E-ISSN : 2774-5783
Volume 2 No. 1 Oktober 2021

PENCURIAN UANG PADA REKENING BANK DENGAN MEDIA INTERNET (ANALISIS KASUS PASAL 362 KUHP JO UNDANG-UNDANG RI NOMOR 11 TAHUN 2008 TENTANG INFORMASI TRANSAKSI ELEKTRONIK)

Fatin Hamamah dan Yanti Apriyani
Fakultas Hukum Universitas 17 Agustus 1945 Cirebon
Email: fatinpdihunissula@gmail.com

Received:
02 September 2021
Accepted:
20 September 2021
Published:
25 Oktober 2021
Kata kunci:
Pencurian uang, media internet

ABSTRAK

Globalisasi memberikan banyak dampak salah satunya adalah bekembangnya teknologi seperti internet yang kita rasakan saat ini. Media Internet yang memberikan kemudahan kehidupan kita seperti kegiatan operasional bank yang bisa diakses melalui internet. Namun, penggunaan internet pada bank juga mempunyai dampak negatif salah satunya adalah pencurian melalui media internet dengan berbagai macam kasus. Berdasarkan uraian diatas peneliti memiliki tujuan untuk mengetahui bagaimana Hal ini dapat dilihat dari Pasal 362 KUHP jo Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik dan bagaimana pembuktian tindak pidana pencurian dana di media internet dalam suatu tindak pidana. Pembukaan rekening bank di media internet melalui teknologi informasi. Penulis mengambil pendekatan normatif, yaitu berdasarkan hukum pidana empiris Indonesia, dengan fokus pada pengaturan tentang tindak pidana pencurian dana melalui rekening bank dengan fasilitas internet. Hasil penelitian ini adalah tindak pidana pencurian rekening bank media internet berdasarkan Pasal 362 KUHP dan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik. dari bank-bank di Indonesia.Hukum terhadap kerupuk. Untuk tindak pidana pencurian dana rekening bank melalui teknologi informasi dengan menggunakan media jaringan digunakan alat bukti elektronik untuk melengkapi alat bukti yang ditentukan dalam Pasal 184 KUHAP alinea pertama.

ABSTRACT

Globalization has many impacts, one of which is the development of technology such as the internet that we feel today. Internet media that provide convenience in our lives such as bank operations that can be accessed via the internet. However, the use of the internet in banks also has a negative impact, one of which is theft through the internet with various cases. Based on the description above, the researcher aims to

find out how this can be seen from Article 362 of the Criminal Code in conjunction with the Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Transaction Information and how to prove the crime of theft of funds on the internet in a criminal act. Opening a bank account on the internet through information technology. The author takes a normative approach, which is based on Indonesian empirical criminal law, with a focus on the regulation of criminal acts of theft of funds through bank accounts with internet facilities. The results of this study are the theft of internet media bank accounts based on Article 362 of the Criminal Code and the Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Transaction Information. from banks in Indonesia. The law on crackers. For criminal acts of theft of bank account funds through information technology using network media, electronic evidence is used to complete the evidence specified in Article 184 of the first paragraph of the Criminal Procedure Code.

Coresponden Author: Fatin Hamamah
Email: fatinpdihunissula@gmail.com

PENDAHULUAN

Manusia adalah makhluk sosial, jadi manusia tidak bisa hidup sendiri, membutuhkan orang lain untuk saling membantu. Aristoteles mengatakan bahwa manusia adalah politikus di kebun binatang, artinya manusia pada dasarnya ingin bergaul dengan orang lain dan berkumpul bersama. Setiap orang memiliki seperangkat kebutuhan yang mungkin sama dengan kebutuhan orang lain, sehingga dapat bekerja sama untuk mencapai tujuan setiap orang. Mungkin kebutuhan atau kepentingan berbeda dengan kebutuhan atau kepentingan orang lain sehingga menimbulkan konflik dan konflik sosial.

Oleh karena itu, hukum didasarkan pada kesadaran diri manusia dan diproduksi dalam pergaulan manusia, merupakan gejala sosial dan hasil pengukuran kualitas perilaku manusia dalam kehidupan bermasyarakat. Undang-undang menjamin bahwa suatu kelompok sosial tertentu tidak mengalami ketidakseimbangan psikis dan fisik dalam kehidupannya, yang berarti selalu menjaga terciptanya keadilan sosial bagi masyarakat.

Hukum dalam masyarakat biasanya dikumpulkan dalam suatu sistem yang sengaja diatur sesuai dengan bidangnya. Jadi hukum juga merupakan masyarakat, kehidupan manusia itu sendiri, dari sudut pandang tertentu, itu adalah hubungan kehidupan yang teratur (Van Apeldoorn, 1996). Hukum pidana bertujuan untuk menemukan kebenaran dalam arti hakiki, yaitu kebenaran yang mendekati keadaan yang sebenarnya (Prodjodikoro, 2003).

Dalam perkara pidana, setiap aparat penegak hukum dituntut untuk lebih tegas, teliti, dan kritis terhadap pelanggaran, serta melindungi setiap orang dari pelanggaran (Yuswandi, 1995). Perbuatan yang dianggap sebagai tindak pidana, di Indonesia menganut asas legalitas (asas legalitas), yaitu asas penetapan bahwa tidak ada perbuatan yang dilarang dan perbuatan yang belum ditentukan terlebih dahulu diancam dengan hukum pidana dalam undang-undang tersebut (Hamzah, 2004).

Dalam peraturan perundang-undangan Indonesia diatur dalam Pasal 1(1) KUHP yang lazim disebut dengan bahasa latin *Nullum Delictum Nulla Poena Sine Praevia lege* (Hamzah, 2004). Penemuan-penemuan baru di bidang teknologi, terjadinya revolusi, modernisasi pendidikan, dll terjadi di satu tempat dan akan segera diketahui oleh masyarakat lain yang jauh dari tempat itu.(Soekanto, 1977)

Satjipto Rahardjo menyatakan bahwa dampak industrialisasi dan penggunaan teknologi modern terhadap kehidupan masyarakat menuntut hukum untuk menyesuaikan diri dengan perubahan-perubahan yang diakibatkan oleh pengaruh tersebut (Soekanto, 1977).

Jika kita mengamati kehidupan di sekitar kita, sulit untuk menyangkal bahwa penggunaan teknologi modern telah mengambil alih kehidupan kita. Dibandingkan dengan era sejarah manusia, teknologi modern ini memang masih sangat tua. Meski begitu, dampaknya terhadap kehidupan sosial manusia sulit dibandingkan dengan peristiwa lain di dunia.

Pada awalnya, Internet tidak dibangun untuk sistem komunikasi global seperti sekarang. Ini pertama kali digunakan oleh militer AS pada akhir 1960-an. Badan Proyek Penelitian Lanjutan Departemen Pertahanan AS mulai mendanai proyek untuk mengembangkan jaringan komputer guna mendukung kegiatan penelitian militer.

Teknologi komputer yang didukung oleh fasilitas internet telah memungkinkan kegiatan di berbagai bidang, namun respon legislator dan pengadilan tampaknya setengah hati. Faktor penting dalam perumusan dan perluasan hukum pidana adalah ruang lingkup penerapan perbuatan terlarang yang baru. Hukum pidana berkaitan dengan kebebasan sipil dan kebebasan individu. Perilaku "meretas" adalah contohnya. Jika akses tidak sah ke sistem komputer dikriminalisasi, itu berarti peretasan akan dikenakan hukum pidana, dan akses ke halaman tanpa izin adalah analogi fisik peretasan komputer dan hanya dapat diselesaikan melalui hukum perdata. Dikatakan bahwa dibandingkan dengan hak milik fisik lainnya, hukum seharusnya tidak terlalu melindungi, dan tidak diperbolehkan masuk tanpa izin (Bainbridge, 2004).

Kasus penggunaan fasilitas Internet untuk mencuri bank tahun 2003 adalah kasus Dody Susilo Haryanto yang tinggal di Malang, yang diduga mencuri rekening bank seorang warga negara AS bernama Wong Sin yang tinggal di Los Angeles. , Amerika. Dody yang masih kuliah di Sekolah Koefisien Elektronika dan Ilmu Pengetahuan Alam Universitas Brawijaya itu dituduh menarik uang sebesar US$ 6.700 dari rekening Wong Sin. media massa. Dodi mengklaim telah mengambil $600.

Selain itu, Indonesia baru-baru ini menjadi aktif karena berita pembobolan ATM. Akibat pencurian oleh orang yang tidak bertanggung jawab, klien tiba-tiba kehilangan saldo rekeningnya. Karena mereka memiliki informasi, terutama di industri perbankan, tidak dapat dihindari bagi pemegang kartu kredit untuk menggunakan fasilitas Internet untuk mencuri dana dari rekening bank. Di Indonesia, tidak ada peraturan khusus mengenai penggunaan internet untuk mencuri dana dari rekening bank. Hanya ada bentuk utama pencurian yang diatur dalam Pasal 362 KUHP.

