BAB III

CYBER CRIME DALAM BENTUK *PHISING* DAN SANKSI HUKUMNYA

A. Pengertian *Cyber Crime*

Cyber crime di definisikan sebagai kejahatan komputer. definisi kejahatan komputer sendiri, sampai sekarang para ahli hukum belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. beberapa ahli hukum menggunakan istilah "*computer misuse*", "*computer abuse*", "*computer fraud*", "*computer-related crime*", "*computer-assisted crime*", atau "*computer crime*" Namun para ahli hukum pada waktu itu, umumnya lebih menerima pemakaian istilah "*computer crime*" oleh karena dianggap lebih luas dan bisa dipergunakan dalam hubungan internasional.[1]

Sistem teknologi informasi berupa *internet* telah menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer, karena adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari definisi *cyber crime* lebih diperluas lagi. Jadi *cyber crime* tidak hanya dimaknai kejahatan komputer saja, tetapi dapat diperluas menjadi kejahatan teknologi informasi.[2]

Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi, serta sistem komunikasi yang merupakan

[1] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya,* (Jakarta:PT Rajagrafindo Persada, 2013), 9.
[2] Ibid., 10.

sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya (*transmiter/originator to recipient*).[3]

B. *Cyber Crime* dalam Bentuk *Phising*

Phising (*password harvesting fishing*) adalah tindakan penipuan yang menggunakan email palsu atau situs *website* palsu yang bertujuan untuk mengelabui *user* sehingga pelaku bisa mendapatkan data *user* tersebut.[4]

Tindakan penipuan ini berupa sebuah email yang seolah-olah berasal dari sebuah perusahaan resmi, misalnya bank dengan tujuan untuk mendapatkan data-data pribadi seseorang, misalnya PIN, nomor rekening, nomor kartu kredit, dan sebagainya.

Phising terjadi saat seseorang menyamar sebagai orang lain, sering kali dengan situs *web* palsu, untuk menipu anda agar berbagi informasi pribadi. Pada *scam phising* biasa, penyerang mengirimkan email yang seolah-olah berasal dari bank atau layanan *web* yang biasa anda gunakan. Baris subjek dapat berisi "Harap perbarui informasi anda di bank!" Email tersebut akan berisi tautan *phising* yang seolah-olah mengarah ke situs *web* anda, tetapi sebenarnya mengarahkan anda ke situs *web* penipu. Di sana, anda diminta

[3] Dikdik M. Arief Mansur dan Elisatris Gulton, *Cyberlaw Aspek Hukum Teknologi Informasi,* (Bandung: PT Refika Aditama, 2009), 10.
[4] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding,* (Yogyakarta:CV Andi Offset, 2013), 214.

untuk masuk dan tanpa sengaja menyingkapkan nomor rekening bank, nomor kartu kredit, sandi atau informasi sensitif lainnya kepada penjahat.[5]

Menurut IGN Mantra dosen peneliti *cyber war* dan *security inspection* menjelaskan bahwa *phising* adalah percobaan penipuan menggunakan *surel* (surat elektronik) dengan tujuan untuk mendapatkan *username*, *password*, *token*, dan informasi-informasi sensitif lainnya yang dikirim melalui *surel*. *Surel phising* datang seolah-olah dari perusahaan/organisasi di mana *user* adalah anggota/*member*.[6]

Pelaku *phising* dikenal dengan sebutan *phiser*. Katakanlah seorang *phiser* mengirimkan email kepada seribu orang korban dengan dalih *update* informasi data konsumen. Dari keseluruhan angka tersebut, 5 % saja yang merespon maka *phiser* telah berhasil mendapatkan data dari 50 orang. Hal ini bisa terjadi karena *phiser* juga berdalih apabila tidak dilakukan perubahan data maka *user account* akan dihapus sehingga tidak bisa digunakan lagi. Para *user* yang tidak tahu modus penipuan ini tentu akan takut *account* mereka dihapus oleh pihak bank sehingga tanpa pikir panjang langsung memberikan informasi rekening termasuk *username* dan *password*-nya. Dalam kebanyakan kasus *phising*, teknik yang digunakan adalah perubahan data, termasuk di dalamnya *password* dan nomor kartu kredit.[7]

---

[5] Min Li Chan dkk, "20 Topik Penting Seputar Peramban dan Dunia Web", dalam http://www.20thingsilearned.com/in-ID/malware/1, diakses pada 04 September 2015.
[6] IGN Mantra, "Potensi Ancaman Keamanan Email Perusahaan", *Info Komputer*, (9 September 2015), 71.
[7] Vyctoria, *Bongkar Rahasia*..., 215.

