unsur Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik tidak bisa dikenakan pada modus tersebut karena pelaku yang menggunakan modus *carding database* secara khusus tidak memenuhi unsur tersebut.

Peneliti akan menguraikan satu persatu unsur-unsur yang terdapat pada unsur objektif yang tidak terpenuhi apabila diterapkan, yaitu:

1. *Carding database* yang dilakukan pelaku tidak mengubah Informasi Elektronik dan/atau Dokumen Elektronik yang terdapat pada katru kredit korban.
2. Pelaku juga tidak menambah Informasi Elektronik dan/atau Dokumen Elektronik apapun yang ada pada kartu kredit korban.
3. Pelaku juga tidak mengurangi Informasi Elektronik dan/atau Dokumen Elektronik apapun pada kartu kredit korban waktu menjalankan aksinya.
4. Pelaku juga tidak mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang diambil di kartu kredit korban.

5. Pelaku juga tidak merusak Informasi Elektronik dan/atau Dokumen Elektronik kartu kredit atau sistem bank yang digunakan oleh korban.
6. Pelaku juga tidak menghilangkan Informasi Elektronik dan/atau Dokumen Elektronik apapun di dalam kartu kredit milik korban.
7. Mungkin unsur memindahkan ini yang sering diartikan bahwa pelaku mencuri uang milik korban, akan tetapi pelaku tidak memindahkan Informasi Elektronik dan/atau Dokumen Elektronik itu, karena Informasi Elektronik dan/atau Dokumen Elektronik kartu kredit milik korban tetap ada sehingga dalam hal seperti itu tidak bisa dikatakan bahwa pelaku memindahkan Informasi Elektronik dan/atau Dokumen Elektronik tersebut. Peneliti menganalogikan apabila ada seseorang memindahkan sebuah benda dari satu tempat ke tempat yang satunya, ketika benda yang dipindahkan tersebut sudah berpindah ke tempat yang satunya, apakah benda tersebut masih ada ditempat sebelumnya?, Jawabannya tentu saja tidak ada, karena benda tersebut sudah dipindahkan ke tempat yang satunya. Ilustrasi tersebut menjelaskan bahwa untuk modus *carding dtabase* unsur memindahkan dalam Pasal 32 ayat (1) secara khusus tidak bisa diterapkan.
8. Yang terakhir adalah unsur menyembunyikan, sudah tentu unsur ini tidak bisa diterapkan terhadap pelaku *carding database,* karena pelaku tidak menyembunyikan Informasi Elektronik dan/atau Dokumen Elektronik apapun dari kartu kredit korban.

Kemudian pada Pasal 32 ayat (2) Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yaitu:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak."

Pasal 32 ayat (2) Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengandung unsur-unsur, baik unsur subjektif maupun unsur objektif, yaitu:

Unsur Subjektif:	1. Dengan sengaja;
	2. Secara melawan hukum atau tanpa hak
Unsur Objektif:	1. Setiap orang.
	2. Memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak

Dari dua unsur subjektif dan unsur objektif juga diatas, unsur subjektif sudah terpenuhi, akan tetapi unsur objektif pada Pasal 32 ayat (2) Undang-undang Nomor 11 Tahun 2008 ada yang tidak terpenuhi. Unsur yang tidak terpenuhi adalah pada unsur Memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak

Kasus pencurian uang di bank melaui internet yang mengunakan modus memalsukan kartu kredit orang lain untuk mencuri uangnya dan dibelanjakan secara online pada situs luar negeri. Unsur Memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak tidak bisa dikenakan pada modus tersebut karena pelaku yang menggunakan modus *carding database* secara khusus tidak memenuhi unsur tersebut.

Unsur-unsur objektif dalam Pasal 32 ayat (2) Undang-undang ITE yang tidak terpenuhi apabila diterapkan, yaitu memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik. Seperti halnya pada Pasal 32 ayat (1) Undang-undang ITE, unsur memindahkan secara khusus tidak dapat diterapkan dalam kasus *carding database.* Selanjutnya unsur mentransfer, kata mentransfer berasal dari bahasa inggris yaitu dari kata transfer yang mempunyai arti memindahkan atau mengirimkan, dengan arti seperti itu apakah unsur mentransfer bisa diterapkan dalam kasus *carding database*?, sedangkan pelaku dalam menjalankan aksinya itu menggandakan Informasi Elektronik dan/atau Dokumen Elektronik kartu kredit milik korban. Jadi unsur-unsur memindahkan dan mentransfer juga tidak secara khusus dapat diterapkan dalam kasus pencurian uang di bank melalui internet dengan modus *carding database.*