Penggunaan fasilitas Internet untuk mencuri uang melalui rekening bank dilakukan oleh para penjahat.Komputer di rumah atau warnet yang menyewakan Internet sudah cukup.Selama Anda dapat terhubung ke Internet, Anda dapat menggunakan fasilitas tersebut di mana saja. Penjahat dapat menggunakan Internet untuk mencuri dana dari rekening bank hanya dengan menggerakkan jari mereka, tanpa menyentuhnya secara aktif.

Berdasarkan latar belakang masalah tersebut, penulis tertarik untuk melakukan penelitian dalam bentuk karya tulis ilmiah yang berjudul: Pencurian Uang di Rekening Bank dengan Media Internet (Analisis Kasus Pasal 362 KUHP No. 11 Undang-Undang tentang Informasi Transaksi Elektronik Tahun 2008).

Dari uraian tersebut di atas dapat dirumuskan permasalahannya sebagai berikut:

1. Bagaimana tindak pidana pencurian uang pada rekening bank dengan media internet dipandang dari Pasal 362 KUHP Jo Undang-Undang RI Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik ?
2. Bagaimana pembuktian dalam tindak pidana pencurian uang pada rekening bank dengan media internet melalui teknologi informasi ?

Tujuan dari penelitian ini adalah untuk mengetahui tindak pidana penggunaan media internet untuk mencuri dana rekening bank juncto Pasal 362 Hukum Pidana Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik. Dalam rangka pemanfaatan teknologi informasi untuk

menemukan barang bukti tindak pidana pencurian dana rekening bank dengan menggunakan media online. Artikel penelitian ini diharapkan memiliki kegunaan teoritis dan praktis, yaitu hasil penelitian ini diharapkan dapat menambah wacana ilmu hukum secara umum khususnya perkembangan hukum pidana, serta masalah pencurian dana melalui media bank. akun dengan bahan pustaka peneliti yang relevan. Internet. Sebagai pengetahuan dan informasi masyarakat dan mahasiswa hukum, serta memberikan ide bagi para praktisi khususnya pemerintah untuk membuat undang-undang dan aparat penegak hukum, dalam hal ini kepolisian dan kejaksaan akan menerbitkan akun media online untuk tindak pidana pencurian uang melalui bank. Menurut dasar hukumnya, menggunakan Internet untuk mencuri dana melalui rekening bank adalah kejahatan menggunakan teknologi informasi.

Pencurian adalah kepemilikan rahasia barang atau milik orang lain. Pasal 362 sampai dengan 365 KUHP mengatur tentang pencurian, antara lain:

a) Pencurian Biasa Pasal 362 :

"Barang siapa mengambil sesuatu barang, yang sama sekali atau sebagian termasuk kepunyaan orang lain, dengan maksud akan memiliki barang itu dengan melawan hak, dihukum, karena pencurian , dengan hukuman penjara selama-lamamya lima tahun atau denda sebanyak-banyaknya Rp 900,-."

Dari perspektif mengambil tindakan ini, pencurian adalah kejahatan formal. Mengambil adalah suatu perbuatan/perbuatan material yang positif, biasanya dilakukan dengan menggunakan jari tangan dan gerakan otot sadar tangan, kemudian mengarahkan jari tangan dan jari ke suatu benda, menyentuhnya, memegangnya dan mengangkatnya, kemudian membawa dan memindahkannya ke tempat lain atau di bawahnya. kontrol... Yang dimaksud di sini adalah bahwa tindakan memperoleh adalah tindakan aktif yang diarahkan pada objek dan mengubah kekuatan objek menjadi kekuatannya. Sebelum pelaku mengambil barang tersebut, ia tahu bahwa memiliki barang orang lain adalah ilegal. Pendapat ini sesuai dengan data yang ada, yaitu jika unsur kesengajaan secara jelas disebutkan dalam rumusan tindak pidana, berarti kesengajaan itu harus ditujukan kepada Semua unsur yang melatarbelakanginya, misalnya unsur objektif meliputi unsur perilaku perolehan, unsur objek yang seluruhnya atau sebagian dimiliki oleh orang lain, dan unsur subjektif seperti niat untuk memiliki adalah tidak sah.

b) Pencurian dengan Pemberatan (*gequalifiseer*)

Pasal 363, yang berbunyi :

(1)Dihukum penjara selama-lamanya tujuh tahun :

ke-1 : Pencurian ternak;

ke-2 : Pencurian pada waktu kebakaran, peletusan, banjir, gempa bumi, atau gempa laut, peletusan gunung api, kapal karena terdampar, kecelakaan kereta api, huru-hara, pemberontakan atau bahaya perang.

ke-3 : Pencurian waktu malam dalam sebuah rumah atau dipekarangan tertutup yang ada rumahnya, dilakukan oleh orang yang ada disitu tiada dengan setahunya atau tiada dengan kemauan yang berhak;

ke-4 : Pencurian yang dilakukan oleh 2 orang atau lebih bersama-sama;

ke-5 : Pencurian yang dilakukan untuk dapat masuk ketempat kejahatan atau untuk dapat mengambil barang yang akan dicuri itu, dengan jalan membongkar, merusak atau memanjat atau memakai anak kunci palsu atau pakaian jabatan palsu.

(2)Jika pencurian yang diterangkan dalam no. 3 disertai dengan salah satu hal tersebut dalam no. 4 dan 5, maka dijatuhkan hukuman penjara selama-lamanya 9 tahun (Moch, 1979).

c) Pencurian Ringan

Pasal 364 :

"Perbuatan yang diterangkan dalam pasal 362, dan pasal 363ayat (1) no. 4, begitu juga perbuatan yang diterangkan dalam pasal 363 ayat (1) no. 5, asal sajatidak dilakukan dalam sebuah rumah atau dalam pekarangan tertutup yang ada rumahnya dan jika barang yang dicuri itu tidak lebih dari dua ratus lima puluh rupiah, dihukum

sebagai pencurian ringan, dengan hukuman penjara selama-lamanya tiga bulan atau denda sebanyak-banyaknya Rp 900,-."

d) Pencurian dengan Kekerasan

Pasal 365 :

(1) Dengan hukuman penjara selama-lamanya sembilan tahun, dihukum pencurian yang didahului, disertai atau diikuti dengan kekerasan atau ancaman kekerasan terhadap orang, dengan maksud akan menyiapkan atau memudahkan pencurian itu atau jika tertangkap tangan (terpergok) supaya ada kesempatan bagi diri sendiri atau peserta lain dalam kejahatan itu untuk melarikan diri atau supaya barang yang dicurinya tetap tinggal ditangannya.

(2) Hukuman penjara selama-lamanya dua belas tahun dijatuhkan :

ke-1: Jika perbuatan itu dilakukan pada malam didalam sebuah rumah atau pekarangan tertutup yang ada rumahnya atau dijalan umum atau dalam kereta api atau trem yang sedang berjalan;

ke-2: Jika perbuatan itu dilakukan bersama-sama oleh dua orang atau lebih;

ke-3: Jika yang bersalah masuk ketempat melakukan kejahatan itu dengan pembongkaran atau memanjat atau memakai anak kunci pasu, perintah palsu atau pakaian jabatan palsu;

ke-4: Jika perbuatan menimbulkan akibat luka berat pada seseorang;

(3) Hukuman penjara selama-lamanya 15 tahun dijtuhkan jika karena perbuatan itu ada orang mati.

(4) *Hukuman mati atau hukuman penjara seumur hidup atau penjara sementara selama-lamanya dua puluh tahun dijatuhkan, jika perbuatan itu menjadikan ada orang mendapat luka berat atau mati, dilakukan oleh 2 orang bersama-sama atau lebih dan disertai pula pleh salah satu hal yang diterangkan dalam no.1 dan 3.*

Terakhir, menurut unsur obyektif dan subyektif Pasal 362 KUHP, dapat juga dijelaskan bahwa pencurian merupakan tindak pidana formil. Mengambil adalah suatu perbuatan/perbuatan material yang positif, biasanya dilakukan dengan gerakan otot sadar dengan menggunakan jari tangan dan jari tangan, kemudian mengarahkan jari dan jemari ke arah suatu benda, menyentuhnya, memegangnya dan mengangkatnya, kemudian membawa dan memindahkannya ke tempat lain atau di bawahnya. control. Yang dimaksud di sini adalah bahwa tindakan yang dilakukan adalah tindakan aktif, yang ditujukan pada objek dan mengubah kekuatan objek menjadi kekuatannya.

METODE

Dalam setiap penulisan ilmiah agar dapat dipertanggung jawabkan dari faktor-faktor yang bisa diselidiki, maka harus ada metode untuk membahas masalah-masalah ini.

1. Metode Pendekatan

   Dalam artikel ini, penulis mengambil pendekatan normatif, yaitu berfokus pada hukum pidana empiris Indonesia tentang tindak pidana pencurian dana melalui rekening bank dengan fasilitas internet. Selain itu, penelitian ini dilakukan melalui kegiatan peradilan.

2. Spesifikasi Penelitian

   Spesifikasi yang digunakan dalam penelitian ini adalah penelitian yang berdasarkan data yang diperoleh dilapangan dan dapat dipadukan dengan teori sehingga penelitian ini dapat dipertanggung jawabkan kebenarannya yang sesuai dengan undang-undang.