Modus operandi yang paling banyak ditemui saat ini adalah usaha *phising* melalui SMS pada telepon genggam, di mana sudah banyak korban yang harus kehilangan uangnya karena diminta untuk melakukan transaksi ke rekening tertentu dengan berbagai alasan yang seolah-olah masuk akal sehingga menjebak sang korban.[8]

Phising biasanya memanfaatkan email, *website* palsu, *spyware* dan berbagai media lainnya untuk melakukan aksinya. Beberapa hal yang menyebabkan aksi *phising* ini terus terjadi dan memakan banyak korban adalah:[9]

1. Ketidaktahuan atau kurangnya pengetahuan

   Kurangnya pengetahuan akan teknologi komputer membuat pelaku *phising* mudah mendapatkan mangsanya. Dengan memberikan email yang menakutkan, seperti ancaman hilangnya nama *domain* akan membuat korbannya segera melakukan apa yang diminta.

2. Tampilan palsu yang menyesatkan

   Pemalsuan *website* dan gambar-gambar sangat mudah dilakukan melalui internet dan pengguna awam biasanya tidak menyadari hal tersebut. Hanya dengan melakukan *copy* dan *paste*, sebuah *website* yang mirip dengan asli akan langsung tercipta. Pelaku *phising* juga bisa membuat *website* yang tampak sangat bagus dengan

[8] Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber,* (Yogyakarta: Graha Ilmu, 2014), 116.
[9] S'to, *Certified Ethical Hacker 400% Illegal,* (t.tp.: Jasakom, 2011), 146.

berbagai komentar pengguna yang semuanya fiktif untuk meyakinkan calon korbannya.

3. Kurangnya perhatian pada indikator keamanan

Sangat sering, pesan-pesan yang muncul tidak dibaca oleh pengguna. Biasanya, pesan-pesan ini terlalu teknis untuk pengguna awam sehingga mereka selalu mengklik tombol "OK" untuk melanjutkan. Kebiasaan semacam ini membawa keuntungan tersendiri untuk pelaku *phising* sehingga mereka bisa memalsukan *website* dan mendapatkan informasi berharga yang dimasukkan oleh korbannya.

C. Metode dan Teknik Serangan *Phising*

Adapun untuk mendapatkan korban *phising*, banyak cara yang digunakan dan hal ini biasanya terus berkembang sesuai dengan perkembangan yang ada di dalam dunia internet. Beberapa metode yang populer digunakan adalah:[10]

1. Email / *SPAM*

Media yang paling favorit digunakan untuk mencari korban adalah email. Email dipilih karena murah dan mudah untuk digunakan. Pelaku bisa mengirimkan jutaan email setiap harinya tanpa perlu mengeluarkan biaya yang cukup besar. Bahkan pelaku

[10] Ibid., 147.

phising juga suka menggunakan *server-server* bajakan untuk melakukan aksinya.

Penggunaan email dilakukan karena sangat mudah memalsukan email. Pelaku bisa mengubah "*From*" menjadi apa saja karena memang tidak ada verifikasi di dalam email. Pelaku bisa membuat email dengan mengambil format dari email resmi agar lebih meyakinkan dan mengubah bagian-bagian yang diperlukan saja.