Penggunaan analogi, dimana apabila dikaitkan dengan asas legalitas yang mengandung tiga pengertian, yaitu:

1. Tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan undang-undang.
2. Untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi. (kiyas)
3. Aturan-aturan hukum pidana tidak berlaku surut.[8]

Di salah satu pengertian asas legalitas Moeljatno mengatakan bahwa untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi (kiyas), akan tetapi peneliti dalam menjelaskan unsur memindahkan dalam Pasal 32 ayat (1) dan (2) Undang-undang ITE menggunakan analogi.

Dalam unsur memindahkan, peneliti tidak menganalogikan untuk menentukan adanya perbuatan pidana, tapi dengan menggunakan pemikiran secara *a contrario* pada hal yang dijelaskan tentang unsur memindahkan diatas, maka untuk mentiadakan perbuatan pidana berarti sah-sah saja peneliti menggunakan analogi (kiyas). Jadi, Pasal 32 ayat (1) dan (2) Undang-undang ITE tidak bisa diterapkan pada kasus pencurian uang di bank melalui internet, karena Unsur-unsur pasal tersebut tidak terpenuhi. Apabila penyidik ataupun penuntut umum memaksakan untuk membawa kasus pencurian uang di bank melalui internet ini ke muka persidangan, maka terdakwa bisa saja mendapatkan putusan bebas (*vrij spraak*) ataupun putusan pelepasan dari segala tuntutan hukum (*onslag van recht vervolging*).

Penindakan tidak bisa dilepaskan dengan sebuah pembuktian, karena untuk melakukan penindakan terhadap pelaku harus mempunyai dua alat bukti yang sah, seperti yang tercantum dalam ketentuan Pasal 183 KUHAP. Pembuktian merupakan titik sentral pemeriksaan perkara dalam sidang pengadilan. Pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan undang-undang yang boleh dipergunakan hakim membuktikan kesalahan yang didakwakan. Persidangan pengadilan tidak boleh semena-mena dan sesuka hati membuktikan kesalahan terdakwa.

Pembuktian-pembuktian dalam *cybercrime* cukup sulit dilakukan mengingat, bahwa hukum di Indonesia yang mengatur masalah ini masih banyak mengalami kendala yang dapat dimanfaatkan oleh para pelaku *cybercrime* untuk lepas dari proses pemidanaan. Di dalam sidang pengadilan penegak hukum tetap harus berpedoman terhadap KUHAP

[8] Moeljatno. 1987. *Asas-asas Hukum Pidana.* Bina Askara, Jakarta, h. 25.

walaupun untuk kejahatan dunia maya sudah diatur di dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Hal ini tercantum dalam pasal 44 undang-undang ITE ini yang menyatakan:

> "Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut:
> a. alat bukti sebagaimana dimaksud dalam ketentuan perundang-undang; dan
> b. alat bukti lain berupa Inforasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)."

Pasal 4 huruf (a) Undang-undang ITE tersebut menyebutkan bahwa alat bukti yang dimaksud adalah alat bukti yang tercantum dalam Pasal 184 ayat (1) KUHAP, yaitu:

a. Keterangan saksi,
b. Keterangan ahli,
c. Surat,
d. Petunjuk, dan
e. Keterangan terdakwa.

Karena *cybercrime, locus delictie*-nya terjadi di dunia maya, maka untuk membuktikan terhadap kejahatan yang terjadi seperti pencurian uang di bank melalui internet, alat bukti yang sering digunakan yaitu alat bukti Keterangan Ahli dan alat bukti yang disebutkan oleh Pasal 44 huruf (b) Undang-undang ITE, dimana alat bukti tersebut adalah Informasi Elektronik, Dokumen Elektronik, dan yang tercantum di Pasal 5 ayat (1), ayat (2), dan ayat (3) Undang-undang ITE, yaitu:

> "(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."

Untuk menemukan alat bukti tersebut penegak hukum akan mengandalkan seorang ahli komputer dan teknologi informasi karena untuk menemukan alat bukti digital dibutuhkan keahlian khusus. Disinilah yang menjadi kendala dalam membuktikan tindak pidana yang terjadi, karena alat bukti digital merupakan berupa data yang disimpan di dalam suatu harddisk komputer milik tersangka, sehingga apabila pelaku bisa menghapus data-data yang disimpan di dalam harddisk dan/atau menghilangkan harddisk tersebut maka bukti tersebut juga akan hilang. Sehingga, bukti digital yang dapat membuktikan atau yang mengarahkan perbuatan tersebut kepada pelaku juga ikut hilang.

