BAB IV

HASIL PENELITIAN DAN ANALISIS

A. Modus Tindak Pidana *Cyber Crime* (Kejahatan Siber) pada Internet Banking

Perbankan nasional saat ini mulai mengembangkan layanan menggunakan digital. Misalnya saja PT Bank Central Asia Tbk (BCA) dan PT Bank Mandiri Tbk (BMRI) yang masing-masing transaksi nasabahnya mayoritas sudah melalui internet banking. Di BCA 8% transaksinya melaui cabang, sisanya *e-channel* yang dimiliki, sedangkan Bank Mandiri penggunaan transaksi 6,8% cabang sisanya digital banking.[113]

Tentunya dengan perkembangan pesat di internet banking perlu diimbangi oleh kewaspadaan adanya potensi kejahatan teknologi dan informasi atau *cyber crime*. Transaksi yang dilakukan, baik melalui sms, internet dan sebagainya harus diimbangi dengan keamanan dan pelayanan *channel*. Potensi *cyber crime* terus mengancam karena transaksi internet banking terus meningkat. Kerahasiaan dan keamanan data tanggungjawab semua pihak tidak hanya bank. Tentu saja menjadi suatu peringatan agar semua pihak turut memikirkan potensi kejahatan siber yang mungkin menimpa pengguna internet banking. Bank dan nasabah harus proaktif untuk mencegah terjadinya kejahatan yang memanfaatkan kemajuan di internet

---

[113] http://ictwatch.com/internetsehat/2014/06/06/internet-banking-indonesia-dibayangi-serangan-cyber/, diakses tanggal 5 Februari 2015 (19.21)

banking. Demikian juga bagi pihak bank untuk proaktif melindungi nasabahnya dengan meningkatkan keamanan situs mereka.[114]

Bank adalah bagian dari sistem keuangan suatu negara. Bank merupakan suatu lembaga keuangan yang eksistensinya tergantung mutlak pada kepercayaan nasabahnya. Pesatnya perkembangan teknologi informasi juga berimbas pada bergesernya sistem pelayanan bank. Saat ini dalam melakukan kegiatan usaha atau memberikan layanan kepada nasabah, bank tidak saja menggunakan model-model konvensional *face to face* dan didasarkan pada *paper document*, tetapi bank juga menggunakan model layanan dengan model *non face to face* dan *paperless document* atau *digital document*. Salah satu sistem layanan berbasis teknologi yang terkenal dalam dunia perbankan saat ini adalah layanan internet banking. Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global.[115]

Disediakannya fasilitas layanan internet banking nasabah mendapat keuntungan berupa fleksibilitas untuk melakukan kegiatannya setiap saat. Nasabah juga dapat mengakses layanan internet melalui personal komputer, ponsel atau media wireless lainnya. Disatu sisi internet banking memiliki banyak manfaat positif, namun disisi lain transaksi internet banking juga berpotensi mengalami kegagalan atau menjadi objek kejahatan elektronik.[116]

Inovasi perbankan berbasis teknologi informasi di industri perbankan dewasa ini memberikan dampak efisiensi dan efektivitas yang luar biasa. Salah

---

[114] *Ibid*
[115] *Ibid*
[116] https://yudicare.wordpress.com/2011/03/28/tanggungjawab-bank-terhadap-potensi-risiko-kegagalan-sistem-danatau-risiko-kejahatan-elektronik-cybercrime-pada-internet-banking/, diakses tanggal 5 Februari 2015 (19.25)

satu bentuk layanan perbankan berbasis teknologi informasi adalah layanan internet banking. Pemanfaatan teknologi informasi bagi industri perbankan dalam inovasi produk jasa bank juga dibayang-bayangi oleh potensi risiko kegagalan sistem dan/atau risiko *cyber crime* yang dilakukan oleh orang-orang yang tidak bertanggungjawab. Kegagalan sistem dapat disebabkan karena adanya kerusakan sistem (seperti misalnya server *down*), dan dalam skala luas bisa disebabkan karena adanya bencana alam.[117]

Berdasarkan data Bank Indonesia (*http://bi.go.id*), terdapat peningkatan yang signifikan terkait penipuan E-Banking dalam 2 tahun terakhir. Pada tahun 2006 terdapat volume laporan 57,766 dengan nilai Rp. 36.500.000.000.000,- (tiga puluh enam triliun lima ratus milyar rupiah), sedangkan pada tahun 2007 terdapat volume laporan 532.533 dengan nilai Rp. 45.700.000.000.000,- (empat puluh lima triliun tujuh ratus milyar rupiah).[118]

Berdasarkan Surat Edaran Bank Indonesia No. 6/18/DPNP, tanggal 20 April tahun 2004, yang dimaksud dengan internet banking adalah salah satu pelayanan jasa bank yang memungkinkan nasabah untuk memperoleh informasi, melakukan komunikasi dan melakukan transaksi perbankan melalui jaringan internet, dan bukan merupakan bank yang hanya menyelenggarakan layanan perbankan melalui internet, sehingga pendirian dan kegiatan *Internet Only Bank* tidak diperkenankan. Pada dasarnya internet banking memiliki tiga tahap pelayanan yang ditawarkan kepada nasabahnya yaitu: Pertama, layanan informasi (*informational*) dimana bank hanya menyediakan informasi jasa keuangan dalam

---

[117] *Ibid*

[118] http://imazshare.wordpress.com/2012/12/03/makalah-permasalahan-smsmobile-banking-yang-terjadi-pada-perbankan-di-indonesia/html, diakses tanggal 5 Februari 2015 (21.15).

websitenya. Kedua, komunikasi (*communicational*) dimana dalam website tersebut juga memungkinkan nasabah dapat berkomunikasi dengan bank. Ketiga, transaksi (*transactional/advance*) dimana sudah memungkinkan nasabah untuk melakukan transaksi-transaksi keuangan virtual seperti, transfer dana, pengecekan saldo ataupun berbagai jenis pembayaran.[119]

Data yang ada saat ini, di Indonesia terdapat enam bank yang telah menyelenggarakan internet banking pada tahap transaksi, sedangkan pada tahap informasi dan komunikasi terdapat sekitar 40 bank yang memiliki website. Bank adalah lembaga kepercayaan, dalam menjalankan kegiatan *internet banking* harus pula diselenggarakan dengan memperhatikan ketentuan maupun prinsip-prinsip kehati-hatian dan manajemen risiko terkait penyelenggaraan *intenet banking* khususnya risiko reputasi dan risiko hukum. *Internet banking* merupakan *delivery channel* dalam industri perbankan. Kegiatan yang potensial menjadi target *cyber crime* dalam kegiatan perbankan antara lain adalah:

