BAB IV

PEMBAHASAN

A. Tindak Pidana Phising

1. Gambaran Umum

Phising adalah suatu kejahatan jenis baru dalam dunia maya. Baru, dalam artian bahwa kejahatan ini terlahir dari bentuk kejahatan cyber yang sudah lama ada, yaitu *hacking*. Walaupun dikatakan sebagai bentuk kejahatan baru nyatanya phising sudah banyak terjadi di dunia maya, dan banyak pula yang menjadi korbannya.

Sebelum dijelaskan tentang phising, marilah kita membahas tentang sistem keamanan dalam dunia maya terlebih dahulu. Dunia maya merupakan suatu dimensi dimana semua orang dapat berinteraksi di dalamnya. Hal ini disebabkan oleh sifat dunia maya itu sendiri yaitu anonimitas (*anonymity*). Melalui anonimitas ini setiap orang dapat turut ambil bagian untuk melakukan interaksi, tanpa harus mengetahui usia, jenis kelamin, pekerjaan, agama, dan sebagainya. Dunia maya layaknya dunia nyata, dimana beberapa aktifitas dalam dunia nyata seringkali dapat dijumpai dalam dunia maya, seperti jual beli, transfer uang, dan sebagainya. Dengan sifatnya yang anonim tersebut apabila terjadi suatu aktifitas layaknya dunia nyata pada dunia maya (contohnya jual-beli), maka akan sangat beresiko sekali untuk disalahgunakan. Oleh karena itu digunakanlah suatu sistem yang bertujuan untuk meminimalkan resiko penyalahgunaan, yaitu dengan penggunaan *user id* dan *password* untuk melakukan *log in*.

Log in adalah suatu sistem dimana kita harus memasukkan *user id* dan *password* yang tepat untuk dapat mengakses informasi dan berinteraksi di dalam suatu website. *User id* dan *password* dalam *log in* layaknya sebuah anak kunci pada pintu masuk suatu rumah yang terkunci, dimana hanya sang pemilik rumahlah yang memiliki kunci tersebut. Dengan kata lain, hanya sang pemilik rumah saja yang berhak masuk ke rumah tersebut. Tanpa kunci yang tepat, seseorang tidak akan dapat memasuki rumah tersebut.

Gambar 4.1

Contoh *Log In* pada facebook.com

Sumber: *Data Sekunder* diolah, 2011

Bagaimana *user id* dan *password* didapatkan, sehingga seseorang dapat melakukan *log in*? *User id* dan *password* biasanya didapatkan melalui registrasi dalam website yang bersangkutan. Dalam form registrasi tersebut biasanya berisi data diri yang meliputi nama asli, tanggal lahir, pekerjaan, pendidikan, dan sebagainya. Setelah data diri tersebut diisikan, maka pendaftar diperkenankan untuk membuat *user id* dan *password*. *User id* merupakan identitas dalam website tersebut, sedangkan *password* merupakan

kata kunci untuk dapat melakukan *log in*. Identitas pada *user id* sifatnya adalah unik, karena dengan identitas tersebut, maka akan dapat membedakan satu orang dengan orang yang lain dalam website tersebut. Sedangkan *password* sifatnya sangat rahasia, sehingga hanya orang yang bersangkutan saja yang tahu. Karena sifat dunia maya yang serba anonim, maka pendaftar diberikan kebebasan untuk menciptakan *user id* dan *passwordnya* sendiri. Hal ini dilakukan dengan harapan hanya ia (pendaftar) sendiri yang tahu tentang informasi tersebut, sehingga sifat kerahasiaan benar-benar terjaga.

Dalam kejahatan phising, informasi rahasia inilah yang dijadikan sasaran. Seperti digambarkan sebelumnya, *user id* dan *password* merupakan anak kunci, sedangkan *log in* merupakan pintu masuk rumah yang terkunci, dimana hanya sang pemilik kunci yaitu tuan rumah lah yang seharusnya memilikinya. Cara paling efektif untuk melakukan pencurian suatu rumah dengan cara yang paling 'bersih' dan tanpa meninggalkan bekas kejahatan adalah dengan mendapatkan anak kunci rumah tersebut. Sehingga manakala sang tuan rumah tidak ada di tempat, maka dengan sangat mudah dan leluasa isi rumah tersebut dapat dijarah. Filosofi seperti inilah yang digunakan dalam phising.

Anak kunci (dalam hal ini *user id* dan *password*) akan berusaha didapatkan pelaku, apapun caranya, tergantung pada kreatifitas sang pelaku. Setelah *user id* dan *password* tersebut didapatkan, maka pelaku akan melakukan *log in* sebagaimana pemilik akun aslinya. Apa yang akan dilakukan pelaku pada akun yang terbobol tersebut dapat bermacam-macam kemungkinannya. Bisa saja ia hanya sekedar iseng, sekedar melihat-lihat isi

akunnya, ataupun menguras habis isinya. Namun, apapun hasil akhirnya, tindakan pelaku itu sudah dapat dianggap sebagai perbuatan phising, dan dapat dikenai ancaman pidana sesuai aturan perundang undangan yang berlaku.