3. Teknik Pengumpulan Data

   a. Penelitian kepustakaan

      Merupakan studi untuk memperoleh data dengan mengumpulkan dan meneliti informasi, teori dan pendapat ahli tentang semua masalah yang terkait dengan masalah yang dibahas dalam artikel ini, termasuk bahan hukum utama dan bahan hukum sekunder yang digunakan dalam penelitian.

b. Dokumentasi

Dokumen adalah suatu cara untuk memperoleh informasi atau bukti yang berkaitan dengan masalah penelitian, dengan cara mencatat bahan hukum mayor dan minor yang diperoleh dari surat kabar dan media internet sebagai bahan pendukung.

4. Analisis Data

Konsep-konsep analisis di atas dilakukan secara bertahap, dikumpulkan melalui proses analisis kritis dan identifikasi, kemudian melalui prosedur klasifikasi sistem logis sesuai dengan pokok permasalahan yang disusun dalam artikel ini dan sistematis, sehingga dapat ditarik analisisnya yaitu, untuk menarik kesimpulan dari data tertentu.

HASIL DAN PEMBAHASAN

Tinjauan Umum Tentang Internet

Perkembangan Internet di Indonesia

Internet pertama kali diperkenalkan ke Indonesia pada tahun 1994 melalui lembaga pendidikan. Internet di Indonesia saat ini berkembang sangat pesat. Memang kecepatan pembangunan lebih rendah dari kecepatan pembangunan, tetapi menunjukkan pertumbuhan yang cukup tinggi. Perkembangan internet telah melahirkan e-commerce yang merupakan pilihan bisnis yang menjanjikan, karena e-commerce dipandang banyak memberikan kemudahan bagi kedua belah pihak, termasuk pedagang dan pembeli. Keberadaan e-commerce di Indonesia dipelopori oleh toko buku online bernama Sanur. Ide bisnis e-commerce yang pertama kali muncul dalam bentuk toko buku online terinspirasi dari bisnis e-commerce sejenis yaitu http://www.amazon.com, sanur adalah sebuah usaha dan menjadi perusahaan Indonesia pertama yang menjual buku di Internet Bookstore. Saat ini, Sanur melakukan 2.500 transaksi sebulan, menawarkan 30.000 buku, dan memiliki 11.000 pelanggan (Andi, 2001).

Berbagai layanan dapat diperoleh melalui internet. Layanan Internet ini disediakan oleh penyedia layanan Internet atau penyedia layanan Internet (ISP) yang menyediakan akses Internet kepada pelanggan mereka (Wahid, 2005). Layanan-layanan tersebut antara lain adalah :

1) E-mail atau e-mail memungkinkan seseorang untuk mengirim dan menerima surat melalui internet. Pada awalnya email hanya berupa teks tanpa gambar/grafik, namun sekarang kita dapat membuat email dengan teks dan gambar yang indah, selain itu pengirim juga dapat menyertakan lampiran berupa file atau grafik.
2) Berita atau news mirip dengan poster yang dipasang di papan pengumuman, semua orang bisa membacanya. Berita dikelompokkan ke dalam newsgroup.
3) Pengguna internet dapat mengirim (upload) dan mengambil (download) file dari komputer lain yang terhubung ke Internet.
4) Internet Relay Chat (IRC) adalah percakapan tertulis yang dilakukan melalui Internet. IRC adalah forum diskusi atau pertemuan jarak jauh.
5) World Wide Web (WWW) atau disebut juga dengan website adalah informasi yang disajikan dalam bentuk halaman-halaman yang berisi teks dan/atau gambar/grafik. Sebuah halaman web dapat memiliki link ke halaman manapun, sehingga terlihat seperti jaring laba-laba (web) di dunia, sehingga disebut World Wide Web.

Diantara layanan yang diberikan internet yang dikenal dan umum dilakukan antara lain :

a. E-commerce, contoh paling umum dari aktivitas semacam ini adalah aktivitas transaksi perdagangan umum yang dilakukan melalui Internet. Melalui e-commerce, penjual (merchant) dapat menjual produknya lintas negara, karena sifat internet itu sendiri yang melintasi batas negara. Transaksi dapat terjadi secara real time dimana saja, selama terkoneksi dengan internet. Umumnya transaksi yang dilakukan melalui fasilitas e-commerce dilakukan melalui sebuah website, dimana website tersebut bertindak sebagai semacam etalase untuk produk yang dijual. Di website ini pembeli bisa melihat barang yang ingin dibeli, kemudian jika tertarik bisa melakukan transaksi dan lain sebagainya.

b. Bay e-banking, yang diartikan sebagai kegiatan perbankan yang dilakukan di dunia maya (virtual) melalui fasilitas internet. Layanan ini memungkinkan bank dan nasabah bank untuk melakukan berbagai jenis transaksi perbankan melalui internet khususnya melalui internet. Melalui internet, masyarakat dapat melihat saldo tabungan, transfer dana antar rekening untuk membayar tagihan, dan lainnya.
c. E-government bukanlah model pemerintahan baru yang didasarkan pada dunia Internet, tetapi penggunaan teknologi Internet oleh departemen-departemen pemerintah. Pemerintah dapat menggunakan fasilitas ini dalam memberikan pelayanan publik. Dengan membuat stius tertentu, pemerintah dapat memberikan informasi kebijakan pemerintah mulai dari regulasi hingga prosedur sehingga masyarakat yang berkunjung dapat memahaminya. Tentu menarik untuk mewujudkan pemerintahan yang bersih dan pemerintahan yang baik dalam kerangka demokrasi.
d. E-Learning, istilah ini diartikan sebagai sekolah dalam dunia maya (virtual). Pengertian E-Learning sendiri sebenarnya sangat luas, bahkan portal informasi mata pelajaran pun dapat dimasukkan dalam E-Learning ini. Namun pada prinsipnya istilah tersebut bertujuan untuk mengubah proses belajar mengajar di sekolah secara digital melalui teknologi internet.Pengertian Perdagangan Elektronik

E-commerce, atau e-commerce untuk jangka pendek, adalah kegiatan bisnis yang melibatkan konsumen (konsumen), produsen (produsen), penyedia layanan dan perantara dengan menggunakan jaringan komputer (jaringan komputer), artinya e-commerce telah mencakup ruang lingkup penuh dari kegiatan usaha (Suparni, 2009). Sejak munculnya website, perusahaan bisnis di seluruh dunia mulai memperhatikan internet sebagai tempat untuk mempromosikan produk atau jasa mereka. Hal ini terjadi karena Web memungkinkan penggunaan nama domain untuk menampilkan grafik, suara, dan gambar yang bergerak di Internet. Bisnis/transaksi melalui internet seperti ini biasa disebut e-commerce.

Kejahatan dalam e-commerce (e-commerce) meliputi penipuan online, penipuan pemasaran online berlapis, dan penipuan kartu kredit (Partodihardjo, 2009).

Hubungan hukum pada website adalah hubungan hukum antara perusahaan dengan perusahaan, perusahaan dengan konsumen, perusahaan dengan pemerintah. Secara umum, dalam hal ini website e-commerce dapat diartikan sebagai segala bentuk perdagangan atau perdagangan barang dan jasa yang dilakukan melalui website dengan menggunakan media elektronik komputer (Partodihardjo, 2009). Jadi singkatnya, e-commerce adalah bentuk bisnis modern yang dilakukan melalui Internet. Dalam praktik penggunaan dan pemanfaatan teknologi atau jaringan internet, dalam hal ini situs e-commerce memiliki jaringan global yang luas, sehingga masyarakat dapat dengan mudah mengaksesnya setiap saat tanpa adanya kontak fisik antara pengguna/konsumen dan penjual.

Penggunaan Fasilitas Internet Oleh Pihak Perbankan

Sebagaimana disebutkan di atas, dengan semakin majunya teknologi internet, khususnya penggunaan website sebagai media transaksi di dunia maya, bank-bank selanjutnya meningkatkan kualitas kegiatan usahanya, dan bank-bank tersebut juga menggunakan komputer sebagai salah satu penunjang kegiatannya. Bank..

Lembaga perbankan memiliki berbagai fasilitas yang disediakan oleh bank, seperti perbankan online dengan sistem online. Tujuan organisasi komputer yang menggunakan komputer adalah untuk secara efektif dan efisien meningkatkan layanan pelanggan untuk membantu menghasilkan informasi yang baik dan sempurna. 1946 Surat Pernyataan Kasir/Kasir Bank Nasional Indonesia tentang penerapan perangkat komputer dalam tugasnya sebagai kasir

> *"..... Sebelum menggunakan sistem on-line, nasabah memang kelihatan ramai; yang ingin mencairkan cek misalnya harus antri sambil menunggu nomor. Sekarang dengan memencet keyboard posisi rekening sudah muncul dan terhitung di*

layar komputer. Ini berarti tidak perlu membongkar arsip yang menumpuk di lemari yang memakan waktu sampai setengah jam, sedangkan dengan sistem baru cukup memerlukan waktu kurang dari lima menit saja…." (Muk/APr, 2001)

Bank, sebagai lembaga pembayaran untuk transaksi online, telah memainkan peran penting sejak munculnya perbankan online. Dengan online banking, transaksi antar nasabah tidak perlu bertemu langsung.