Pembuktian yag hanya dengan menggunakan KUHAP akan sangat kesulitan dalam menghadapi kasus pencurian uang di bank melalui internet ini. Pada pencurian ini biasanya modus yang dipakai oleh pelaku adalah salah satunya juga pelaku mencari kode akses atas kartu kredit seseorang baik dengan cara 'menjebol' suatu situs yang menyimpan kode-kode akses kartu kredit maupun mendapatkannya dari situs yang dengan sengaja

menginformasikan kode-kode akses kartu kredit. Kemudian setelah ia mendapat kode akses tersebut ia pergunakan untuk membeli sesuatu di internet tanpa seijin maupun sepengetahuan si pemilik kartu kredit tersebut. Misalnya pun cara pertama yang dilakukan oleh pelaku maka hal ini bukan berarti kasus ini tidak dapat diajukan ke pengadilan dengan alasan KUHAP tidak mengakui alat bukti elektronik/digital. Pada kasus ini saya menduga kalangan yang 'pro' alat bukti elektronik akan mengatakan bahwa yang akan menjadi alat bukti adalah sistem komputer yang digunakan oleh pelaku, sistem komputer yang di 'jebol', maupun data elektronik yang menyatakan bahwa telah terjadi pembelian suatu barang atas kartu kredit korban.

Barang hasil kejahatan tersebut, misalnya sebuah komputer yang dibeli dari kejahatan tersebut akan dipergunakan sebagai barang bukti karena merupakan satu-satunya bukti yang nyata. Sehingga kembali ke alat bukti yang tercantum dalam Undang-undang ITE lagi, karena *cybercrime* sangat bergantung pada alat bukti digital. Untuk alat bukti lain yang ada di KUHAP juga bisa digunakan untuk membuktikan pelaku bersalah, tetapi akan sulit dalam penerapannya.

Alat bukti Keterangan Saksi akan sulit ditemukan dan hampir tidak ada ditemukan dalam pencurian uang di bank melalui internet ini seorang saksi, karena tindak pidana ini terjadi di dunia maya, tidak mungkin ada orang yang melihat, mengalami, mendengar secara langsung pada saat pelaku menjalankan aksinya. Untuk alat bukti surat juga tidak bisa digunakan dalam kasus *cybercrime,* karena dalam *cybercrime* tidak ada surat yang dibuat atas sumpah jabatan dalam bentuk fisik dan surat yang dikuatkan dengan sumpah.

Penindakan kasus cybercrime sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP (*Internet Protocol) Address* dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila pelaku menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana. Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat data serangan di log server sudah dihapus biasanya terjadi pada kasus *carding*, sehingga penyidik menemui kesulitan dalam mencari log statistik yang terdapat di dalam server sebab biasanya secara otomatis pelaku dengan cepat menghapus data yang ada untuk mengaburkan jejaknya. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti sedangkan data log statistik merupakan salah satu bukti vital dalam kasus *carding database* untuk menentukan arah datangnya serangan.

Penyelidikan merupakan tahap pertama yang dilakukan oleh penyidik dalam melakukan penyelidikan tindak pidana serta tahap tersulit dalam proses penyidikan. Karena dalam tahap ini penyidik harus dapat membuktikan tindak pidana yang terjadi serta bagaimana dan sebab-sebab tindak pidana tersebut untuk dapat menentukan bentuk laporan polisi yang akan dibuat. Informasi biasanya didapat dari NCB/Interpol yang menerima surat pemberitahuan atau laporan dari negara lain yang warganya menjadi

korban dalam pencurian uang di bank melalui internet, yang kemudian diteruskan ke Unit *cybercrime* atau satuan yang ditunjuk. Dalam penyelidikan kasus-kasus *cybercrime* yang modusnya seperti kasus *carding database,* metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika terutama dalam *undercover* dan *control delivery*. Petugas setelah menerima informasi atau laporan dari Interpol atau korban yang dirugikan melakukan koordinasi dengan pihak *shipping* untuk melakukan pengiriman barang. Permasalahan yang ada dalam kasus seperti ini adalah laporan yang masuk terjadi setelah pembayaran barang ternyata ditolak oleh bank dan barang sudah diterima oleh pelaku, disamping adanya kerjasama antara carder dengan karyawan *shipping* (jasa pengirim/pengepak barang) sehingga apabila polisi melakukan koordinasi informasi tersebut akan bocor dan pelaku tidak dapat ditangkap sebab identitas yang biasanya dicantumkan adalah palsu, hal tersebut apabila pelaku bekerja sama dengan pihak *shipping*.