1. Layanan pembayaran menggunakan kartu kredit pada situs-situs toko online.
2. Layanan Perbankan Online.[120]

Dalam kaitannya dengan *cyber crime*, maka sudut pandangnya adalah kejahatan internet yang menjadikan pihak bank, merchant, toko online atau nasabah sebagai korban yang dapat terjadi karena maksud jahat seseorang yang memiliki kemampuan dalam bidang teknologi informasi atau seseorang yang

---

[119] http://hadi-gun.blogspot.com/2010/03/saat-ini-pemanfaatan-teknologi.html, diakses tanggal 5 Februari 2015 (19.49)

[120] *Ibid*

memanfaatkan kelengahan pihak bank pihak merchant maupun pihak nasabah. Beberapa bentuk potensi *cyber crime* dalam kegiatan perbankan antara lain :

1. *Typo site*: Pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika ada seorang korban salah mengetikkan alamat dan masuk ke situs palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi *user* dan *password* korbannya, dan dapat dimanfaatkan untuk merugikan korban.[121]
2. *Keylogger/Keystroke Logger:* Modus lainnya adalah keylogger. Hal ini sering terjadi pada tempat mengakses internet umum seperti di warnet. Program ini akan merekam karakter-karakter yang diketikkan oleh *user* dan berharap akan mendapatkan data penting seperti *user* ID maupun *password.* Semakin sering mengakses internet di tempat umum, semakin rentan pula terkena modus operandi yang dikenal dengan istilah *keylogger atau keystroke logger* ini. Sebab, komputer-komputer yang berada di warnet digunakan berganti-ganti oleh banyak orang. Cara kerja dari modus ini sebenarnya sangat sederhana, tetapi banyak para pengguna komputer di tempat umum yang lengah dan tidak sadar bahwa semua aktivitasnya dicatat oleh orang lain. Pelaku memasang program *keylogger* di komputer-komputer umum. Program *keylogger* ini akan merekam semua tombol keyboard yang ditekan oleh pengguna komputer berikutnya. Di lain waktu, pemasang *keylogger* akan mengambil hasil "jebakannya" di komputer

[121] *Ibid*

sistem korban dan untuk mencemarkan nama baik pembuat perangkat lunak tertentu.[123]

Modus kejahatan dapat terjadi akibat lemahnya sistem autentifikasi kegiatan perbankan online (*online banking*). Kejahatan siber yang pernah muncul di Indonesia www.klikbca.com, namun ternyata nasabah yang bersangkutan salah mengetik menjadi www.klickbca.com, dikenal dengan istilah *Typosite* yang memanfaatkan kelengahan nasabah yang salah mengetikkan alamat bank online yang ingin diaksesnya. Pelakunya sudah menyiapkan situs palsu yang mirip dengan situs asli bank online (*forgery*). Jika ada nasabah yang salah ketik dan masuk ke situs bank palsu tersebut, maka pelaku akan merekam *user* ID dan *password* nasabah tersebut untuk digunakan mengakses ke situs yang sebenarnya (*illegal access*) dengan maksud untuk merugikan nasabah. Misalnya yang dituju adalah situs.[124]

Faktor yang mendorong atau yang menonjol yang membuat para pelaku terus melakukan perbuatan kejahatan di dunia maya yakni karena adanya rasa aman dalam melakukan perbuatannya. Pada umumnya para pelaku mengetahui kelemahan hukum Indonesia dan aparaturnya dalam upaya untuk menjangkau perbuatannya, terlebih jika korban berdomisili di luar negeri dan jumlah kerugiannya tidak banyak. Beberapa *hacker* bahkan menjad *"hero"* dan bangga dengan dalih bahwa perbuatannya bertujuan untuk melawan arogansi negara adikuasa berkaitan dengan penguasaan teknologi canggih. Dengan kata lain para *hacker* tersebut merasa bahwa perbuatannya adalah sebuah panggilan. Oleh

---

[123] *Ibid*
[124] *Ibid*

karena itu harus dilakukan terus menerus untuk menyadarkan negara adikuasa agar tidak meremehkan kemampuan penguasaan teknologi bagi negara-negara berkembang.[125]

Era kemajuan teknologi informasi ditandai dengan meningkatnya penggunaan internet dalam setiap aspek kehidupan manusia. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, di sisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana. Faktor-faktor yang mempengaruhi *cyber crime* (kejahatan siber) pada internet banking adalah :

1. Faktor Politik

Mencermati maraknya *cyber crime* (kejahatan siber) yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak hukum, proses kejahatan siber yang terjadi merugikan masyarakat. Faktor yang mempengaruhi *cyber crime* (kejahatan siber) dalam bidang politik, misalnya sabotase untuk menjatuhkan lawan politik untuk menduduki posisi/jabatan tertentu, atau dengan merusak data atau program komputer milik suatu perusahaan agar mendapatkan keuntungan yang diinginkan, pembuatan website yang berisi informasi yang bersifat provokasi melawan Pemerintah.[126] Bahkan dapat dengan cara penyebaran virus komputer yang dapat merusak jaringan komputer yang digunakan oleh Pemerintah, Perbankan, Pelaku usaha maupun Perorangan yang dapat berdampak terhadap kekacauan dalam sistem jaringan.

---

[125]Al. Wisnusubroto, 2010, *Strategi Penanggulangan Kejahatan Telematika,* Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 41-42.
[126]*Ibid,* hlm. 39-40.

Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja akan mengakibatkan kekacauan dalam transaksi perbankan. Kondisi ini memerlukan kebijakan politik Pemerintah Indonesia untuk menanggulangi *cyber crime* yang berkembang di Indonesia. Aparat penegak hukum telah berupaya keras untuk menindak setiap pelaku *cyber,* tapi penegakkan hukum tidak dapat berjalan maksimal sesuai harapan masyarakat karena perangkat hukum yang mengatur khusus tentang *cyber crime* belum ada. Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku *cyber crime* maka diperlukan kebijakan politik Pemerintah Indonesia untuk menyiapkan perangkat hukum khusus *(lex specialist)* bagi *cyber crime* atau dengan memperbaharui peraturan perundangan yang sudah ada agar dapat menanggulangi kejahatan siber yang banyak terjadi. Dengan ini aparat penegak hukum tidak ragu-ragu lagi dalam melakukan penegakan hukum terhadap *cyber crime* (kejahatan siber).[127]

2. Faktor Ekonomi

Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi. Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi. Masyarakat dunia banyak yang menggunakan media ini untuk mencari barang-barang kepentingan perorangan maupun korporasi. Produk barang yang dihasilkan oleh industri di Indonesia sangat banyak dan digemari oleh komunitas Internasional. Kepentingan mencari barang-barang secara online tersebut dimanfaatkan para *hacker* yang mengetahui PIN kartu kredit yang bukan miliknya melalui internet, kemudian memanfaatkannya untuk