2. *Web-based Delivery*

Pelaku *phising* juga memanfaatkan *website* dalam melakukan aksinya. Pelaku biasanya membuat *website* yang mirip dengan *website-website* terkenal untuk mengelabui korbannya. Membuat *website* yang mirip dengan *website* perusahaan besar sangatlah mudah untuk dilakukan karena pelaku hanya perlu membuat tampilan yang sama, tanpa perlu membuat fungsi atau fasilitas yang sama karena tujuannya adalah agar korban memasukkan *username* dan *password* di dalamnya kemudian korban akan dibawa ke situs asli agar tidak curiga.

Pelaku *phising* yang kreatif bahkan memanfaatkan *banner* dan media iklan resmi untuk mengelabui korbannya. Karena merasa mengklik iklan dari *website* resmi, mereka mengira *website* yang dikunjungi pantas untuk dipercaya juga, padahal hal ini tidak berhubungan sama sekali.

Misalnya, anda melihat sebuah iklan di situs kompas yang tepercaya, tentunya anda tidak akan mengira *website* yang anda kunjungi mempunyai maksud buruk. Atas dasar kepercayaan semacam ini, pelaku *phising* tidak akan ragu-ragu memanfaatkan *website-website* ternama untuk melakukan aksinya.

3. IRC / *Instant Messaging*

   Media *chatting* yang banyak digunakan juga menjadi sebagai pelaku *phising* untuk mengirimkan alamat-alamat yang menjebak kepada korbannya. Biasanya pelaku mengirimkan *link* ini secara acak namun ada juga yang melakukan pendekatan terlebih dahulu sebelum mengirimkan informasi situs palsu ini.

4. *Trojan*

   Pelaku *phising*, terkadang juga menipu korbannya agar *menginstall trojan* dan memanfaatkan *trojan* tersebut untuk mengelabui korbannya. *Trojan* memungkinkan pengontrolan secara penuh komputer korban sehingga korban bisa dialihkan ke situs yang telah disediakan jebakan.

Adapun menurut Vyctoria mengenai metode yang digunakan dalam *phising* adalah sebagai berikut:[11]

1. Penggunaan alamat email palsu untuk menyesatkan nasabah sehingga nasabah terpancing menerima keabsahan email atau situs

[11] Vyctoria, *Bongkar Rahasia...*, 122.

web. Agar tampak meyakinkan, pelaku juga sering kali memanfaatkan logo atau merek dagang milik lembaga resmi, seperti bank atau penerbit kartu kredit. Pemalsuan ini dilakukan untuk memancing korban menyerahkan data pribadi (*password,* PIN, dan nomor kartu kredit).

2. Membuat situs *web* palsu yang sama persis dengan situs *web* resmi. Bisa juga pelaku *phising* mengirimkan email yang berisi *link* ke situs *web* palsu tersebut.
3. Membuat *hyperlink* ke situs *web* palsu atau menyediakan formulir isian yang ditempelkan pada email yang dikirim.

Serangan *phising* mengikuti perkembangan teknologi, karenanya di dalam dunia *underground* (kumpulan para *hacker* yang jahat), terdapat pasar gelap yang menjual berbagai program untuk melakukan aksi *phising* ini. Aksi *phising* juga sangat erat hubungannya dengan teknik *hacking* karena pelaku *phising* banyak memanfaatkan kelemahan-kelemahan yang ada untuk mengelabui korban.[12]

Adapun teknik serangan *phising* adalah sebagai berikut:

1. *Man in the middle*

   Pada teknik ini, *hacker* menempatkan dirinya ditengah-tengah antara korban dan *website* asli yang hendak diakses. *Hacker* menerima data-data komunikasi yang lewat untuk kemudian diubah sesuai dengan kebutuhannya. Serangan *man in the middle* bisa terjadi

[12] S'to, *Certified Ethical...*, 148.

di dalam jaringan lokal maupun jaringan internet yang bersifat global.[13]