Untuk kasus *carding database* atau mencuri data kartu kredit komputer orang lain secara ilegal, penyidikannya dihadapkan problematika yang rumit, terutama dalam hal pembuktian. Banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit, belum lagi kendala masalah bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan sumber daya manusia serta peralatan komputer forensik yang baik.

Banyak informasi beredar juga yang menginformasikan adanya penjebolan bank-bank swasta secara online oleh *cracker* tetapi korban menutup-nutupi permasalahan tersebut. Hal ini berkaitan dengan kredibilitas bank bersangkutan yang takut apabila kasus ini tersebar akan merusak kepercayaan terhadap bank tersebut oleh masyarakat. Dalam hal ini penyidik tidak dapat bertindak lebih jauh sebab untuk mengetahui arah serangan harus memeriksa server dari bank yang bersangkutan, bagaimana kita akan melakukan pemeriksaan jika kejadian tersebut disangkal oleh bank.

Penerapan pasal-pasal yang dikenakan dalam kasus *cybercrime* merupakan suatu permasalahan besar yang sangat merisaukan, misalnya apabila ada *cracker* yang melakukan pencurian uang di bank melalui internet tidak bisa dikenakan Pasal 362 KUHP, karena Pasal tersebut mengharuskan ada sebagian atau seluruhnya milik orang lain yang hilang, sedangkan dengan modus *carding database,* data yang dicuri oleh *cracker* tersebut sama sekali tidak berubah. Hal tersebut baru diketahui biasanya setelah selang waktu yang cukup lama karena orang yang mempunyai uang yang telah dicuri mengetahui setelah merasa uangnya berkurang dan tidak merasa mengambilnya, hal ini bisa diketahui dalam hal yang lama apabila korban juga melihat uangnya dikemudian hari. Pemeriksaan terhadap saksi dan korban banyak mengalami hambatan, hal ini disebabkan karena pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat. Mereka hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan tersebut seperti dana yang berkurang maupun kartu kredit tidak berfungsi, hal ini terjadi untuk kasus-kasus *carding database* tersebut. Untuk kasus carding, permasalahan yang ada adalah saksi korban kebanyakan berada di luar negeri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban.

Peranan saksi ahli sangatlah besar sekali dalam memberikan keterangan pada kasus *cybercrime*, sebab apa yang terjadi di dunia maya membutuhkan keterampilan dan keahlian yang spesifik. Saksi ahli dalam kasus *cybercrime* dapat melibatkan lebih dari satu orang saksi ahli sesuai dengan permasalahan yang dihadapi.

PENUTUP

Kendala pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melalui internet, antara lain:

1. Terdapat 2 (dua) kendala pokok dalam pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melalui internet. Kendala yang pertama yaitu terletak di penerapan pasal-pasalnya, dan kendala yang kedua terletak di keterbatasan sumber daya manusia (SDM) dalam pembuktian.
2. Perbuatan yang dilakukan oleh pelaku pencurian uang di bank melalui internet dengan modus *carding database,* apabila dijerat dengan Pasal 32 Informasi dan Transaksi Elektronik tindakan tersebut tidak bisa dipidana karena unsur-unsurnya seperti mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, dan mentransfer tidak terpenuhi, sehingga jelas Undang-undang Informasi dan Transaksi Elektronik tersebut tidak mengatur secara khusus tindak pidana pencurian uang di bank melalui internet dengan modus *carding database.*
3. Penindakan tidak bisa dilepaskan dengan sebuah pembuktian, karena untuk melakukan penindakan terhadap pelaku harus mempunyai dua alat bukti yang sah, walaupun *cybercrime* sudah diatur di peraturan perundang-undangan sendiri, akan tetapi untuk hukum formilnya tetap tidak bisa dipisahkan dengan KUHAP khususnya dalam alat bukti minimum yang tetap mengacu pada ketentuan Pasal 183 KUHAP.
4. Pembuktian dalam kasus *cybercrime* atau tindak pidana pencurian uang di bank melalui internet dengan modus *carding database* kesulitan dalam menemukan alat bukti keterangan saksi karena deliknya yang terjadi di dunia maya, sehingga untuk alat bukti yang digunakan banyak bertumpu pada alat bukti keterangan ahli.
5. Alat bukti digital yang digunakan dalam Undang-undang Informasi dan Transaksi Elektronik untuk membuktikan tindak pidana yang terjadi disimpan di dalam Harddisk, sehingga tidak gampang ditemukan oleh penegak hukum karena data yang disimpan dalam Harddisk ini rawan dimanipulasi dan dihilangkan/dihapus oleh pelaku.
6. Penangkapan tersangka dan penyitaan alat buktinya mengalami hambatan karena pelaku menggunakan komputer yang bisa menjalankan dari tempat mana saja, sehingga aparat penegak hukum sering kali tidak dapat menentukan secara pasti siapa pelakunya.
7. Penyelidikan merupakan tahap tersulit yang dialami oleh aparat penegak hukum, karena dalam tahap ini aparat penegak hukum tidak hanya harus dapat membuktikan tindak pidana yang terjadi, akan tetapi aparat penegak hukum harus juga menentukan sebab-sebab tindak pidana tersebut untuk dapat menetukan bentuk laporan polisi yang akan dibuat.
8. Dalam hal penindakan untuk memberantas *cybercrime,* sumber daya manusia seperti aparat penegak hukumnya kurang, karena untuk memberantas tindak pidana ini