---

[127] *Ibid*

berbelanja di toko *online*, atau perbuatan *hacker* yang berhasil membobol sistem *online* perbankan yang kemudian dilanjutkan dengan mentransfer sejumlah uang ke rekening pribadinya termasuk dalam contoh faktor ekonomi yang mempengaruhi *cyber crime* (kejahatan siber) pada internet banking. Krisis ekonomi yang melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat Indonesia untuk bangkit dari krisis ekonomi yang dimaksud. Seluruh komponen bangsa Indonesia harus berpartisipasi mendukung pemulihan ekonomi. Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk mempromosikan Indonesia.[128]

3. Faktor Tantangan atau Rasa ingin tahu

Faktor tantangan atau rasa ingin tahu ini termasuk dalam faktor yang mempengaruhi *cyber crime* (kejahatan siber) yang bersifat khusus. Pelaku kejahatan melakukan perbuatan seperti *hacking* karena terdorong faktor tantangan (*challenge*) atau rasa ingin tahu. Sudah merupakan hal lazim dalam dunia *hackers* untuk berlomba saling mengungguli dalam hal kemampuan menerobos sistem pengamanan komputer. Misalnya, dalam kasus penyerangan situs KPU pada tahun 2004. Pelaku kejahatan berkeyakinan bahwa perbuatannya dilandasi dengan tujuan yang mulia karena memberitahukan kepada tim IT KPU bahwa sistem keamanannya amat lemah.[129]

4. Faktor Kelalaian Pengguna atau Nasabah

Pengguna atau nasabah dalam sebuah bank terkadang lalai dalam pengaplikasian layanan internet banking yang digunakan, contohnya apabila

---

[128] *Ibid*
[129] *Ibid*, hlm. 41.

membuat PIN/*Password* yang dibuat oleh nasabah di ATM atau langsung di bank cabang hanya digunakan pada log in awal dan dalam penggunaan berikutnya nasabah tidak mengubah PIN/*Password* tersebut. Sehingga menjadi kesempatan para pelaku kejahatan untuk membobol sistem layanan yang digunakan oleh nasabah. Sistem keamanan dari pihak bank sendiri juga terkadang masih sangat lemah dan perlu untuk ditingkatkan agar nasabah merasa aman dan nyaman dalam menggunakan layanan internet bankingnya.[130]

Berdasarkan wawancara dengan Pakar Hukum Universitas Atmajaya, Aloysius Wisnubroto yang melatarbelakangi terjadinya *cyber crime* (kejahatan siber) atau faktor-faktor terjadinya *cyber crime* adalah faktor ekonomi yang membuat pelaku kejahatan ini seringkali membobol bahkan mencuri uang milik orang atau seorang nasabah pada sebuah bank melalui internet dengan menggunakan komputer sebagai alat untuk melancarkan kejahatannya. Pelaku kejahatan *cyber crime* ini juga biasanya hanya ingin mengetes kemampuannya sebagai seorang *hacker* yang sudah bisa dikatakan levelnya tinggi atau belum daripada hacker yang lain, dan pelaku juga ingin mengetes kemampuan dari sistem keamanan dari bank itu sendiri. Karena masih banyak sistem dari perbankan yang terkadang sistem keamanannya masih lemah.[131]

Faktor-faktor yang melatarbelakangi terjadinya *cyber crime* (kejahatan siber) pada internet banking ini bukan hanya faktor ekonomi dan faktor rasa ingin tahu atau tantangan saja melainkan ada faktor lain yaitu untuk mengetahui apakah

---

[130]Dumadia, *Faktor-faktor yang Mempengaruhi Terjadinya Cybercrime*, https://dumadia.wordpress.com/2009/02/03/faktor-faktor-yang-mempengaruhi-terjadinya-cyber- crime/, diakses Jumat tanggal 15 Januari (19.48).

[131]Hasil wawancara dengan Aloysius Wisnubroto, Pakar Hukum di Universitas Atmajaya Yogyakarta pada hari Jumat tanggal 7 November 2014.

teknologi di dunia sekarang sudah canggih atau belum. Di Indonesia sepertinya teknologinya belum bisa dikatakan canggih bahkan Sumber Daya Manusianya pun belum bisa menyesuaikan dengan teknologi yang sudah ada. Oleh karena itu di Indonesia masih sering terjadi tindak pidana *cyber crime* (kejahatan siber) ini karena semakin lemah atau rapuhnya teknologi serta Sumber Daya Manusianya yang belum bisa menyesuaikan dengan teknologi ini akan lebih memicu munculnya kejahatan melalui dunia maya seperti halnya *cyber crime* (kejahatan siber).[132]

Pada tahun 2001, Indonesia pernah menjadi peringkat teratas dalam kasus *cyber crime* (kejahatan siber) dalam Perbankan. Survey dari AC Nielsen Indonesia berada pada posisi keenam terbesar di dunia dan keempat di Asia dalam kejahatan siber, pada tahun 2002 (catatan Clear Commerce yang bermarkas di Texas AS) Indonesia menduduki urutan kedua setelah Ukraina sebagai negara asal carder terbesar di dunia, pada tahun 2003 (catatan Verisign, perusahaan keamanan TI) Indonesia berada pada tingkat paling atas di dunia dalam hal persentase kejahatan penipuan perbankan di dunia. Peringkat tertinggi dalam hal kejahatan cyber yang disandang Indonesia tersebut tetap bertahan hingga dekade pertama abad 21 ini.[133]

Di Indonesia ini belum ada peraturan khusus yang menangani tentang *cyber crime* (kejahatan siber) seperti negara-negara lain yang sudah memiliki peraturan bahkan dari strukturnya dalam menangani tindak pidana *cyber crime* (kejahatan siber). Dari sisi kultur hukumnya pun Indonesia terlalu percaya dengan

---

[132]Hasil wawancara dengan Aloysius Wisnubroto, Pakar Hukum di Universitas Atmajaya Yogyakarta pada hari Jumat tanggal 7 November 2014.