Tinjauan Objek Penelitian

Penyalahgunaan teknologi internet dalam transaksi transaksi melalui pencurian rekening bank. Pesatnya perkembangan e-commerce telah memberikan manfaat yang sangat besar bagi nasabah yang dapat dengan mudah melakukan pembayaran melalui e-banking. Namun, perkembangan tersebut memberikan ruang bagi peretas untuk memanfaatkan perkembangan tersebut, yaitu akses ilegal ke situs web komersial.

Peretas adalah upaya memasuki sistem keamanan tertentu secara ilegal untuk mendapatkan informasi dalam jaringan komputer (Alfagih, 2019). Hacker pada awalnya digunakan untuk menggambarkan orang yang mencari pengetahuan tentang sistem komputer hanya demi pengetahuan (Alfagih, 2019). Hacker memiliki dua arti, yang pertama adalah orang yang suka memperbaiki, mengubah, mendesain komputer, atau menemukan hal-hal baru dalam pengoperasian komputer (Rahardjo, 2005) Saat ini, peretas sering menyebut diri mereka peretas sejati. Orang yang tidak berwenang kedua dapat mengakses komputer orang lain. Secara umum, definisi ini dimaksudkan untuk digunakan dalam setiap diskusi tentang kejahatan komputer.

Hacker dibagi menjadi 4 tahapan saat melakukan tindakan, yaitu sebagai berikut:

1) Cari sistem komputer untuk memasukkan (dan mengumpulkan informasi).
2) Menyelinap masuk. Inti dari kegiatan penyusupan ini adalah untuk mengelabui sistem keamanan, biasanya berupa proteksi password.
3) Jelajahi sistem. Begitu seorang peretas sejati memasuki sistem, ia kemungkinan besar akan berpindah-pindah, menelusuri konten sistem yang baru saja ia masuki, dan mencoba berbagai perintah untuk memahami fungsinya.
4) Buat pintu belakang untuk menghilangkan jejak (Artha, 2001)

Peretas harus memiliki keterampilan komputer dasar saat melakukan tindakannya, termasuk:

a. Semacam. Memiliki kemampuan untuk mempelajari bahasa pemrograman komputer.
b. Mampu mencari, mempelajari, dan menjalankan salah satu versi open source Unix.
c. Kemampuan untuk mempelajari dan memahami sistem situs web dengan mengetahui cara menulis bahasa markup hypertext (HTML) (Artha, 2001).

Bentuk- Bentuk Kejahatan Teknologi Informasi

Dilihat dari ciri-ciri komputer tersebut di atas, muncul suatu bentuk komputer baru yaitu computer crime. Ada beberapa kejahatan dalam menggunakan fasilitas komputer ini (Magdalena & Setiyadi, 2007), yaitu :

Memasukkan instruksi yang tidak sah, yaitu seseorang secara tidak sah memasukkan instruksi untuk membuat sistem komputer mentransfer dana dari satu rekening ke rekening lainnya.Perilaku ini dapat dilakukan oleh personel internal atau eksternal bank yang mencoba mengakses sistem komputer tanpa izin.

Data masukan diubah, yaitu data yang secara sah dimasukkan ke komputer sengaja diubah. Cara ini paling sering digunakan karena mudah dilakukan, tetapi sulit dilacak, kecuali diperiksa secara rutin.

Korupsi data terutama terjadi pada data keluaran, misalnya laporan berupa hasil cetakan komputer dirobek, tidak dicetak, atau diubah hasilnya.

Komputer yang digunakan sebagai pembantu kriminal, misalnya seseorang menggunakan komputer untuk mencari akun seseorang yang tidak aktif kemudian menarik dana dari akun tersebut.

Akses tidak sah ke sistem komputer atau yang disebut serangan hacker. Peretasan ini terkait dengan aturan kerahasiaan bank. Tentu saja Anda mengetahui status keuangan nasabah dan catatan lainnya. Sesuai dengan kelaziman

industri perbankan, itu harus dirahasiakan.

Kenyataannya, tidak mudah untuk memahami dengan jelas kejahatan komputer dan cyber seperti dijelaskan di atas, dan kejahatan komputer juga memiliki kualifikasi di berbagai bidang. Seperti :

a. Jenis-jenis kejahatan komputer dan internet berdasarkan jenis aktivtasnya
   1. Unauthorized Acces to Computer System and Service

      Kejahatan yang dilakukan dengan cara secara tidak sah memasuki/menembus suatu sistem jaringan komputer tanpa izin atau tanpa sepengetahuan pemilik sistem jaringan komputer yang dimasukinya (Pandjaitan et al., 2005). Biasanya para penjahat (hacker) melakukan ini dengan tujuan untuk menghancurkan atau mencuri informasi penting dan rahasia. Namun, beberapa orang melakukan ini hanya karena mereka merasa itu adalah tantangan untuk mencoba keterampilan mereka untuk menembus sistem dengan tingkat perlindungan yang tinggi. Dengan perkembangan teknologi Internet, kegiatan kriminal seperti itu menjadi semakin umum.

      Tentu kita tidak akan melupakan masalah Timor Timur, beberapa website pemerintah Indonesia dirusak oleh hacker (Kompas, 11/08/1999). Beberapa waktu lalu, peretas juga berhasil meretas database data pengguna layanan America Online (AOL) yang merupakan perusahaan Amerika yang bergerak di bidang e-commerce dengan kerahasiaan tinggi (Indonesia Observer, 26/06/2000). Situs web FBI tidak kebal terhadap serangan peretas, yang menyebabkan situs web gagal berfungsi secara normal untuk jangka waktu tertentu.
   2. Illegal Contents

      Merupakan kejahatan memasukkan data atau informasi di Internet yang tidak benar, tidak etis dan dapat dianggap ilegal atau mengganggu ketertiban umum. Misalnya memuat berita bohong atau memfitnah orang lain yang merusak martabat atau harga diri orang lain, konten pornografi atau memuat informasi rahasia negara, propaganda melawan pemerintah yang sah, dll.
   3. Data Forgery

      Merupakan kejahatan untuk memalsukan data file penting yang disimpan sebagai file tanpa skrip melalui Internet. Jenis kejahatan ini biasanya menargetkan dokumen e-commerce agar seolah-olah ada "salah ketik" yang pada akhirnya akan menguntungkan pelakunya.
   4. Cyber Espionage

      Merupakan kejahatan menggunakan Internet untuk memasuki sistem jaringan komputer pihak sasaran untuk melakukan kegiatan spionase terhadap orang lain. Kejahatan ini biasanya menargetkan pesaing komersial yang file atau data penting disimpan dalam sistem komputerisasi.
   5. Cyber Sabotage and Extortion

      Kejahatan ini dilakukan dengan menghancurkan, menghancurkan atau menghancurkan data, program komputer atau sistem jaringan komputer yang terhubung ke Internet. Kejahatan semacam ini biasanya dilakukan dengan cara menyusup ke dalam bom logika, virus komputer, atau program tertentu untuk membuat data, program komputer, atau sistem jaringan komputer tidak dapat digunakan, tidak dapat bekerja secara normal, atau beroperasi sesuai kebutuhan.

      Setelah ini terjadi, dalam beberapa kasus, pelaku akan secara aktif memberikan korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang rusak, tentu saja akan dikenakan biaya tertentu. Jenis kejahatan ini sering disebut sebagai cyber terrorism. Cyberterrorism merupakan salah satu bentuk perkembangan teknologi informasi yang sangat pesat, khususnya perkembangan internet. Sangat mudah diprediksi bahwa terorisme harus dilakukan dengan menggunakan program komputer sebagai sarana atau melalui dunia maya (Remy Syahdeini, 2009).

      Operasi cyberterrorism seringkali lebih murah, dan hanya dengan kemampuan yang memadai mereka dapat bertindak cepat dan menghasilkan hasil yang luar biasa. Peretas dapat membobol komputer bank dan

mentransfer dana secara ilegal atau menggunakan kartu kredit orang lain untuk membeli peralatan untuk melakukan aktivitas teroris, melakukan kejahatan pencucian uang, dan merusak sistem komputer. Melalui internet, proses komunikasi, koordinasi dan integrasi, rekrutmen dan promosi antar anggota dapat dilakukan dengan lebih mudah (Mansur & Gultom, 2005).

6. Offense against Intellectual Property

Kejahatan ini ditujukan terhadap kekayaan intelektual yang dimiliki oleh pihak lain di Internet. Misalnya meniru secara tidak sah tampilan situs web milik orang lain di halaman web, menyiarkan informasi di Internet, dan ternyata itu adalah rahasia dagang orang lain, dan sebagainya. Pelanggaran hak kekayaan intelektual, umumnya dikenal sebagai cybersquatting, adalah tindakan spekulan mendaftarkan nama domain sebelum pihak lain (yaitu, pihak yang benar-benar menggunakan nama domain). Tujuannya adalah untuk menipu semua orang yang pasti akan menggunakan nama domain (Mansur & Gultom, 2005).