dibutuhkan keahlian khusus di bidang komputer, sedangkan aparat kepolisian yang mempunyai divisi *cybercrime* yang bertaraf internasional hanya terletak di Mabes Polri.

9. Perlunya pembaharuan peraturan perundang-undangan yang mengatur tentang *cybercrime,* baik formil maupun materil. Seperti memperbaharui Undang-undang Nomor 11 Tahun 2008 tentang Infomasi dan Transaksi Elektronik, ataupun bisa juga perubahan itu dilakukan terhadap Kitab Undang-undang Hukum Pidana (KUHP) dan Kitab Undang-undang Hukum Acara Pidana (KUHAP).
10. Mengingat terbatasnya sumber daya manusia dalam memberantas tindak pidana *cybercrime,* penegak hukum hendaknya mengirimkan anggotanya untuk mengikuti kursus-kursus atau pelatihan-pelatihan di negara-negara maju agar nantinya ilmu yang diperoleh dapat diterapkan di Indonesia, khususnya ilmu yang berkaitan dengan pemberantatasan tindak pidana kejahatan dunia maya atau *cybercrime.* Selain di Kepolisian perlunya dibentuk unit khusus yang menangani kejahatan dunia maya atau *cybercrime* dalam setiap pemeriksaan, seperti di Kejaksaan, Komisi Pemberantasan Korupsi (KPK), dan pengadilan.

DAFTAR BACAAN

Buku

Arief, Barda Nawawi. 2006. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia.* Raja Grafindo Persada, Jakarta.

Lamintang, P.A.F dan Lamintang, Theo. 2009. *Delik-delik khusus: Kejahatan Terhadap Harta Kekayaan.* Sinar Grafika, Jakarta.

Marzuki, Peter Mahmud. 2009. *Penelitian Hukum.* Prenada Media Group, Jakarta.

Moeljatno. 1987. *Asas-Asas Hukum Pidana*. Bina Askara, Jakarta.

Prodjodikoro, Wirjono. 1986. *Tindak-tindak Pidana Tertentu di Indonesia.* Eresco, Bandung.

Soekanto, Soerjono. 2010. *Pengantar Penelitian Hukum.* UI Press, Jakarta.

Subekti, R. 2008. *Hukum Pembuktian.* Pradnya Paramita, Jakarta.

Suhariyanto, Budi. 2012. *Tindak Pidana Teknologi Informasi.* Raja Grafindo Persada, Jakarta.

Sunaryo. 2009. *Hukum Lembaga Pembiayaan*. Sinar Grafika, Jakarta.

Widodo. 2009. S*istem Pemidanaan dalam Cyber Crime.* Aswaja Pressindo, Yogyakarta.

Williams, Brian K. dan Sawyer, Stancey C. 2007. *Using Information Technology: Pengenalan Praktis Dunia Komputer dan Komunikasi.* Andi, Yogyakarta.

Zacharia, Herry Purnomodan Theo. 2005. *Pengenalan Informatika Perspektif Teknik dan Lingkungan.* Andi, Yogyakarta.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Kitab Undang-undang Hukum Pidana (KUHP).

Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana.

Herzien Inlandsch Reglement (HIR).