[133]*Cybercrime Indonesia Tertinggi di Dunia,* KOMPAS.com 25 Maret 2009, http://nasional.kompas.com/read/2009/03/25/18505497, diakses 22 Desember 2014 (19.54).

dunia nyata, sebagai contoh apabila menjadi nasabah pada sebuah bank dan memiliki kartu kredit atau ATM (Anjungan Tunai Mandiri) yang didalamnya terdapat tabungan dengan jumlah besar tetapi nasabah tersebut tidak mengetahui dan menyadari apabila uang yang ada di dalam tabungannya tersebut telah dicuri orang (*hacker*). Para nasabah hanya berfikir uang tersebut mungkin sebagian dari potongan per bulan oleh pihak bank atau potongan-potongan lain dari sistem bank tersebut.[134]

Kejahatan pun mendapat tempat yang spesial di sini. Mulai dari penipuan sederhana sampai yang sangat merugikan, ancaman terhadap seseorang atau kelompok, penjualan barang-barang ilegal, sampai tindakan terorisme yang menewaskan ribuan orang juga bisa dilakukan menggunakan komputer dan internet. Melihat semakin meningkatnya kejahatan di internet dan dunia komputer, mulai banyak negara yang merespon hal ini. Dengan membuat pusat-pusat pengawasan dan penyidikan pada kejahatan di dunia cyber ini diharapkan kejahatan *cyber* tidak akan terus berkembang merajalela tak terkendali. Tindakan, perilaku, perbuatan yang termasuk dalam kategori *cyber crime* atau kejahatan siber adalah sebagai berikut:

1. Penipuan finansial melalui perangkat komputer dan media komunikasi digital.
2. Sabotase terhadap perangkat-perangkat digital, data-data milik orang lain, dan jaringan komunikasi data.
3. Pencurian informasi pribadi seseorang maupun organisasi tertentu.

[134]Hasil wawancara dengan Aloysius Wisnubroto, Pakar Hukum di Universitas Atmajaya Yogyakarta pada hari Jumat tanggal 7 November 2014.

4. Penetrasi terhadap sistem komputer dan jaringan sehingga menyebabkan privasi terganggu atau gangguan pada fungsi komputer yang digunakan (*denial of service*).
5. Para pengguna internal sebuah organisasi melakukan akses-akses ke server tertentu atau ke internet yang tidak diijinkan oleh peraturan organisasi.
6. Menyebabkan virus, worm, backdoor, trojan pada perangkat komputer sebuah organisasi yang mengakibatkan terbukanya akses-akses bagi orang-orang yang tidak berhak.[135]

Beberapa penyebab kejahatan siber kian marak dilakukan antara lain adalah:

1. Akses internet yang tidak terbatas.
2. Kelalaian pengguna komputer. Hal ini merupakan salah satu penyebab utama kejahatan siber.
3. Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan siber mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan hal ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan siber tentang cara kerja sebuah komputer jauh di atas operator komputer.
5. Sistem keamanan jaringan yang lemah.

---

[135] http://www.academia.edu/6518821/Kejahatan_Di_Dunia_Maya_Cybercrime_Oleh_I_Wayan_Putra_Yasa_100010236_Kelas_AF_101, diakses tanggal 23 Januari 2015 (20.46)

6. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvensional. Pada kenyataannya para pelaku kejahatan siber masih terus melakukan aksi kejahatannya.
7. Belum adanya undang-undang atau hukum yang mengatur tentang kejahatan siber.[136]

Modus tindak pidana berdasarkan motif kegiatan antara lain:

1. *Cyber crime* sebagai tindakan murni kriminal

Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh *carding* yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Pemanfaatan media internet (*webserver, mailing list*) untuk menyebarkan material bajakan. Pengirim email anonim yang berisi promosi *(spamming)* juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku spamming dapat dituntut dengan tuduhan pelanggaran privasi.[137]

2. *Cyber crime* sebagai kejahatan "abu-abu"

Pada jenis kejahatan di internet yang masuk dalam wilayah "abu-abu", cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Contoh: *Probing* atau *Portscanning.* Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-

---

[136] *Ibid*
[137] *Ibid*

banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun tertutup, dan sebagainya.[138]

Modus yang berdasarkan sasaran kejahatan yaitu:

1. *Cyber crime* menyerang hak milik

Cyber crime yang dilakukan untuk menggangu atau menyerang hak milikorang lain. Contoh:

a. Pengaksesan komputer secara tidak sah melalui dunia *cyber*.
b. Pemilikan informasi elektronik secara tidak sah/pencurian informasi, *carding*, *cybersquating*, *hijacking*, data *forgery*.
c. Kegiatan yang bersifat merugikan hak milik orang lain.[139]

B. Peraturan yang dapat diterapkan terhadap terjadinya *Cyber Crime* (Kejahatan Siber) pada Internet Banking

Berkembangnya penggunaan internet banking di Indonesia menjadi salah satu alasan makin banyaknya kejahatan siber yang menyerang pengguna internet banking. Pengguna internet banking di Indonesia pada akhir tahun 2013 yang lalu sebanyak 23 juta pengguna. Jumlah ini tentu masih sangat kecil bila dibandingkan dengan pengguna ponsel yang mencapai 297 juta orang. Namun makin banyaknya pengguna internet banking ini dibayangi oleh serangan kejahatan teknologi informasi atau *cyber crime*.[140]

Berikut data contoh kasus tentang kejahatan siber pada internet banking:

---

[138] *Ibid*

[139] https://amicha321.files.wordpress.com/2010/06/cybercrime-kelompok-7.pdf, diakses tanggal 23 Januari (21.10).

[140] http://ictwatch.com/internetsehat/2014/06/06/internet-banking-indonesia-dibayangi-serangan-cyber/, diakses tanggal 5 Februari 2015 (19.21)

No.	Jenis Kasus	Pasal/Dasar Hukum	Keterangan
1.	Kasus Steven Haryanto (Tahun 2001)	Kasus ini tidak dibawa ke Pengadilan karena berakhir atau diselesaikan dengan proses perdamaian	Kejahatan ini termasuk dalam kategori *cyber crime "data forgery"* dan *"Typosite"*. Dilihat dari modus operandinya kasus atau kejahatan ini menggunakan nama domain, komputer, internet serta *user id* dan *password* nasabah pada Bank BCA. Modusnya karena ada faktor sosial budaya yang dipengaruhi oleh kemajuan teknologi informasi dan sumber daya manusia yang mempunya peranan sebagai pengendali sebuah alat informasi dan komunikasi. Pelaku juga mempunyai motivasi untuk mengetes seberapa tinggi kemampuannya dan sistem keamanan pada layanan internet banking Bank BCA
2.	Kasus pencurian uang nasabah melalui layanan internet banking (Tahun 2009)	Pasal 363 KUHP dan Pasal 32 ayat (2) UU Nomor 11 Tahun 2008 tentang ITE	Menurut keterangan dari Kasat Cyber Crime Polda Metro Jaya, AKBP Winston Tommy Watuliu, mengungkap kasus pencurian uang nasabah melalui layanan internet banking yang terjadi pada tanggal 25 Januari 2009 sampai Agustus 2009 di kawasan Jakarta Selatan. Tersangka berinisial EYN dan Tersangka lainnya yang berinisial HH yang masih dalam pencarian telah melakukan pengacakan *Password* nasabah pada salah satu bank swasta (Polisi merahasiakan nama Bank swasta yang bersangkutan) dengan menggunakan data-data pribadi korban. Dua nasabah

			atau korban akibat pembobolan uang melalui layanan internet banking pada bank swasta tersebut yang berinisial AS ini menderita kerugian sebesar 60 juta rupiah dan korban yang berinisial WRS menderita kerugian sebesar 610 ribu.