2. URL *Obfuscation*

URL (*Uniform Resource Locator* atau alamat *web* yang diketik dalam *browser* untuk membuka suatu *website*) *Obfuscation* adalah suatu teknik menyamarkan alamat URL sehingga tampak tidak mencurigakan untuk pengguna. Adapun macam-macamnya adalah sebagai berikut:

a. *String* yang menyesatkan

Memanfaatkan *string* yang tampak asli seperti adanya kata-kata "Microsoft" atau kata-kata yang umum dikenal. Untuk memalsukan *website* "Microsoft" misalnya, pelaku akan membuat *direktori* yang menggunakan kata-kata "Microsoft" seperti http://XX.com/Microsoft.com /freelogin.php pelaku kemudian akan membuat halaman jebakan untuk mendapatkan *username* dan *password* atau informasi berharga lainnya.[14]

b. Menggunakan tanda "@"

Tanda keong (@) sebenarnya digunakan untuk *website* yang membutuhkan autentikasi di mana tanda sebelum tanda @ menunjukkan *username*, sedangkan

[13] Ibid.
[14] Ibid., 149.

setelahnya menunjukkan domain. Contoh sederhana pada email sto@jasakom.com.[15]

Kata "sto" menunjukkan nama sedangkan "jasakom.com" menunjukkan domain. Teknik ini pernah memakan banyak korban dan pernah sangat populer, yaitu http://www.microsoft.com@www.hacker.com. Domain ini jika di klik oleh pengguna maka akan masuk ke situs www.hacker.com, bukan situs Microsoft yang sebenarnya.

c. Nama yang mirip

Teknik yang pernah menimpa situs klikbca.com ini akan membuat nama yang mirip dan memanfaatkan kelemahan *user* yang suka salah ketik atau salah ingat. Sebagai contoh pada kasus klikbca.com, *hacker* bisa membuat *website* kilikbca.com, klickbca.com dan lain sebagainya.[16]

Tentu saja, alamat palsu ini juga dibuat dengan tampilan yang sama persis dengan situs aslinya. Memanfaatkan nama yang mirip tidak harus selalu memanfaatkan kesalahan ketika atau kesalahan ingat. *Hacker* juga bisa membuat nama domain yang tampak asli

[15] Ibid.
[16] Ibid., 150.

seperti microsoft-online.com, microsoft-user.com, dan lain sebagainya.

d. Pemendek URL

Layanan pemendek URL menjadi terkenal dan sering digunakan, sebagai contoh perhatikan URL dari Amazon berikut ini:

http://www.amazon.com/Kindle-Wireless-Reading-Display-Globally/dp/B003FSUDM4/ref=amb_link_353459562_2?pf_rd_m=ATVPDKIKX0DER&pf_rd_s=center-10&pf_rd_r=11EYKTN682A79 =1i=B002Y27P3M

Menghafal alamat yang sedemikian panjang tentu akan sulit dan bahkan hampir tidak mungkin untuk dilakukan kecuali untuk orang-orang jenius. Kini, dengan bantuan layanan pemendek URL, alamat contoh di atas bisa berubah menjadi http://tinyurl.com/KindleWireless.[17]

Karena terbiasa untuk menggunakan layanan semacam ini, banyak orang yang tidak lagi memperhatikan alamat asli yang digunakan. Pelaku *phising* bisa memanfaatkan ini untuk menutupi URL asli yang digunakan.

3. Gambar yang menyesatkan

[17] Ibid., 155.

Pelaku *phising* menggunakan berbagai teknik yang sangat licik untuk mengelabui korbannya, namun URL yang ditampilkan pada *browser* menjadi senjata utama pengguna untuk mengenali alamat palsu.

Adapun *phiser* membuat *address bar* yang menyerupai aslinya, dan *address bar* yang asli di sembunyikan oleh *phiser*, sehingga terlihat seperti URL yang ada pada *browser* semuanya tampak asli dan tidak ada tanda-tanda atau karakter aneh.[18]

4. *Malware Based Phising*

Pada teknik ini, pelaku *phising* memanfaatkan *malware* untuk menyerang komputer pengguna atau korbannya. Kebanyakan *malware* menyebarkan dirinya dengan memanfaatkan situs-situs yang memberikan *software* gratis pada penggunanya. Pelaku juga sering kali membuat *software* yang diklaim akan menghilangkan registrasi atau menjalankan aktivasi program populer seperti Adobe atau Microsoft namun kenyataannya adalah instalasi program *malware* ke dalam komputer korbannya.[19]