7. Infringements of Privacy

Kejahatan ini merupakan informasi yang sangat pribadi dan rahasia terhadap seseorang. Kejahatan ini biasanya menargetkan informasi pribadi yang disimpan dalam bentuk data pribadi yang terkomputerisasi.Jika orang lain mengetahui informasi ini, dapat menyebabkan kerugian yang substansial atau tidak berarti bagi korban, seperti nomor kartu kredit, kode PIN ATM, cacat tersembunyi atau penyakit, dll.

8. Cracking

Penggunaan teknologi komputer untuk melakukan kejahatan adalah dengan merusak sistem keamanan suatu sistem komputer, biasanya pencurian. Sering terjadi kesalahpahaman antara hacker dan cracker. Hacker sendiri identik dengan perilaku negatif. Meskipun hacker adalah orang yang suka pemrograman dan percaya bahwa informasi sangat berharga, beberapa informasi dapat dibuat publik dan rahasia. Faktanya, tujuan hacker dan cracker adalah sama, dan tidak ada penilaian positif atau negatif. Pada dasarnya keduanya negatif, karena kita tahu bahwa hacker dan cracker sebagai penjahat adalah sama. Seorang hacker adalah seorang administrator sistem yang membobol sebuah sistem komputer, dan seorang cracker adalah orang yang mencuri, jadi cracking sama dengan hacking (Mansur & Gultom, 2005). Jadi harus jelas bahwa cracking adalah serangan hacking untuk tujuan jahat. Istilah untuk kerupuk adalah kerupuk topi hitam. Berlawanan dengan pembaca kartu kredit yang hanya mengintip kartu kredit, scammers mengintip simpanan nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan mereka sendiri. Bahkan jika mereka telah melanggar keamanan komputer orang lain, peretas lebih memperhatikan proses ini. Dan cookies lebih fokus menikmati hasilnya.

9. Carding

Salah satu gaya hidup global yang berkembang adalah penggunaan kartu kredit. Dengan kartu kredit, semuanya menjadi sederhana, mudah dan cepat. Sekarang tidak perlu lagi membawa uang tunai dalam jumlah besar saat berbelanja atau membeli tiket pesawat, membayar tagihan dan tagihan, dll. Menggesek kartu adalah kejahatan, menggunakan teknologi komputer untuk menggunakan kartu kredit orang lain untuk transaksi, yang dapat menyebabkan kerugian material dan non-materi kepada orang lain.

Carding adalah murni kejahatan transnasional, karena dapat dilakukan oleh siapa saja dari berbagai belahan dunia dan sistem hukum yang berbeda. Carding dilakukan secara online dengan menggunakan internet dan komputer sebagai media penyalahgunaan kartu kredit, dan dengan memalsukan nomor yang sudah ada (Ade Ary Syam Indradi, 2006).

Kartu kredit adalah cara hidup, bagian dari komunitas manusia, dan tergolong modern dalam cara hidup di kota metropolitan atau kota internasional. Namun, keberadaan kartu kredit seringkali disalahgunakan. Menurut Johannes Ibrahim (Ibrahim, 2004), Hal ini dapat dilihat dari dua (dua) aspek. Salah satunya adalah melihat wanprestasi dalam lingkup hukum kontrak dari perspektif hukum perdata.

Misalnya, menggunakan kartu kredit tanpa hak, bukan seperti biasa. Kedua, dari perspektif hukum pidana, bentuk pidana penggunaan kartu kredit disebut credit card fraud atau penipuan kartu kredit. Swiping adalah penggunaan kartu kredit melalui internet untuk menyalahgunakan kartu kredit.Swiping adalah ternary yang biasa digunakan oleh hacker dan digunakan untuk kegiatan yang berhubungan dengan penipuan penggunaan kartu kredit. Menurut Thom Mrozek, combing adalah ternary yang digunakan oleh hacker untuk menggambarkan penggunaan informasi kartu kredit curian untuk membeli barang dan jasa (Ade Ary Sam Indradi, 2006).

Jenis kejahatan ini, dari sudut pandang sasaran kejahatan, mencakup bentuk kejahatan dunia maya yang menargetkan properti dan jenis kejahatan dunia maya yang menargetkan properti pribadi. Pada saat yang sama, dilihat dari modus operandi, itu adalah kejahatan komputer yang menargetkan properti pribadi. Sedangkan dari modus operandinya tergolong computer-assisted crime, yaitu modus kejahatan umum yang menggunakan komputer dalam perilakunya.

10. Defacing

Defacing adalah kegiatan mengubah Halaman/web parpol lain, seperti yang terjadi belakangan ini di website Menkominfo dan Partai Golkar, NI, dan website KPU pada Pemilu 2004. Ada yang murni untuk bersenang-senang, memamerkan keahlian mereka dan memamerkan kemampuan mereka untuk membuat program, tetapi ada juga yang jahat mencuri data dan menjualnya kepada orang lain.

11. Phising atau Identity theft

Phishing adalah kegiatan yang membujuk pengguna komputer (users) di Internet untuk memberikan informasi tentang data pribadi pengguna (user name) dan kata sandi (password) di situs web yang telah dirusak. Phishing biasanya berlaku untuk pengguna online banking. Bidang data penting pengguna dan kata sandi yang telah dikirimkan pada akhirnya akan menjadi milik penjahat dan digunakan untuk melakukan pembelian menggunakan kartu kredit atau rekening bank korban.

Phishing biasanya dilakukan dengan mengirimkan email palsu berupa logo yang menarik perhatian penerima email. Secara umum, phishing dilakukan melalui email, tetapi ada juga yang dilakukan melalui pesan teks ponsel. Meskipun banyak dari email palsu ini terlihat meyakinkan (seperti aslinya), yaitu dengan logo perusahaan dan menampilkan tautan ke situs web yang salah, banyak dari mereka terlihat sangat konyol karena dibuat oleh amatir (Ketimbang profesional). Hal ini terlihat pada format yang berantakan, kesalahan tata bahasa dalam kalimat tertulis, dan kesalahan ejaan pada kata-kata yang biasa digunakan atau digunakan bersama (Remy Syahdeini, 2009).

12. Spamming

Spam adalah mengirimkan berita atau iklan yang tidak diinginkan melalui email (email). Spam sering disebut sebagai email massal atau spam, atau "spam". Namun, banyak orang yang terkena dampak dan menjadi korban. Yang paling umum adalah mengirim email untuk mendapatkan hadiah, tiket lotre, atau orang yang mengaku memiliki rekening bank di Afrika atau Timur Tengah, meminta bantuan netizen untuk mencairkannya, dan berjanji untuk berbagi keuntungan. Korban kemudian diminta untuk memberikan nomor. Menurut laporan, kepala sebuah universitas swasta di Indonesia ditipu hingga Rp1.000.000.000 (Rp1 miliar) karena mengirim spam. Akun dan kirim uang / dana sebagai phisher, tentu saja dolar AS, tidak ada kabar darinya baru-baru ini.

13. Malware

Malware adalah program komputer yang cari kelemahan dalam perangkat lunak. Umumnya, malware dibuat untuk menyerang atau merusak perangkat lunak atau sistem operasi. Malware mencakup berbagai jenis, yaitu: virus, worm, Trojan horse, adware, pembajak peramban, dll. Di pasar toko peralatan komputer dan perangkat lunak, Anda dapat menggunakan perangkat lunak anti-spam dan anti-virus dan anti-malware. Namun, bagi mereka yang tidak tahu, akan selalu ada orang yang terkena. Karena pembuat virus dan malware biasanya masih

kreatif dan produktif dalam membuat program untuk para korban prank.

14. Cyber-Child Pornography

Pornografi anak atau pornografi anak mengacu pada materi pornografi (cabul) yang menampilkan anak-anak. Sebagian besar negara menyebutnya sebagai bentuk pelecehan seksual terhadap anak dan itu ilegal. Di sebagian besar negara/kawasan, undang-undang secara otomatis melarang penggunaan foto untuk menunjukkan partisipasi anak dalam aktivitas seksual dan pembuatan materi ini sebagai pornografi anak untuk pelecehan seksual anak (Remy Syahdeini, 2009)

.

Kasus Kejahatan Komputer

Terdapat beberapa kasus kejahatan yang komputer yang telah diajukan kepengadilan. Adapun kasus-kasus tersebut adalah sebagai berikut (Suparni, 2009) :

Putusan Mahkamah Agung No. 363 K/Pid/1984 tanggal 25 Juni 1984 tentang penggelapan dana bank melalui komputer. Dari tanggal 15 September sampai 12 Desember 1982, tindak pidana ini adalah orang luar bekerja sama dengan Brigjen Katamso, pegawai tidak sah cabang "Belt and Road", antara tanggal 15 September sampai 12 Desember 1982 yaitu Tanpa disadari pegawai illegal melalui "Belt and Road" mentransfer dana ke rekening orang lain melalui likuidasi. Lainnya, bukan rekening yang tertulis pada laporan pelunasan melalui posting komputer tanpa kartu atau kwitansi mesin.