Pada tahun 2001, Steven Haryanto telah membuat dunia IT dan Perbankan Indonesia gempar, dengan membuat nama domain tiruan pada sistem internet banking milik PT Bank Central Asia (BCA).[141]

Kasus pertama tentang kasus kejahatan siber dengan nama domain pada internet banking milik PT Bank Central Asia. Kejahatan ini dilakukan oleh Steven Haryanto tahun 2001. Steven sendiri bukan ahli elektro maupun informatika, melainkan Insinyur Kimia ITB Bandung dan juga merupakan karyawan media online Satunet.com. Dalam kasus ini nama domain 'www.klikbca.com' diplesetkan menjadi empat nama domain yang mirip, yakni 'www.clikbca.com', 'www.klickbca.com','www.kilkbca.com','www.klikbac.com. Awalnya motivasi Steven adalah agar semua orang sadar terhadap masalah keamanan sistem internet banking. Namun munculnya *web site* "tandingan" buatan Steven tersebut membuat banyak nasabah BCA yang "kesasar" masuk ke *web site* yang salah. Akibat yang lebih serius lagi sekitar 130 *user ID* dan PIN internet banking milik nasabah BCA secara otomatis terkirim pada pemilik situs BCA plesetan, sehingga Steven sempat terseret urusan hukum. Beruntung pada akhirnya persoalan Steven

[141]R. Kresno Aji, 2002, *Kejahatan Internet: Trik Aplikasi dan Tip Penanggulangannya,* Jakarta, PT Elex Media Komputindo, hlm. 137.

dan Pihak BCA berakhir dengan proses perdamaian.[142] Dan kemudian Steven mengirimkan email yang isinya permohonan maaf kepada pihak PT Bank Central Asia serta para nasabah BCA dan email tersebut juga dipublikasikan di media online.

Menurut Pakar Hukum Universitas Atmajaya, Aloysius Wisnubroto, kejahatan ini termasuk dalam kategori *cyber crime "data forgery"* dan *"Typosite"*. Dilihat dari modus operandinya kasus atau kejahatan ini menggunakan nama domain, komputer, internet serta *user id* dan *password* nasabah pada Bank BCA. tindak pidana yang dilakukan oleh Steven Haryanto adalah suatu tindak kejahatan yang menggunakan komputer dengan tujuan untuk mengetes sistem keamanan dalam dunia Perbankan. Mulanya Steven tidak mempunyai niat untuk melakukan tindak kejahatan tersebut tetapi karena rasa ingin tahunya tinggi maka Steven berusaha mencoba menduplikat atau membuat nama domain tiruan pada sistem internet banking milik Bank BCA. Termasuk juga dalam motif pelaku dalam mengetes kemampuan yang dimilikinya dalam bidang telematika dan teknologi, sehingga Steven terseret pada urusan hukum dan beruntungnya persoalan antara Steven dengan pihak BCA berakhir dengan proses perdamaian.[143]

Kejahatan yang dilakukan oleh Steven Haryanto ini apabila dikaitkan dengan penerapan hukumnya maka dapat digunakan Pasal 362 KUHP tentang Pencurian, Pasal 378 KUHP tentang Penipuan dan Pasal 35 Undang-Undang

---

[142]Hasil wawancara dengan Aloysius Wisnubroto, selaku Pakar Hukum di Universitas Atmajaya Yogyakarta pada hari Jumat tanggal 7 November 2014.

[143]Hasil wawancara dengan Aloysius Wisnubroto selaku Pakar Hukum di Universitas Atmajaya Yogyakarta pada hari Jumat tanggal 7 November 2014.

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) tentang pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik.[144]

Pada kasus kedua, berdasarkan keterangan dari Kasat Cyber Crime Polda Metro Jaya, AKBP Winston Tommy Watuliu, mengungkap kasus pencurian uang nasabah melalui layanan internet banking yang terjadi pada tanggal 25 Januari 2009 sampai Agustus 2009 di kawasan Jakarta Selatan. Tersangka berinisial EYN yang berumur 30 tahun sebagai pengangguran yang sebelumnya bekerja menjadi karyawan swasta dan memiliki riwayat pendidikan S1 di Perguruan Tinggi di Jakarta dan Tersangka lainnya yang berinisial HH yang masih dalam pencarian telah melakukan pengacakan *Password* nasabah pada salah satu bank swasta (Polisi merahasiakan nama Bank swasta yang bersangkutan) dengan menggunakan data-data pribadi korban.[145]

Tersangka melakukan pembobolan *Password* nasabah dengan menggunakan data-data pribadi nasabah yang umumnya nasabah bank menggunakan tanggal lahir sebagai nomor PIN atau *Password* di layanan internet banking bank tersebut. Setelah berhasil menemukan *Password* nasabah, maka uang nasabah yang tercantum di *User ID* itu dipindahkan ke rekening penampung. Dan selanjutnya uang yang berhasil dicuri digunakan untuk keperluan pribadi. Sehingga pelaku dapat dengan mudah membobol uang nasabah ketika PIN yang dimasukkan cocok dengan milik nasabah. Tersangka terancam Pasal 363 KUHP dan Pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi

---

[144]Hasil wawancara dengan Aloysius Wisnubroto, selaku Pakar Hukum di Universitas Atmajaya Yogyakarta pada hari Jumat tanggal 7 November 2014.

[145]http://nasional.inilah.com/read/detail/320891/polisi-ungkap-pembobolan-bank-via-internet, diakses 23 Maret 2015 (23.15).

dan Transaksi Elektronik (ITE). Adapun barang bukti yang disita Polisi yaitu 1 buah laptop, 1 buah modem internet, 1 buah flashdisk, dan 1 buah telefon genggam. Dua nasabah atau korban akibat pembobolan uang melalui layanan internet banking pada bank swasta tersebut yang berinisial AS ini menderita kerugian sebesar 60 juta rupiah dan korban yang berinisial WRS menderita kerugian sebesar 610 ribu.[146]

Kejahatan yang dilakukan oleh Tersangka EYN dan HH termasuk dalam kategori "*Infringements of privacy*" dan "*Brute Force* Attacking". Kejahatan ini menggunakan informasi seseorang yang merupakan hal rahasia dan sangat pribadi dengan usaha untuk mendapatkan *Password* atau *Key* dengan mencoba semua kombinasi acak. Dan apabila diketahui orang lain akan dapat merugikan korban secara materiil seperti *Password* atau nomor PIN ATM.[147] Dilihat dari modus operandinya karena adanya faktor ekonomi dengan membobol data-data pribadi nasabah dalam layanan internet banking kemudian uang yang berhasil dipindahkan pada rekening penampung oleh Tersangka digunakan untuk keperluan pribadi.