Malware yang telah di *install* ke dalam komputer korban, bisa melakukan banyak hal sesuai dengan keinginan pelaku *phising*. beberapa fungsi yang sering dijadikan adalah:

[18] Ibid., 156.
[19] Ibid., 159.

a. *Keylogger*, yaitu aksi mencuri ketikan *keyboard* komputer korban untuk mendapatkan *password* atau informasi berharga lainnya.

b. *Screen Logger,* yaitu aksi mencuri tampilan layar yang bisa digunakan untuk melihat apa yang sedang ditampilkan di depan monitor komputer korban.

c. *Web Trojan,* di sini *malware* yang telah di *install* dalam komputer korban, akan memunculkan *pop up window* seakan-akan berasal dari *website* yang sedang dikunjungi. Sebagai contoh, anda mengunjungi website bank.com dan tiba-tiba muncul *pop-up* yang meminta anda memasukkan kembali *username* dan *password*. Beberapa *malware* suka menggunakan cara ini karena membuat pengguna menyalahkan *website* yang mereka gunakan, padahal *pop-up* tersebut berasal dari *malware* yang ada di dalam komputer korban.

5. *Search Engine Phising*

Biasanya pelaku *phising* secara aktif mengirimkan email atau memanfaatkan *malware* untuk mengarahkan anda ke tempat yang telah disediakan. *Search Engine Phising* menggunakan cara yang berbeda lagi. Pelaku *phising* menyiapkan *website* tipuan dan menunggu *websitenya* di *index* oleh *search engine* seperti Google,

Yahoo, Bing dan lain sebagainya. Setelah di *index* oleh *search engine*, pelaku *phising* tinggal menunggu korban mengunjungi *websitenya*.[20]

Supaya efektif, pelaku *phising* biasanya mempelajari SEO (*search engine optimization*) yaitu suatu metode yang digunakan agar *websitenya* di *index* dan mendapatkan posisi yang bagus pada saat dilakukan suatu pencarian. *Website search engine* seperti Google, Yahoo, Bing dan lain sebagainya menjadi tempat yang diandalkan untuk melakukan pencarian informasi karena itu, pelakunya biasanya memanfaatkan metode-metode yang digunakan oleh *search engine* ini dalam menilai atau merangking suatu *website*.

Pelaku *phising*, menyiapkan *website* tipuan dan mengharapkan pengguna yang mempercayai *website* tersebut akan melakukan tindakan yang diharapkan seperti membeli barang, memasukkan emailnya dan lain sebagainya.[21]

D. Contoh Kasus *Cyber Crime* dalam Bentuk *Phising* di Indonesia

Kasus *cyber crime* dalam bentuk *phising* yaitu kasus perusakan fasilitas *Internet Banking* Bank Central Asia (BCA) pada situs www.klikbca.com dengan cara melahirkan lima nama situs pelesetan yang mirip situs aslinya, adapun nama situs pelesetan yang dibuat *hacker* yaitu *kilkbca.com*, *wwwklikbca.com*, *clikbca.com*, *klickbca.com* dan *klikbac.com*.

[20] Ibid., 161.
[21] Ibid., 162.

sehingga apabila nasabah yang menggunakan fasilitas *Internet Banking* BCA salah mengetik nama situsnya (klikbca.com) seperti lima nama situs pelesetan tersebut, yang terjadi adalah nasabah akan dibawa pada situs palsu buatan *hacker* tadi, selanjutnya si nasabah pun tak bisa bertransaksi, sementara *Personal Identification Number* (PIN) milik nasabah terekam di situs palsu tersebut.[22]

Pelaku *phising* pada *Internet Banking* klikbca.com adalah Steven Haryanto, ia berhasil melakukan tindakan *phising* ini dengan merekam 130 *user ID* dan *Personal Identification Numbers* (PIN) milik nasabah Bank Central Asia.