Perilaku tersebut dilakukan sebanyak 44 kali, dan jumlah Rp815.000.000 (Rp815 juta) dan Rp10.000.000 (Rp10 juta) tercapai melalui verifikasi tunai, dan kartu nasabah Ibu tidak diganti. Karina. Dalam sengketa tersebut, Pengadilan Negeri Yogyakarta mengambil keputusan No. 33/1983/Pid/PN tanggal 20 September 1983, terdakwa divonis korupsi, divonis 10 tahun penjara, dipotong hukumannya, dan harus membayar biaya perkara sebesar Rp100.000 (Rp100.000).

Putusan tersebut diperoleh Pengadilan Tinggi Yogyakarta No. 41/1983/Pid/PTY, tanggal 6 Maret 1984, dan nomor putusan Mahkamah Agung. Surat No. 363/K/Pid/1984 tanggal 25 Juni 1984 menolak permohonan kasasi yang diajukan jaksa karena hak untuk mengajukan kasasi telah habis karena tidak ada memori kasasi.

Dasar hukum penuntutan adalah Pasal 55(1). Pasal 64 (1) KUHP. Pasal 1 (1) Huruf a Undang-Undang Nomor 3 Tahun 1971 tentang Pemberantasan Tindak Pidana Korupsi pada hakikatnya dilakukan oleh terdakwa dan pegawai "Belt and Road" tidak etis dan merugikan negara.

Kasus pemindahbukuan kredit palsu melalui komputer BDN Jakarta Cabang Bintaro-Jaya dilakukan oleh Terdakwa dengan menyiapkan beberapa rekening untuk menampung mutasi tanpa tagihan (fiktif); dengan menggunakan rekening orang lain (dengan persetujuan nasabah) atau aktivasi Rekening tidak aktif dari 20 Juli 1988 hingga Januari 1989.

Setelah rekening tersebut tersedia, selanjutnya terdakwa menyetorkan virtual deposit ke rekening tersebut, yang mencapai Rp 1.525.132.300. Terdakwa kemudian mentransfer dari rekening tersebut ke beberapa rekening yang telah disiapkan sebelumnya oleh bank lain (Bank Duta Barito Plaza, Bank Umum Nasional Cabang Kemayoran, Bank Exim Indonesia Cabang Kemayoran, dan orang yang memberikan rekening untuk rencana tersebut).

Yang menarik adalah catatan Andi Hamzah (Suparni, 2009), Susunan surat dakwaan sebaliknya, yaitu dakwaan pokok sesuai dengan Pasal 1 ayat (1) b Undang-Undang Nomor 3 Tahun 1971, dan surat dakwaan tambahan dalam Pasal 1 (1) a. Meskipun kedua alinea tersebut mengandung ancaman pidana yang sama (Pasal 28), sub a lebih sulit dibuktikan. Menarik juga bahwa Pengadilan Negeri Jakarta sedang mempertimbangkan penggunaan Pasal 362 (Pencurian) KUHP, terutama pada tahap pengambilan (kartu nasabah, dokumen jurnal debet dan kredit fiktif, salinan giro, floppy disk/ komputer floppy disk)). Sulit dibuktikan dan dimintai keterangan, tetapi perilaku terdakwa akhirnya ditentukan sebagai tindak pidana pencurian.

Kasus pemalsuan/pencurian di Bank Danamon Pusat pada tahun 1998 melibatkan terdakwa BH dan KH sehingga mengakibatkan kerugian sebesar 372.100.000- (3,721 miliar rupiah).

Prosesnya dimulai dengan pembukaan

rekening dengan alamat dan nama palsu di Cabang Utama Bank Danamon, dan KH yang bekerja di ruang rekonsiliasi cabang akan membantunya. KH diam-diam mempelajari pengoperasian komputer setelah mengetahuinya.KH menggunakan komputer di kantor dan menggunakan nama pengguna dan kata sandi tertentu untuk mentransfer uang dari berbagai rekening prabayar oleh kantor pusat. Kemudian, dari sini, masukkan rekening yang dibuka oleh BH di cabang utama Bank Danamon

JPU menuntut BH bersalah karena memalsukan Pasal 264 ayat 2 KUHP. Putusan Pengadilan Negeri Jakarta Pusat No. 5 68/Pid/B/1991/PN, tanggal 20 Agustus 1991, memvonis BH 18 (delapan belas) bulan penjara, dikurangi masa penahanan dan biaya perkara sebesar 2.500 rupee,-

Selain itu, ada kasus uang Tabanas dari BRI Jatinegara Timur pada tahun 1991. Modus operandinya adalah menyalahgunakan rekening tabanas pasif dengan mengubah nama nasabah dan memasukkan saldo yang sebenarnya tidak ada. Kemudian mengisi buku tabanas yang kosong tanpa sepengetahuan teller, bekerjasama dengan pihak lain dan menggunakan password teller, kemudian transfer tabungan.

Dapat dilihat dari uraian kasus-kasus di atas bahwa tindak pidana pada dasarnya dilakukan dengan cara atau melalui komputer, perangkat telekomunikasi dan informasi, baik berupa perangkat keras maupun perangkat lunak.

Secara umum barang bukti yang disita polisi sehubungan dengan pembobolan ini antara lain mesin EDC, oil skimmer, kamera, laptop, kartu kredit dan kartu ATM, KTP, tagihan, card changer, dan data yang berisi catatan password. baterai, limbah cair, tangan, paspor, dan beberapa kendaraan sewaan.

Pencurian Uang Pada Rekening Bank Dengan Media Internet

Tindak Pidana Pencurian Uang Pada Reken Penggunaan Bank Media Internet sesuai dengan ketentuan Pasal 362 KUHP Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik

Selama ini penyalahgunaan komputer di Indonesia hanya dijerat dengan ketentuan hukum pidana, yaitu Pasal 362 tentang pencurian, Pasal 378 tentang penggelapan dana publik, dan Pasal 263 tentang pemalsuan. Namun dengan berkembangnya zaman, tentunya kualitas kegiatan kriminal dengan menggunakan komputer sebagai sarana atau alat juga semakin meningkat, dan diperlukan aturan khusus untuk meredam ancaman penyalahgunaan komputer.

Tujuan dari penyusunan aturan internet adalah untuk memberikan kepastian hukum kepada pengguna internet dan mengurangi dampak negatif dari pesatnya perkembangan internet, salah satunya untuk menghindari para hacker yang sering menyalahgunakan komputer.

Indonesia sebenarnya memiliki beberapa undang-undang yang sementara menangani cracker, seperti Pasal 362 KUHP dan Undang-Undang Nomor 12 Tahun 1997 tentang Hak Cipta, serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan-peraturan perundang-undangan tersebut dapat dijelaskan sebagai berikut:

Pasal 362 KUHP

Dari Pasal 362 tersebut dapat ditarik unsur-unsur baik unsur obyektif maupun unsur subyektif yang antara lain sebagai berikut:

1. Unsur obyektif
2. Perbuatan mengambil

Perbuatan mengambil dalam hal ini telah Dari perspektif kualitas tindakan, mengalami perkembangan. Menurut Adami, pengambilan adalah suatu perilaku atau tindakan material yang positif, biasanya dilakukan dengan menggunakan gerakan otot sadar jari dan tangan, kemudian mengarahkan jari dan jemari tersebut ke suatu benda, menyentuhnya, memegangnya dan mengangkatnya, kemudian membawa. itu dan memindahkannya ke tempat lain atau memasukkan kekuatannya.

Namun, konsep yang dianut oleh penulis telah mengalami perkembangan yang berbeda. Pasalnya, perilaku meretas situs web berbeda dengan perilaku mencuri tradisional. Kunci untuk menerima pencurian tradisional adalah tindakan aktif terhadap objek, dan jari-jari dan tangan pelaku harus bersentuhan langsung. Hal ini berbeda dengan pencurian melalui website, karena pelaku tidak terkait secara aktif dengan barang tersebut, tetapi terkait

dengan komputer yang terhubung ke jaringan internet di rumah atau dengan menyewa tempat yang menyediakan layanan jaringan internet.

Penulis berpendapat bahwa penggunaan jari-jari tersebut oleh pelaku di atas, khususnya komputer, adalah untuk mengalihkan seluruh atau sebagian barang milik orang lain kepada kekuasaan, yang dapat dikatakan sebagai tindakan perampasan. Perbuatan mengambil juga berkaitan dengan tindak pidana dalam hukum pidana. Moeljatno mengemukakan bahwa unsur-unsur tindak pidana adalah sebagai berikut:

Adanya perbuatan

1. Memenuhi rumusan Undang-Undang
2. Bersifat melawan hukum

Melengkapi perumusan RUU merupakan syarat formal. Persyaratan ini didasarkan pada asas legalitas. Pelanggaran adalah persyaratan materi. Hal ini diperlukan karena masyarakat harus benar-benar mempertimbangkan perilaku yang dilakukan sebagai sesuatu yang tidak boleh dilakukan. Pelanggaran hukum merupakan syarat mutlak terjadinya kejahatan.