Berdasarkan keterangan dari Kasat Cyber Crime Polda Metro Jaya, AKBP Winston Tommy Watuliu, Tersangka diancam dengan Pasal 363 KUHP. Kesesuaian antara unsur-unsur dari Pasal 363 KUHP dalam kasus tersebut yaitu:

a. Unsur "barang siapa" yang dimaksud "barang siapa" dalam hukum pidana adalah subjek hukum (pelaku tindak pidana), yang

---

[146]*Ibid*

[147]H. Abdul Wahid, Mohammad Labib, 2005, *Kejahatan Mayantara (cyber crime),* Bandung, Refika Aditama, hlm. 82.

pengertiannya adalah siapa saja sehingga yang dimaksud "barang siapa" tidak lain adalah Tersangka yang berinisial EYN dan HH.

b. Unsur "mengambil suatu barang" bahwa Tersangka yang berinisial EYN bersama dengan Tersangka yang berinisial HH, telah mengoperasikan 1 (satu) buah laptop untuk melakukan pengacakan *Password* nasabah dengan membobol data-data pribadi nasabah dalam layanan internet banking yang umumnya nasabah menggunakan tanggal lahir sebagai *User ID* dan *Password* atau nomor PIN dalam layanan internet banking tersebut. Setelah berhasil melakukan pembobolan dalam layanan internet banking nasabah tersebut, Tersangka mentransfer uang tersebut ke rekening penampung.

c. Unsur "barang tersebut seluruhnya atau sebagian kepunyaan/milik orang lain". Bahwa uang yang ditransfer ke rekening penampung oleh Tersangka yang berinisial EYN dan yang berinisial HH bukan milik Tersangka melainkan milik nasabah bank swasta yang menggunakan layanan internet banking yang berinisial AS dan WRS.

d. Unsur "dengan maksud untuk memiliki secara/dengan melawan hukum". Bahwa uang tersebut ditransfer dengan tanpa hak.

e. Unsur "dilakukan oleh dua orang atau lebih secara bersama-sama". Bahwa dalam kasus ini kerjasama antara Tersangka yang berinisial EYN dan HH. Dengan terpenuhinya unsur-unsur tersebut, maka diterapkan ketentuan tentang "pencurian yang dilakukan dua orang atau lebih secara bersama-sama".

Berdasarkan kasus yang dilakukan oleh Steven Haryanto yang telah diuraikan di atas terjadi pada Tahun 2001 sebelum lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), namun kasus ini tidak diselesaikan dengan jalur hukum karena antara para pihak yaitu pihak bank BCA dan Steven Haryanto menyelesaikan dengan proses perdamaian sehingga tidak ada putusan pengadilan. Pada kasus yang kedua terjadi pada Tahun 2009 dengan tersangka yang berinisial EYN dan berinisial HH. Kasus tersebut terjadi setelah lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Teguh Arifiyadi mengkategorikan beberapa hal secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat intensitas terjadinya kasus tersebut yaitu ketentuan yang berkaitan dengan delik pencurian dalam Pasal 362 KUHP yang berbunyi:

> "Barangsiapa 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 pidana denda paling banyak sembilan ratus rupiah".[148]

Unsur-unsur dalam Pasal 362 KUHP yang lain seperti milik orang lain dan secara melawan hukum, pada dasarnya cukup bersesuaian apabila dikaitkan dengan unsur-unsur perbuatan yang terdapat dalam kejahatan siber maupun telematika. Dengan demikian pada prinsipnya Pasal 362 KUHP yang mengatur tentang pencurian bisa diterapkan pada kasus perbuatan yang terjadi pada kejahatan siber karena mengkopi informasi secara melawan hukum dengan

[148]Teguh Arifiyadi, *Menjerat Pelaku Cybercrime dengan KUHP*, diakses hari Selasa 27 Januari 2015, www.depkominfo.go.id, (19.48)

catatan dalam pasal tersebut "mengkopi" atau "mentransfer" dalam pasal tersebut diperluas sedemikian rupa sehingga informasi yang terdapat dalam media elektronik (komputer, handphone, CD, dll) termasuk di dalamnya.[149]

Tersangka juga dikenakan Pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) pengaturan mengenai pencurian diatur dalam Pasal 32 ayat (2), kaidah yang mendasar adalah sama dengan yang diatur dalam pasal pencurian dalam KUHP, yaitu dengan adanya unsur memindahkan suatu barang dari tempat asalnya kepada tempat lain dengan tidak memiliki hak atau izin dari pemiliknya. Barang di sini adalah Informasi Elektronik/Dokumen Elektronik kepada Sistem Elektronik. Pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) berbunyi:

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

Dalam hal sanksi pidana terhadap Pasal 32 ayat (2) ditentukan oleh Pasal 48 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang menentukan:

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (Sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000,00 (tiga miliar rupiah)".[150]

Berdasarkan ketentuan umum Bab I Pasal 1 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang dimaksud

---

[149] *Ibid*

[150] Budi Suharyanto, 2013, *Tindak Pidana Teknologi Informasi (Cybercrime)*, Jakarta, PT Raja Grafindo Persada, hlm. 143-144.

disadari memberi peluang untuk dijadikan sarana melakukan tindak kejahatan-kejahatan baru (*cyber crime*) sehingga diperlukan upaya proteksi.[152]

Undang-Undang RI Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) adalah wujud dari tanggung jawab yang harus diemban oleh negara, untuk memberikan perlindungan maksimal pada seluruh aktivitas pemanfaatan teknologi informasi dan komunikasi di dalam negeri agar terlindungi dengan baik dari potensi kejahatan dan penyalahgunaan teknologi. Perbuatan melawan hukum di dunia maya merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan *carding, hacking,* penipuan, terorisme, dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas pelaku kejahatan dunia maya. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika.[153]

Kenyataannya kegiatan siber tidak lagi sederhana, karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun, dimana pun. Kerugian dapat terjadi, baik pada pelaku transaksi maupun pada orang lain, yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui intenet dan digunakan untuk pembelanjaan di internet.[154]

Di Indonesia persoalan menjadi lebih komplek karena pesatnya perkembangan telematika khususnya yang berkaitan dengan *trend* pemanfaatan media transaksi melalui teknologi telematika (internet, telepon, fax, SMS, dll)

---

[152]Siswanto Sunarso, 2009, *Hukum Informasi Dan Transaksi Elektronik*, Jakarta, Rineka Cipta, hlm. 39.
[153]*Ibid,* hlm. 40.
[154]*Ibid,* hlm. 44.