2. Cara Melakukan Phising

a. Pengiriman *E-Mail* Palsu

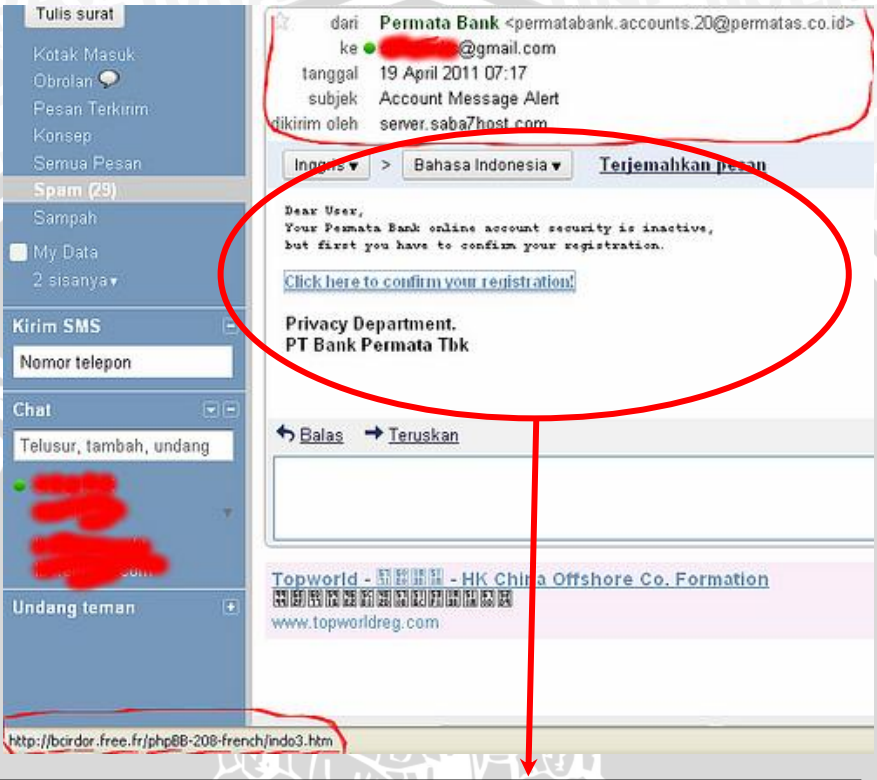
Cara ini merupakan cara yang cukup populer untuk menjerat korban. Pelaku akan mengirimkan sebuah e-mail palsu, dimana ia seolah olah adalah petugas ataupun admin website suatu perusahaan perbankan. Bagaimana cara pelaku dapat mendapatkan alamat e-mail korban sehingga korban dapat dikirimi e-mail palsu tersebut? Ada banyak kemungkinan sebenarnya. Kemungkinan dapat berasal dari searching Internet, mendapatkan keterangan dari kartu nama, melihat dari anggota *mailing list*, dan sebagainya.[35] Isi e-mail palsu tersebut biasanya seputar pemberitahuan kepada nasabahnya tentang suatu hal tertentu yang sifatnya penting, mendesak, dan membutuhkan respon cepat. Untuk membuat korban percaya, maka tampilan e-mail palsu tersebut didesain semirip e-mail aslinya, dengan bahasa, gaya bahasa, kop surat, logo, dan sebagainya. Untuk semakin memudahkan korban terjerat, dalam e-mail palsu tersebut dicantumkan suatu hyperlink yang diharapkan diklik oleh korban, yang apabila diklik akan menuntun korban ke suatu halaman web yang juga sudah dirancang

[35] Richardus Eko Indrajit, 2009, *Seluk Beluk Teknik Social Engineering (online)*, http://www.idsirtii.or.id/content/files/0a9fdab9f5bdccb6b264a6faf35193d6.pdf, (5 April 2011).

sedemikian rupa oleh pelaku. Cara ini kemudian berlanjut pada tahapan selanjutnya, yaitu *web forgery*.

Gambar 4.2

Phising Bank Permata melalui gmail.com



Dear user,

Your Permata Bank online account security is inactive,

but first you have to confirm your registration

Click here to confirm your registration

Privacy Department.