Jika mengacu pada unsur-unsur tindak pidana yang dijelaskan oleh Moeljatno, maka unsur-unsur pencurian melalui fasilitas internet adalah:

1. Adanya perbuatan
2. Memenuhi rumusan Undang-Undang
3. Bersifat melawan hukum
4. Penulis menyimpulkan bahwa perbuatan mengambil oleh pelaku telah memenuhi unsur yang terdapat pada pasal 362.

Obyeknya suatu benda

Menurut MvT, objek mengakui bahwa pembentukan Pasal 362 KUHP terbatas pada benda bergerak (roerend goed) dan benda berwujud (stoffelijk goed). Benda tidak bergerak hanya dapat menjadi benda curian jika dipisahkan dari benda tetap dan menjadi benda bergerak, seperti pohon yang ditebang atau daun pintu yang dicabut. Objek didefinisikan sebagai objek nyata dan objek bergerak konsisten dengan unsur-unsur perilaku akuisisi. Benda yang dapat memancarkan daya secara mutlak dan jelas adalah benda yang aktif dan berwujud. Dalam prakteknya, dengan membobol sebuah website, objek dari tindakan tersebut adalah rekening bank seseorang. Ketika Hamzah mengatakan listrik adalah komoditas:

1. Listrik itu tidak dapat dipisah secara tersendiri
2. Energi listrik dapat diangkut dan dikumpulkan

Energi listrik mempunyai nilai karena Membangkitkan energi membutuhkan uang dan energi, dan dapat digunakan sendiri atau untuk digunakan orang lain.

Menurut pengertian di atas, objek pada perangkat komputer adalah data atau program yang disimpan pada media penyimpanan floppy disk atau sejenisnya. Bentuk data atau program yang disimpan pada floppy disk atau sejenisnya tidak diketahui, tetapi data atau program tersebut dapat berwujud dengan ditampilkan pada layar atau layar komputer (monitor), dan juga dapat diwujudkan pada printer atau printer di bentuk tertulis dengan mencetak. . Data atau program yang disimpan dalam floppy disk dll juga memiliki nilai ekonomis karena bermanfaat bagi orang yang menggunakannya. Oleh karena itu, data/program komputer yang disimpan dalam media penyimpan disket dan lain-lain dapat digolongkan sebagai objek sebagaimana dimaksud dalam Pasal 362 KUHP.

Dari pengertian pengertian objek yang dikembangkan ini, menurut penulis, objek adalah benda berwujud atau tidak berwujud yang memiliki nilai ekonomis, termasuk rekening nasabah bank di website internet.

Unsur keadaan yang menyertai atau melekat pada suatu benda, yaitu benda itu sebagian atau seluruhnya dimiliki oleh orang lain.

Seperti yang dikatakan Chazawi, barang-barang tersebut tidak perlu sepenuhnya dimiliki oleh orang lain, hanya sebagian saja, dan sebagian dari barang milik pelaku dan barang-barang yang dapat dijadikan objek pencurian haruslah barang-barang dengan ciri-ciri sebagai Tuan mereka.

Unsur ini juga terpenuhi oleh pelaku dalam pencurian rekening seseorang melalui pembobolan web-site internet.

1. Unsur subyektif
   a. Maksud untuk memiliki

      Ada dua unsur dalam hal ini, yaitu kesengajaan sebagai kesengajaan

dan penguasaan pelaku terhadap objek perbuatan yang telah dilakukan atau yang dapat dikatakan sebagai kesengajaan dari perbuatan tersebut. Memiliki milik orang lain berarti mengambilnya.

b. Melawan hukum

Pengertian melawan hukum ada dua aliran yaitu menurut aliran melawan hukum formil adalah suatu perbuatan itu bersifat melawan hukum apabila perbuatan diancam pidana dan dirumuskan sebagai suatu tindak pidana dalam UU, sedang sifat melawan hukum itu dapat dihapus hanya berdasarkan suatu ketentuan UU. Menurut aliran materiil berpendapat suatu perbuatan bersifat melawan hukum bukan hanya karena bertentangan dengan Undang-Undang, akan tetapi juga bertentangan dengan hukum tidak tertulis, atau norma-norma yang hidup di masyarakat, hapusnya sifat melawan hukum berdasarkan ketentuan UU dapat pula berdasarkan aturan-aturan tidak tertulis.

Perbuatan Doddy yang tanpa hak mengambil rekening bank milik Wong Sin dengan cara membobol data base web-site tersebut dapat dikatakan melawan hukum sehingga unsur subyektif melawan hukum sudah terpenuhi.

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Pasal 362 KUHP tentang tindak pidana pencurian dipersamakan dengan perbuatan seseorang yang menggunakan komputer secara tidak sah, tanpa izin atau menggunakannya melampaui wewenang yang diberikan, disebut juga dengan Joy Computing.

Dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Joy Computing diatur dalam Pasal 30, Pasal 46, dan Pasal 52.

Pasal 30 ayat (1), ayat (2), dan ayat (3):

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses kompuer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun."

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektonik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik."

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

Pasal 46 ayat (1), ayat (2). Dan ayat (3)

"Setiap orang yang memenuhi unsur sebagaimana dimaksud Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paing banyak Rp 600.000.000,- (enam ratus juta rupiah)."

"Setiap orang yang memenuhi unsur sebagaimana dimaksud Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 2 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,-n(tujuh tatus juta ruiah)."

"Setiap orang yang memnuhi unsur sebagaimana dimaksud Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,- (delapan ratus juta rupiah)."

Pasal 52 ayat (2) dan ayat (3):

"Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga."

"Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak

terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pokok masing-masing pasal ditambah duapertiga."

Terdapat 19 bentuk tindak pidana dalam Pasal 27 sampai 37 UU ITE. Diantara 19 macam tindak pidana ITE tersebut, seperti halnya dengan pembobolan bank via ATM, kiranya yang dekat dengan peristiwa pencurian uang melalui rekening bank dengan sarana internet yakni :

Pasal 30 Ayat (3) jo. 36 jo. 46 ayat (3):

Pasal 30 Ayat (3) jo 36 merumuskan: *"…dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan, yang mengakibatkan kerugian bagi orang lain".*

Perbuatan dalam wujud apa dan caranya yang belum diketahui yang dilakukan pembobol tersebut dapat dikualifikasikan (disamakan) dengan perbuatan mengakses ….. dengan "menjebol" sistem pengaman. Perbuatan seperti itu berakibat kerugian bagi orang lain. Mengenai kerugian orang lain merupakan unsur yang harus ditambahkan pada delik ITE yang dirumuskan dalam Pasal 30 Ayat (3). Unsur kerugian ini terdapat dalam Pasal 36. Semua delik yang dirumuskan dalam Pasal 27 sampai 34 tersebut, baru dapat menjadi tindak pidana ITE bila terdapat unsur kerugian orang lain dalam Pasal 36 ini.

Pasal 33 jo. 36 jo. 49

Pasal 33 jo 36 merumuskan:

"… dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya, yang mengakibatkan kerugian bagi orang lain".

Memenuhi syarat Pasal 33 saja tidak cukup untuk merupakan tindak pidana ITE, dan syarat menimbulkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 36 harus ditambah. Perilaku yang menyebabkan sistem elektronik tidak berfungsi dengan baik.

Pembuktian Dalam Tindak Pidana Pencurian Uang Pada Rekening Bank Dengan Media Internet Melalui Teknologi Informasi

Pembuktian Menurut UU ITE

Undang-Undang ITE mengatur bahwa informasi elektronik/arsip elektronik dan/atau salinan cetaknya adalah alat bukti hukum yang sah, yang merupakan perpanjangan dari alat bukti hukum yang diatur dalam hukum acara Indonesia saat ini.

Menurut undang-undang ITE, dokumen elektronik mengacu pada setiap informasi elektronik yang dibuat, diteruskan, dikirim, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optik, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar oleh komputer atau sistem. elektronik dengan cara sebagai berikut Produk, termasuk tetapi tidak terbatas pada kata-kata, suara, gambar, peta, desain, foto, dll., huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki arti atau makna atau dapat dipahami oleh orang yang bisa memahami mereka. Yang dimaksud dengan informasi elektronik adalah satu atau sekelompok data elektronik, termasuk namun tidak terbatas pada teks, suara, gambar, peta, desain, foto, electronic data interchange (EDI), surat elektronik (email), telegram, teleks, teleks atau Huruf, tanda, angka, kode akses, simbol, atau perforasi yang diproses dengan analog memiliki arti atau dapat dipahami oleh orang yang dapat memahaminya.

Penggunaan alat bukti elektronik untuk melegalkan penggunaan media online untuk mengungkap pasal pidana antara lain:

Pasal 44 yang berbunyi :

1. Alat bukti penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut :
2. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan;
3. Alat bukti lain berupa Informasi Elektronik sebagaimana dimaksud dalam Pasal 1 angka

1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Selanjutnya Pasal 1 angka 1, yang berbunyi:

> *"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 (electronic mail), telegram, teleks, telecopy atau sejenis huruf, tanda, angka, Kode Akses, symbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya."*

Selanjutnya Pasal 1 angka 4, yang berbunyi:

> *"Dokumen Elektronik adalah setiap informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam benuk analog, digital, elektromagnetik, optilkal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, symbol atau perforasi yang memiliki makna atau arti atau dapat dipah*ami oleh orang yang mampu memahaminya."