terus berjalan tanpa diikuti keberadaan hukum yang mengatur dan melingkupinya (*cyber law*). Padahal fenomena pelanggaran dalam aktivitas transaksi elektronik semakin nampak berkembang seiring dengan semakin meningkatnya pemanfaatan IT di Indonesia, khususnya internet, mulai di Instansi Pemerintah, Perusahan Swasta, Lembaga Pendidikan, rumah hingga warnet diberbagai belahan kota di Indonesia. Pelanggaran dalam teknologi tersebut dilatarbelakangi oleh berbagai tujuan mulai dari yang bermotif iseng-iseng hingga yang dilandasi motivasi yang mengarah pada tindak kriminal.[155]

Untuk dapat menjerat perbuatan *cyber crime* (kejahatan siber) yang belum ada aturannya dalam sumber hukum pidana di Indonesia, maka pertama harus dicermati peristiwa hukumnya dengan melihat unsur-unsur, sifat dan motivasi serta tujuan akhir atau akibat/dampak dari perbuatan para *hackers/crackers* tersebut. Langkah selanjutnya adalah mencari ketentuan yang terdapat dari sumber hukum pidana positif yang paling relevan unsur-unsurnya untuk kemudian diterapkan dengan metode penafsiran yang dikenal dalam ilmu hukum dan langkah terakhir adalah menerapkannya pada kasus konkret.[156] Pasal yang secara khusus mengatur masalah *cyber crime* (kejahatan siber) pada internet banking belum ada yang mengatur, namun dapat diterapkan melalui interprestasi yang bersifat kontekstual yang dalam beberapa ketentuan dalam KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Menurut AKP. Novita Ekasari, selaku Penyidik Polda Daerah Istimewa Yogyakarta biasanya untuk peraturan yang berkaitan dengan *cyber crime*

---

[155]Al. Wisnubroto, 2010, *Strategi Penanggulangan Kejahatan Telematika,* Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 111.
[156]*Ibid,* hlm. 122.

(kejahatan siber) pada layanan internet banking yang internet banking itu sendiri adalah salah satu dari fasilitas atau sistem bank dalam memudahkan nasabah, maka bisa diterapkan dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Tetapi untuk kasus *cyber crime* (kejahatan siber) pada internet banking yang kejahatannya melalui SMS Banking sendiri belum pernah menangani karena Penyidik lebih sering menangani kasus *carding*, pencurian ATM, kredit macet, dan pelelangan pinjaman nasabah oleh pihak bank.[157]

Perbuatan pidana di bidang perbankan yang diatur dalam Undang-Undang Nomor 7 Tahun 1992 jo Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, baik yang dikategorikan sebagai perbuatan pidana kejahatan maupun perbuatan pidana pelanggaran belum cukup memadai untuk mencegah dan menindak kejahatan di bidang perbankan yang bersifat komplek. Keadaan yang demikian tentu memerlukan adanya pembaharuan peraturan perundang-undangan yang dapat diterapkan atau yang dapat diberlakukan terhadap perbuatan pidana di bidang perbankan. Pada pokoknya undang-undang yang dapat diberlakukan dalam perbuatan pidana di bidang perbankan adalah KUHP Buku Kedua tentang Kejahatan dan Buku Ketiga tentang pelanggaran yaitu dalam bab dan pasal yang terkait dengan perbuatan pidana yang dilakukan.[158]

Pemberian sanksi dalam hal kebijakan hukum pidana, maka harus terlebih dahulu mengetahui seluk beluk hakikat suatu sanksi hukum. Sanksi hukum (dalam arti sempit) adalah sanksi atau hukuman yang dijatuhkan pada seseorang yang

---

[157]Hasil wawancara dengan AKP. Novita Ekasari, selaku Penyidik di POLDA DIY dari Ditkrimsus bagian Kasubdit 1 pada hari Jumat tanggal 7 November 2014.

[158]Mahesa Jati Kusuma, 2012, *Hukum Perlindungan Nasabah Bank*, Bandung, Nusa Media, hlm. 93.

melanggar hukum. Sanksi hukum diatur oleh hukum baik mengenai ruang lingkup maupun cara pelaksanaanya. Sanksi diadakan sebagai konsekuensi dari perbuatan yang dianggap merugikan masyarakat dan yang menurut maksud dari tata hukum harus dihindari. Pelanggaran terhadap norma hukum akan berakibat adanya sanksi hukum yang sifatnya memaksa, yaitu hukuman mati, hukuman penjara atau kurungan, dan hukuman denda.[159]

Sistem peradilan pidana tidak sekedar dilihat sebagai sistem penanggulangan kejahatan, tetapi dilihat sebagai "social problem" yang sama dengan kejahatan itu sendiri. Dikatakan demikian karena di samping kenyataan menunjukkan bahwa kejahatan tetap terus meningkat, yang dapat dilihat sebagai indikator tidak efektifnya sistem peradilan pidana. Kitab Undang-Undang Hukum Pidana (KUHP) telah mengatur hubungan hukum tentang kejahatan yang berkaitan dengan siber yang kemudian berkembang menjadi *cyber crime.* Dalam hal ini, diragukannya KUHP dalam menanggulangi *cyber crime* secara efektif karena kejahatan tetap terus meningkat. Sehingga Pemerintah perlu memperbaharui Undang-Undang yang ada agar dapat diterapkan untuk mengatur tentang *cyber crime* (kejahatan siber).[160]

Informasi dalam komputer sering kali jauh lebih berharga dari aset peranti keras itu sendiri. Bisa dibayangkan betapa besar kerugian yang diderita suatu instansi atau perusahaan apabila terjadi pencurian informasi penting oleh oknum tertentu. Jenis informasi berharga ini meliputi data finansial, kartu kredit, informasi perbankan, data pribadi, bahkan juga rahasia negara, formula obat,

---

[159]Mochtar Kusumaatmadja dan Arief Sidharta, 2000, *Pengantar Ilmu Hukum, Buku I,* Bandung, hlm. 43.