PT Bank Permata Tbk

Sumber: *Data Sekunder* diolah, 2011

b. Web Forgery

Web forgery adalah website / situs yang sengaja dirancang untuk menipu pengunjungnya. Hal ini sering dikenal dengan istilah pharming. Pharming berasal dari kata dalam Bahasa Inggris, *farming* yang berarti memanen. Cara ini diawali dengan pelaku menghost sebuah domain dalam dunia maya, dapat melalui *web hosting* gratis yang dapat dengan mudah ditemui di Internet, maupun jasa *web hosting* yang disediakan oleh perusahaan penyedia jasa internet. Kemudian setelah mendapatkan domain tersebut, pelaku akan merancang sebuah website. Tampilan website ini akan dibuat semirip aslinya, baik tata letak, logo perusahaan, kata-kata, huruf (jenis, ukuran, warna), maupun objek yang disertakan (gambar, suara, maupun animasi) pada website. Kemudian korban akan dituntun untuk memasukkan identitasnya melalui suatu form isian yang sudah disiapkan oleh pelaku. Setelah korban memasukkan *user id* dan *password*-nya, maka data akan tersimpan dalam *database* website palsu tersebut, dan pelaku phising hanya akan tinggal 'memanen' data-data tersebut untuk kemudian disalahgunakan.

c. Phising Melalui Telepon (*Phone Phising*)

Cara ini merupakan pengembangan dari teknik phising secara konvensional. Hanya saja, teknik ini lebih banyak menggunakan media telepon daripada internet. Pelaku akan menelpon pihak yang berwenang dengan menggunakan nama seseorang dengan menggunakan kedok tertentu. Umumnya kedok yang digunakan

pelaku antara lain kedok sebagai *user* penting, kedok sebagai *user* yang sah, kedok sebagai mitra *vendor*, kedok sebagai konsultan audit, kedok sebagai penegak hukum, dan sebagainya.[36]

1) Kedok Sebagai User Penting

Seorang penipu menelpon help desk bagian divisi teknologi informasi dan mengatakan hal sebagai berikut "Halo, di sini pak Abraham, Direktur Keuangan. Saya mau log in tapi lupa password saya. Boleh tolong beritahu sekarang agar saya dapat segera bekerja?". Karena takut dan merasa sedikit tersanjung karena untuk pertama kalinya dapat berbicara dan mendengar suara Direktur Keuangan perusahaannya, yang bersangkutan langsung memberikan *password* yang dimaksud tanpa rasa curiga sedikitpun. Si penipu bisa tahu nama Direktur Keuangannya adalah Abraham karena melihat dari situs perusahaan

2) Kedok Sebagai User Yang Sah

Dengan mengaku sebagai rekan kerja dari departemen yang berbeda, seorang wanita menelepon staf junior teknologi informasi sambil berkata "Halo, ini Iwan ya? Wan, ini Septi dari Divisi Marketing, dulu kita satu grup waktu outing kantor di Cisarua. Bisa tolong bantu reset *password*-ku tidak? Dirubah saja menjadi tanggal lahirku. Aku takut ada orang yang tahu *password*-ku, sementara saat ini aku di luar kantor

[36] *Ibid.*

dan tidak bisa merubahnya. Bisa bantu ya?". Sang junior yang tahu persis setahun yang lalu merasa berjumpa Septi dalam acara kantor langsung melakukan yang diminta rekan sekerjanya tersebut tanpa melakukan cek dan ricek. Sementara kriminal yang mengaku sebagai Septi mengetahui nama-nama terkait dari majalah dinding "Aktivitas" yang dipajang di lobby perusahaan dan nomor telepon Iwan diketahuinya dari satpam dan / atau resepsionis.

3) Kedok Sebagai Mitra Vendor

Dalam hal ini penjahat yang mengaku sebagai mitra vendor menelepon bagian operasional teknologi informasi dengan mengajak berbicara hal-hal yang bersifat teknis sebagai berikut: "Pak Aryo, saya Ronald dari PT Teknik Alih Daya Abadi, yang membantu outsource file CRM perusahaan Bapak. Hari ini kami ingin Bapak mencoba modul baru kami secara cuma-cuma. Boleh saya tahu *username* dan *password* Bapak agar dapat saya bantu instalasi dari tempat saya? Nanti kalau sudah terinstal, Bapak dapat mencoba fitur-fitur dan fasilitas canggih dari program CRM versi terbaru". Merasa mendapatkan kesempatan, kepercayaan, dan penghargaan, yang bersangkutan langsung memberikan *username* dan *password*-nya kepada si penjahat tanpa merasa curiga sedikitpun. Sekali lagi sang penjahat bisa tahu nama nama yang bersangkutan melalui berita-berita di koran dan majalah

mengenai produk / jasa PT Teknik Alih Daya Abadi dan nama-nama klien utamanya.