Selanjutnya Pasal 5, yang berbunyi :

> *"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya meupakan alat bukti hukum yang sah."*
>
> *"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."*
>
> *"Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketntuan yang diatur dalam Undang-Undang ini."*

Pasal-pasal diatas dianggap telah Memberikan pedoman bagi penyidik untuk mengumpulkan barang bukti elektronik untuk mengungkap pelaku kejahatan internet, khususnya penggunaan internet untuk mencuri dana melalui rekening bank.

Alat bukti elektronik ini biasanya digunakan untuk melengkapi alat bukti yang ditentukan dalam alinea pertama Pasal 184 KUHAP, di antaranya alat bukti yang sah dapat digunakan sebagai alat bukti:

1. Keterangan Saksi
2. Keterangan Ahli
3. Surat
4. Petunjuk
5. Keterangan Terdakwa

Sistem Pembuktian

Pada hakikatnya pembuktian dimulai dengan adanya peristiwa hukum. Apabila terdapat unsur pidana (bukti permulaan telah terjadi suatu tindak pidana), maka dari proses tersebut akan dilakukan penyidikan (serangkaian tindakan yang dilakukan penyidik untuk menemukan dan menemukan dugaan tindak pidana). Menentukan apakah penyidikan dapat dilakukan menurut cara yang ditentukan undang-undang)), dan dalam butir 13 Pasal 1 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian, penyidikan merupakan rangkaian tindakan penyidikan. Dan menurut cara yang ditentukan dalam undang-undang ini, mencari dan mengumpulkan bukti yang cukup untuk membuktikan perilaku kriminal, apa yang terjadi, dan bukti untuk melacak tersangka kriminal. Menurut M. Yahya Harahap, alat bukti adalah klausul yang memuat garis-garis besar dan pedoman, serta isinya berkaitan dengan cara hukum membuktikan kesalahan terdakwa.

Dalam sistem pembuktian terdapat macam-macam sistem atau teori pembuktian. Sistem atau teori pembuktian tersebut adalah :

Pembuktian Berdasarkan Keyakinan Hakim Belaka (*Conviction in time)*

Sistem pembuktian subjektif yang hanya menentukan bersalah atau tidaknya terdakwa berdasarkan keyakinan hakim. Keputusan hakim tidak didasarkan pada alat bukti yang diberikan oleh undang-undang, hakim hanya mengandalkan hati nuraninya. Hakim dapat memperoleh dan menarik suatu keyakinan bagi hakim dari alat bukti yang diperiksanya dalam persidangan. Hakim juga

dapat mengabaikan hasil pemeriksaan alat bukti dan segera mencabut keyakinannya dari keterangan atau pengakuan terdakwa. Sistem ini seolah-olah menyerahkan nasib terdakwa pada keyakinan penuh hakim. Menurut Yahya Harahap, keyakinan hakim menentukan bentuk kebenaran dalam sistem pembuktian ini.

Sitem Pembuktian Berdasarkan Undang-Undang Secara Positif (Positief Wettelijk Bewijstheorie)

Sistem pembuktian yang dikembangkan pada Abad Pertengahan untuk menentukan bersalah atau tidaknya seorang terdakwa harus mengikuti prinsip pembuktian yang ditetapkan oleh undang-undang. Sistem ini kontras dengan hukuman waktu, di mana hukuman hakim dikecualikan. Menurut sistem ini, undang-undang menetapkan jenis alat bukti yang dapat digunakan hakim. Bukti apa yang bisa digunakan hakim? Jika alat bukti itu telah digunakan secara sah menurut undang-undang, hakim harus menentukan status keabsahan alat bukti itu, sekalipun hakim dengan jelas meyakini bahwa isi yang harus dibuktikan itu tidak benar.

Dalam pandangan D. Simmon, sistem ini berusaha menghilangkan semua penilaian subjektif hakim dan membatasi hakim dengan aturan pembuktian yang ketat, sistem ini disebut juga teori pembuktian formal.

Sistem pembuktian berdasarkan keyakinan hakim pada alasan logis (La Conviction Raisonnee)

Menurut sistem pembuktian ini, seorang hakim dapat menilai seseorang bersalah berdasarkan keyakinan seseorang, dan keyakinan ini didasarkan pada bukti dan disertai dengan alasan yang logis. Dengan kata lain, hakim hanya dapat menghukum terdakwa jika terdakwa yakin bahwa pernyataan itu terbukti benar, dan keyakinan ini harus disertai dengan alasan untuk meyakini bahwa terdakwa bersalah. Sistem atau teori pembuktian ini disebut juga dengan pembuktian bebas, karena hakim dapat dengan bebas menyatakan alasan keyakinannya.

Sistem Pembuktian Hukum Negatif (Negatief Wettelijk Bewijstheorie)

Sistem pembuktian bergantung pada keputusan hakim apakah terdakwa salah, dan terikat oleh alat bukti yang ditentukan oleh undang-undang dan keyakinan hakim itu sendiri. Dalam sistem ini, ada dua prasyarat untuk membuktikan kesalahan terdakwa, yaitu alat bukti yang sah yang telah diterapkan dan keyakinan hakim bahwa terdakwa bersalah berdasarkan alat bukti.

KESIMPULAN

Berdasarkan dari hasil pembahasan dapat disimpulkan bahwa Tindak pidana pencurian uang pada rekening bank dengan media internet dipandang dari Pasal 362 KUHP Jo Undang-Undang RI Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik Bahwa perundang - undangan yang terkait dengan pencurian uang di Bank dengan menggunakan media Internet di Indonesia sesungguhnya telah memiliki sejumlah perundangan dalam menghadapi para *craker*, misalnya, Pasal 362 KUHP, dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pembuktian dalam tindak pidana pencurian uang pada rekening bank dengan media internet melalui teknologi informasi, bahwasannya alat-alat bukti elektronik tersebut digunakan untuk melengkapi alat-alat bukti yang sebelumnya diatur dalam Pasal 184 ayat (1) KUHAP, dimana diantara alat bukti yang sah dan boleh dipergunakan dalam pembuktian adalah keterangan saksi, keterangan ahli, surat, petunjuk, keterangan terdakwa.

REFERENSI

Alfagih, M. A. (2019). *Jaringan Komputer*.

Andi, H. (2001). Apa dan Bagaimana E-Commerce. *Semarang, Penerbit Wahana Komputer*.

Artha, G. (2001). *Hacker Sisi Lain Legenda Komputer*. Medikom.

Bainbridge, D. I. (2004). *Introduction to computer law*. Pearson Education.

Hamzah, A. (2004). *Asas-asas Hukum Pidana, Rineka Cipta*. Jakarta.

Ibrahim, J. (2004). *Kartu kredit: dilematis antara kontrak dan kejahatan*. Refika Aditama.

Indradi, Ade Ary Sam. (2006). Carding. *Penerbit Pensil-324, Jakarta*.

Indradi, Ade Ary Syam. (2006). *Carding: modus operandi, penyidikan, dan penindakan*. PTIK.

Magdalena, M., & Setiyadi, M. R. (2007). *Cyberlaw, tidak perlu takut*.

Mansur, D. ., & Gultom, A. (2005). *Cyber law – Aspek Hukum Teknologi Informasi*. Refika Aditama.

Moch, H. A. K. (1979). Anwar, hukum pidana bagian khusus (KUHP buku II). *Alumni, Bandung*.

Muk/APr. (2001). *Lemahnya Ketentuan Internet Banking Masih Dipertanyakan*. Hukumonline.com. https://www.hukumonline.com/berita/baca/hol4047/lemahnya-ketentuan-iinternet-bankingi-masih-dipertanyakan

Pandjaitan, H. I. P., Pranoto, H., Siregar, M. D. A., & Fahmi, I. (2005). *Membangun Cyber Law Indonesia yang Demokratis*. Jakarta: IMLPC.

Partodihardjo, S. (2009). Tanya Jawab Sekitar Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *PT Gramedia Pustaka Utama: Jakarta*.

Prodjodikoro, W. (2003). Asas-asas Hukum Pidana. *Bandung: Refika Aditama*.

Rahardjo, B. (2005). Keamanan sistem informasi berbasis internet. *Bandung: PT. Insan Indonesia*.

Remy Syahdeini, S. (2009). Kejahatan & Tindak Pidana Komputer. *PT Pustaka Utama Grafiti. Jakarta*.

Soekanto, S. (1977). Kesadaran hukum dan kepatuhan hukum. *Jurnal Hukum & Pembangunan*, *7*(6), 462–470.

Suparni, N. (2009). *Cyberspace: problematika & antisipasi pengaturannya*. Sinar Grafika.

Van Apeldoorn, L. (1996). Pengantar Ilmu Hukum, PT. *Pradnya Paramita, Cetakan Kedupuluhenam, Terjemahan: Mr. Oetarid Sadino, Jakarta*.

Wahid, A. (2005). *Kejahatan Mayantara (cyber crime)*.

Yuswandi, A. (1995). *Penuntutan hapusnya kewenangan menuntut dan menjalankan pidana*. Pedoman Ilmu Jaya.