[160]*Ibid*

temuan sains dan banyak lagi. Konsep pencurian data ini mencakup menggandakan data atau mengunduh informasi yang bukan menjadi haknya. Oleh karenanya sebaiknya sanksi minimum khusus perlu diakumulasikan juga mengingat *cyber crime* ini bukanlah kejahatan biasa yang menimbulkan kerugian yang tidak sederhana.[161]

Pada kenyataan yang ada, tidak terlihat secara nyata korban dari kejahatan *cyber* dibandingkan korban dari kejahatan konvensional, tetapi selain korban dari kejahatan *cyber* lebih besar jumlahnya, juga dampak yang ditimbulkan bila diperhatikan justru lebih berbahaya dari kejahatan konvensional. Artinya kondisi seperti itu tidak dapat dibiarkan begitu saja, khususnya dalam praktik penegakan hukum terhadap kejahatan tersebut. Mengenai ganti kerugian dalam sanksi pidana untuk *cyber crime* perlu adanya keseimbangan perlindungan antara pelaku dan korban.[162]

Cyber crime (kejahatan siber) pada layanan internet banking ini belumlah cukup apabila hanya diterapkan dengan pasal-pasal dalam KUHP karena kejahatan ini sangat sulit untuk ditelusuri dan dibuktikan. Kejahatan ini bukan seperti kejahatan dunia nyata yang dalam penyelidikan atau pun proses pemeriksaannya bisa dilakukan dalam dunia nyata melainkan kejahatan ini adalah kejahatan dunia maya. Selain KUHP dapat juga diterapkan Undang-Undang Perbankan sebagaimana kaitannya dengan internet banking yang tidak lain adalah salah satu sistem dalam bidang perbankan itu sendiri. Undang-Undang Perbankan

---

[161] *Ibid*
[162] *Ibid*

di Indonesia telah beberapa kali mengalami pergantian dan perubahan. Setidaknya semenjak industri jasa perbankan berkembang.

Perubahan dari Undang-Undang Nomor 14 Tahun 1967 menjadi Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan tersebut antara lain didasarkan pada pertimbangan perlunya perundang-undangan dalam perbankan yang mampu menjangkau perkembangan perekonomian nasional maupun internasional yang senantiasa bergerak cepat disertai dengan tantangan-tantangan yang semakin luas. Salah satu tantangan perkembangan perekonomian pada era globalisasi terutama globalisasi ekonomi adalah pengembangan pengaplikasian teknologi canggih seperti sarana teknologi telematika di bidang perbankan. Tuntutan peningkatan fasilitas kemudahan dan kenyamanan bagi nasabah dan peningkatan persaingan antar bank memacu lembaga perbankan berlomba-lomba menciptakan keunggulan dengan sarana komputerisasi.[163]

Sarana komputerisasi tersebut mulai dengan komputerisasi hingga sistem bank elektronik (*e-banking*) termasuk di dalamnya adalah fasilitas internet banking. Pemanfaatan teknologi tersebut di bidang perbankan di satu sisi meningkatkan kualitas pelayanan namun di sisi lain juga membuka potensi terhadap gangguan teknis hingga penyimpangan yang bersifat kriminal. Dengan penerapan teknologi komputer dalam operasional kegiatan perbankan, data yang menyangkut rahasia bank dan nasabah tidak lagi terbatas dalam bentuk tertulis di atas kertas, namun juga banyak yang berbentuk elektronis. Dalam sistem

[163]Al wisnubroto, 2011, *Konsep Hukum Pidana Telematika,* Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 188.

perbankan global telah terjadi pergeseran dari sistem manual ke sistem elektronik atau sistem virtual.[164]

Oleh sebab itu jika terjadi kasus pembocoran rahasia bank atau pun nasabah dengan sarana teknologi canggih misalnya dengan cara "*hacking*" pada server yang menyimpan informasi mengenai simpanan nasabah, terhadap pelaku dapat diancam dengan ketentuan Pasal 47 Undang-Undang Nomor 7 Tahun 1992 jo Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Dengan demikian masih bisa diterapkan terhadap kasus-kasus penyalahgunaan komputer yang terjadi dalam perbankan dengan perkembangan layanan internet banking. Kejahatan siber dalam perbankan pada layanan internet banking ini juga berkaitan dengan kejahatan telematika mengingat komputer merupakan alat untuk menggunakan layanan sistem informasi seperti internet.[165]

Keberadaan Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi bisa dipandang sebagai "*lex generalis*" bila dihadapkan dengan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), sekaligus sebagai "*lex specialis*" bila dihadapkan dengan KUHP. Namun demikian dalam tataran praksis pembahasan mengenai telematika hampir selalu berkisar pada persoalan teknologi informatika yakni terkait dengan pemanfaatan komputer sebagai sarana berkomunikasi semata. Konkretnya telematika hampir selalu identik dengan internet atau teknologi dunia *cyber*.[166] Maka persoalan-persoalan yang terkait dengan telematika termasuk kejahatan komputer atau telematika bisa pula diselesaikan dengan Undang-Undang

---

[164]*Ibid*
[165]*Ibid,* hlm. 190.
[166]Edmon Makarim, 2003, *Kompilasi Hukum Telematika,* Jakarta, Raja Grafindo Persada, hlm. 4-5

Telekomunikasi. Beberapa ketentuan dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang dapat diterapkan dalam kejahatan siber tersebut antara lain Pasal 22 jo Pasal 50 Undang-Undang Telekomunikasi dan Pasal 40 jo Pasal 56 Undang-Undang Telekomunikasi.

Pasal 22 Undang-Undang Telekomunikasi yang berbunyi:

"Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: a. akses ke jaringan telekomunikasi; dan atau
b. akses ke jasa telekomunikasi; dan atau
c. akses ke jaringan telekomunikasi khusus".

Pasal 50 Undang-Undang Telekomunikasi berbunyi:

"Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)".

Pasal 22 jo Pasal 50 Undang-Undang Telekomunikasi dapat diterapkan misalnya pada kejahatan telematika seperti *hacking* atau *carding*. Dalam *hacking* pelaku pada dasarnya melakukan akses ke jaringan komputer secara tidak sah. Jaringan komputer (internet) dapat ditafsirkan sebagai telekomunikasi khusus. Jaringan komputer bersifat khusus karena memerlukan sarana khusus seperti kode akses, *IP Address,* ISP dan berbagai prosedur khusus yang dikenal dalam teknologi informatika.[167] Dalam *carding* pelaku telah melakukan manipulasi *password,* PIN, atau berbagai kode akses lainnya sehingga bisa memanfaatkan fasilitas transaksi elektronik secara online dan illegal untuk perbuatan yang illegal pula, sehingga *carder* telah melakukan perbuatan memanipulasi akses jaringan telekomunikasi secara illegal.

Pasal 40 Undang-Undang Telekomunikasi yang berbunyi:

---

[167]Judhariksawan, 2005, *Pengantar Hukum Telekomunikasi,* Jakarta, Raja Grafindo Persada, hlm.14.

"Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun".

Pasal 56 Undang-Undang Telekomunikasi yang berbunyi:

"Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun".

Demikianlah pembahasan berbagai peraturan perundang-undangan di Indonesia yang dapat diterapkan terhadap kasus kejahatan yang berkaitan dengan kejahatan siber (*cyber crime*). Dari peraturan yang diterapkan menggunakan KUHP, Undang-Undang Nomor 10 tahun 1998 tentang Perbankan, Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Sebelum diberlakukannya Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) berbagai peraturan perundangan lain bisa diterapkan terhadap berbagai kejahatan siber tetapi memerlukan perluasan kepastian hukum dalam menangani *cyber crime* (kejahatan siber) khususnya dalam perbankan.