Tindakannya tersebut tidak dimaksudkan untuk menarik keuntungan, tetapi hanya menguji kemampuannya dan mengukur sampai berapa banyak pengguna internet yang akan terjebak ke situs buatannya. Dalam konteks sistem hukum pidana tindakan pelaku sudah dapat dimasukkan sebagai tindak pidana karenanya pelaku dapat dipidana. Namun karena pada saat itu belum terbentuknya undang-undang yang mengatur tentang *cyber crime* maka tindakan Steve Haryanto tidak dapat dihukum.[23]

Kasus *cyber crime* dalam bentuk *phising* yang terbaru adalah pencurian yang dilakukan oleh seorang *hacker* yang berasal dari Ukraina, *hacker* tersebut berhasil mengambil uang senilai 130 miliar rupiah dari 300 rekening nasabah bank di Indonesia. Di mana *hacker* tersebut melakukan

---

[22] Majalah Tempo, "Rubrik Teknologi Informasi", (24 Juni 2001) dikutip dari Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law...,* 88.
[23] Ibid., 93.

kejahatannya dengan cara memanipulasi *website internet banking*, sehingga pengguna aplikasi yang *login* pada *website internet banking* palsu ini, transaksi yang dilakukan oleh nasabah tidak sesuai dengan yang diinginkan oleh nasabah, melainkan diarahkan kepada rekening orang lain yang telah bekerja sama dengan *hacker*, karena *hacker* berasal dari luar negeri sehingga tidak dapat membuka rekening Indonesia.[24]

Direktur Tindak Pidana Ekonomi dan Khusus (Dirtipideksus) Brigjen Victor Simanjuntak mengungkapkan, pihaknya sedang mengusut kasus tersebut. Sesuai data Bareskrim, cara yang dilakukan *hacker* Ukraina tersebut adalah menyebarkan virus ke komputer seluruh nasabah. Cara penyebaran virus bermacam-macam, ada yang menyebarkan melalui email dan ada pula yang memalsukan software. Akibatnya, nasabah bank bisa secara tidak sengaja *mendownload software* yang ternyata virus.

E. *Cyber Crime* dalam Bentuk *Phising* Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Indonesia memiliki undang-undang *cyber law* pertamanya yang disusun oleh Departemen Komunikasi dan Informatika dan disetujui oleh Dewan Perwakilan Rakyat untuk mulai diundangkan semenjak tanggal 25 Maret 2008. Undang-undang nomor 11 Tahun 2008 ini dikenal dengan nama Undang-Undang ITE atau Undang-Undang Informasi dan Transaksi Elektronik. Dengan diberlakukannya undang-undang ini, maka berbagai jenis

[24] Idr, "*Hacker* Sedot Rp 130 Miliar dari Rekening 300 Nasabah", *Jawa Pos,* (14 April 2015), hlm 1.

tindakan kriminal di dunia maya dapat dikenakan sanksi secara perdata maupun pidana.[25]

Kriminalisasi *cyber crime* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdiri atas perumusan tindak pidana dan perumusan sanksi pidana. Dalam hal perumusan tindak pidana pada dasarnya perbuatan pokoknya sama dengan pengaturan dalam KUHP, hanya dalam lingkupnya adalah dunia maya. Sedangkan dalam hal sanksi pidana pada dasarnya terdapat pemberatan sanksi dibanding KUHP, selain itu juga diatur mengenai kejahatan korporasi.[26]

Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat 10 Pasal yang menyimpan ancaman sanksi pidana bagi pelanggarnya, yakni mulai dari Pasal 27 sampai dengan Pasal 37.

Hal-hal yang diancam dengan sanksi pidana antara lain adalah:[27]

1. Perbuatan mendistribusikan, mentransmisikan, dan/atau membuat dapat diakses informasi elektronik dan/atau dokumen elektronik yang memiliki muatan:
    a. Melanggar kesusilaan;
    b. Perjudian;
    c. Pemerasan dan/atau pengancaman (ditujukan untuk umum);
2. Perbuatan menyebarkan:

[25] Richardus Eko Indrajit, *Konsep dan Strategi...*, 14.
[26] Budi Suhariyanto, *Tindak Pidana...,* 181.
[27] Shidarta, "Catatan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", *Jurnal Komunikasi Universitas Tarumanegera,* I (Januari, 2009), 80.

a. Berita bohong dan menyesatkan sehingga merugikan konsumen dalam transaksi elektronik;
b. Rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan SARA;

3. Perbuatan mengirim pesan ancaman kekerasan dan/atau menakut-nakuti pribadi tertentu;
4. Perbuatan sengaja dan tanpa hak mengakses komputer dan/atau sistem elektronik pihak lain;
5. Perbuatan sengaja dan tanpa hak mengintersepsi atau menyadap informasi elektronik dan/atau dokumen elektronik milik orang lain;
6. Perbuatan sengaja dan tanpa hak mengubah, menambah, mengurangi, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi elektronik dan/atau dokumen elektronik milik orang lain;
7. Perbuatan sengaja dan tanpa hak mengganggu sistem elektronik, sehingga sistem tersebut tidak dapat bekerja sebagaimana mestinya;
8. Perbuatan sengaja dan tanpa hak memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang khusus untuk memfasilitas perbuatan-perbuatan pidana yang telah disebutkan di atas; dan
9. Perbuatan sengaja dan tanpa hak memanipulasi informasi elektronik dan/atau dokumen elektronik agar dinilai seolah-olah otentik.

Cyber crime adalah jenis tindak pidana yang sulit dideteksi. Tidak seperti kejahatan konvensional biasa, korban kejahatan pada umumnya tidak menyadari bahwa ia telah menjadi korban. Walau mereka mengetahui telah menjadi korban, umumnya mereka tidak melaporkan karena beranggapan bahwa hukum yang ada belum dapat menjerat pelaku, kurangnya pengetahuan aparat hukum mengenai perkembangan teknologi sehingga kurang dapat mengantisipasi perkembangan kejahatan ini, juga karena menganggap pembuktian telah terjadi kejahatan di depan pengadilan sangatlah sulit.[28]

Kejahatan terhadap komputer dan program komputer (termasuk *cyber crime*) merupakan kejahatan yang sulit dibuktikan, karena dalam Pasal 184 KUHAP telah diberikan pembatasan berbagai alat bukti yang sah yang dapat digunakan sebagai dasar pertimbangan hakim dalam memberikan putusan.[29]

Hal lain yang penting dalam pengaturan UU-ITE (Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik) adalah ditetapkannya informasi elektronik, dokumen elektronik, dan hasil cetaknya sebagai alat bukti hukum yang sah. Dengan demikian, tidak ada lagi kontroversi tentang apakah rekaman suara, video, email, atau struk bukti transaksi di anjungan tunai mandiri (ATM), untuk dipakai sebagai alat bukti di pengadilan.[30]

---

[28] Niniek Suparni, *Cyberspace Problematika & Antisipasi Pengaturannya,* (Jakarta: Sinar Grafika, 2009), 122.
[29] Ibid., 124.
[30] Shidarta, *Jurnal Komunikasi Universitas Tarumanegera,* I (Januari, 2009), 77.

Dengan telah diberlakukannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka telah secara sah berlaku pula alat bukti elektronik pada tahap penyidikan, penuntutan dan pemeriksaan sidang pengadilan, terhadap setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang tersebut, baik di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.[31]

Adapun pengaturan alat bukti terdapat dalam Pasal 44 yaitu:

Alat bukti penyidikan, penuntutan dan pemeriksaan disidang pengadilan adalah sebagai berikut:

a. Alat bukti sebagaimana dimaksud dalam ketentuan perundang-undangan, dan;
b. Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Adapun penjelasan dalam Pasal 44 huruf b sebagai berikut:

Pasal 1 angka 1

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 sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Pasal 1 angka 4

Dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem

[31] Niniek Suparni, *Cyberspace Problematika*..., 127.

> elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
>
> Pasal 5
>
> (1) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
> (2) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.
> (3) Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini.

Jika melihat dari pengertian *cyber crime* dalam bentuk *phising* sebelumnya, terdapat unsur adanya penipuan dan juga melakukan plagiat dalam hal tampilan *website* yang menyerupai aslinya.

Penyebaran berita bohong dan menyesatkan merupakan padanan kata yang semakna dengan penipuan. Penipuan dapat dilakukan dengan motivasi, yaitu untuk menguntungkan dirinya sendiri atau paling tidak untuk menguntungkan dirinya sendiri dan merugikan orang lain secara sekaligus. Dengan motivasi-motivasi tersebut maka penyebaran berita bohong dan penyesatan dapat dikategorikan sebagai penipuan.[32]

Secara umum penipuan itu telah diatur sebagai tindak pidana dalam Pasal 378 KUHP yang berbunyi:

> Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat atau rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberikan utang maupun menghapuskan

[32] Budi Suhariyanto, *Tindak Pidana...*, 124.

piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun.

Menurut Soesilo yang dimaksud dengan "tipu muslihat" dalam Pasal tersebut adalah suatu tipu yang demikian liciknya, sehingga seorang yang berpikiran normal dapat tertipu. Sedangkan pekerjaan penipu adalah membujuk orang supaya memberikan barang, membuat utang atau menghapuskan piutang.[33]

Perbuatan mengutak-atik komputer dapat ditafsirkan sebagai perbuatan "menyesatkan" yang ada dalam delik penipuan dalam Pasal di atas. Sebagai ketahui penipuan termasuk "membuat utang" atau "menghapus utang", jadi termasuk benda tidak berwujud (hak), berbeda dengan delik pencurian, penggelapan dan lainnya yang syaratnya benda berwujud.[34]

Adapun dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pengaturannya terbatas dalam hal transaksi elektronik. Sebelumnya bagian ini (transaksi elektronik) tidak mempunyai payung hukum, tapi kini makin jelas sehingga bentuk-bentuk transaksi elektronik sekarang dapat dijadikan sebagai alat bukti elektronik sah.[35]

Namun tetap saja dalam pengaturannya masih memiliki keterbatasan, yaitu terletak kepada hubungan transaksi elektronik, yaitu antara produsen dan konsumen serta dalam lingkup pemberitaan bohong dan penyesatan

[33] R. Soesilo, *Kitab Undang-Undang Hukum Pidana,* (Bogor: Politeia, 1991), 261.
[34] Niniek Suparni, *Cyberspace Problematika*..., 144.
[35] Budi Suhariyanto, *Tindak Pidana*..., 126.

melalui internet. Jika merugikan konsumen, pemberitaan bohong tersebut dapat dijerat dengan Pasal 28 ayat (1) sebagai berikut:[36] "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik".

Dan diancam dengan sanksi pidana dalam Pasal 45 ayat (2) yang menentukan: "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama (6) enam tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah)".

Sedangkan dalam hal pelanggaran hak cipta yang ada dalam perbuatan *cyber crime* dalam bentuk *phising*, yang mana perbuatannya adalah membuat tampilan yang mirip dengan aslinya, juga diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Pasal 35 sebagai berikut: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik".

Unsur sengaja dalam Pasal tersebut menurut keterangan Menkominfo dan Menhukham pada persidangan Mahkamah Konstitusi adalah pelaku harus menghendaki perbuatannya memanipulasi data agar seakan-akan data tersebut

[36] Ibid.

otentik. Sedangkan yang dimaksud "dokumen elektronik tersebut dianggap seolah-olah data yang otentik" adalah data tersebut akurat dan relevan.[37]

Dan perbuatan tersebut diancam dengan sanksi pidana dalam Pasal 51 ayat (1) yang menentukan: "setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar)".

Juga diancam dengan sanksi pidana dalam Pasal 52 ayat (2) dan (3) sebagai berikut:

Pasal 52 Ayat (2) yaitu "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"

Pasal 52 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 badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

[37] Muchammad Nashir, "Tinjauan Hukum Pidana Islam terhadap *Cyber Crime* dalam Bentuk *Spam*" (Skripsi—IAIN Sunan Ampel, Surabaya, 2010), 45.