4) Kedok Sebagai Konsultan Audit

Kali ini seorang penipu menelpon Manajer Teknologi Informasi dengan menggunakan pendekatan sebagai berikut: "Selamat pagi Pak Basuki, nama saya Roni Setiadi, auditor teknologi informasi eksternal yang ditunjuk perusahaan untuk melakukan validasi prosedur. Sebagai seorang Manajer Teknologi Informasi, boleh saya tahu bagaimana cara Bapak melindungi website perusahaan agar tidak terkena serangan *defacement* dari *hacker*?". Merasa tertantang kompetensinya, dengan panjang lebar yang bersangkutan cerita mengenai struktur keamanan website yang diimplementasikan perusahaannya. Tentu saja sang kriminal tertawa dan sangat senang sekali mendengarkan bocoran kelemahan ini, sehingga mempermudah yang bersangkutan dalam melakukan serangan.

5) Kedok Sebagai Penegak Hukum

Contoh terakhir ini adalah peristiwa klasik yang sering terjadi dan dipergunakan sebagai pendekatan penjahat kepada calon korbannya: "Selamat sore Pak, kami dari Kepolisian yang bekerjasama dengan Tim Insiden Keamanan Internet Nasional. Hasil monitoring kami memperlihatkan sedang ada serangan menuju server anda dari luar negeri. Kami bermaksud untuk melindunginya. Bisa tolong diberikan perincian kepada

kami mengenai topologi dan spesifikasi jaringan anda secara detail?". Tentu saja yang bersangkutan biasanya langsung memberikan informasi penting tersebut karena merasa takut untuk menanyakan keabsahan atau keaslian identitas penelpon.

d. Phising Melalui SMS (*SMS Phising*)

Telepon genggam merupakan sebuah teknologi yang cukup fenomenal. Dalam beberapa waktu saja penggunanya sudah menunjukkan kenaikan yang cukup signifikan. Hal ini juga dibarengi dengan kenaikan penjualan nomer selular. Fakta ini rupanya juga tak luput dimanfaatkan oleh para kriminal dalam melakukan tindak kejahatan. Melalui metode pengiriman pesan pendek atau SMS, pelaku akan mengirimkan sebuah SMS kepada korban. Bagaimana cara pelaku mendapatkan nomor korban? Dengan menjamurnya counter-counter penjualan pulsa, maka mendapatkan nomor telpon seluler seseorang bukanlah suatu hal yang sulit. Isi dari SMS tersebut umumnya berisi ucapan selamat karena korban telah memenangkan undian tertentu yang hadiahnya umumnya berupa uang dengan nominal yang relatif besar. Untuk dapat mengambil hadiah tersebut, korban diharapkan mengkonfirmasi dengan cara memberikan user id dan password internet bankingnya kepada pelaku.

Contoh SMS phising:

"Selamat. Anda baru saja memenangkan hadiah sebesar Rp 25,000,000 dari Bank X yang bekerjasama dengan provider telekomunikasi Y. Agar kami dapat segera mentransfer uang tunai

kemenangan ke rekening bank anda, mohon diinformasikan user name dan passoword internet bank anda kepada kami. Sekali lagi kami atas nama Manajemen Bank X mengucapkan selamat atas kemenangan anda…"

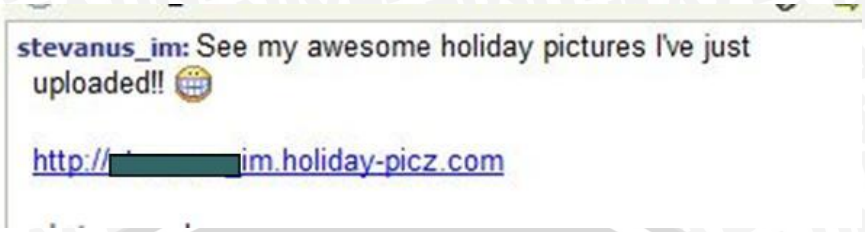
e. Phising Melalui Aplikasi Percakapan (*Chat Phising*)

Dalam cara ini, pelaku akan menyiapkan sebuah program otomatis. Program ini dapat disisipkan pada aplikasi *chatting* populer seperti Yahoo! Messenger, MSN Messenger, dan lain sebagainya. Cara ini juga dapat ditemui pada layanan *customer service online* sebuah perusahaan. *Customer service online* adalah sebuah layanan yang disediakan oleh perusahaan kepada pelanggannya apabila terjadi suatu keluhan atau permasalahan, ataupun sekedar mencari informasi secara online. Umumnya suatu *customer service online* berbasis *chatting*.

Apabila disisipkan pada sebuah aplikasi *chatting* (dalam contoh ini menggunakan Yahoo! Messenger), maka pelaku akan menampilkan sebuah pesan pada korbannya dengan disertai sebuah *hyperlink*. Pesan tersebut biasanya berisi tentang seseorang yang telah mengunggah suatu gambar yang akan membuat korban merasa penasaran. Untuk mengetahui gambar tersebut, maka korban diharuskan mengklik *hyperlink* yang tersedia.

Gambar 4.3

Pesan Phising pada Yahoo! Messenger

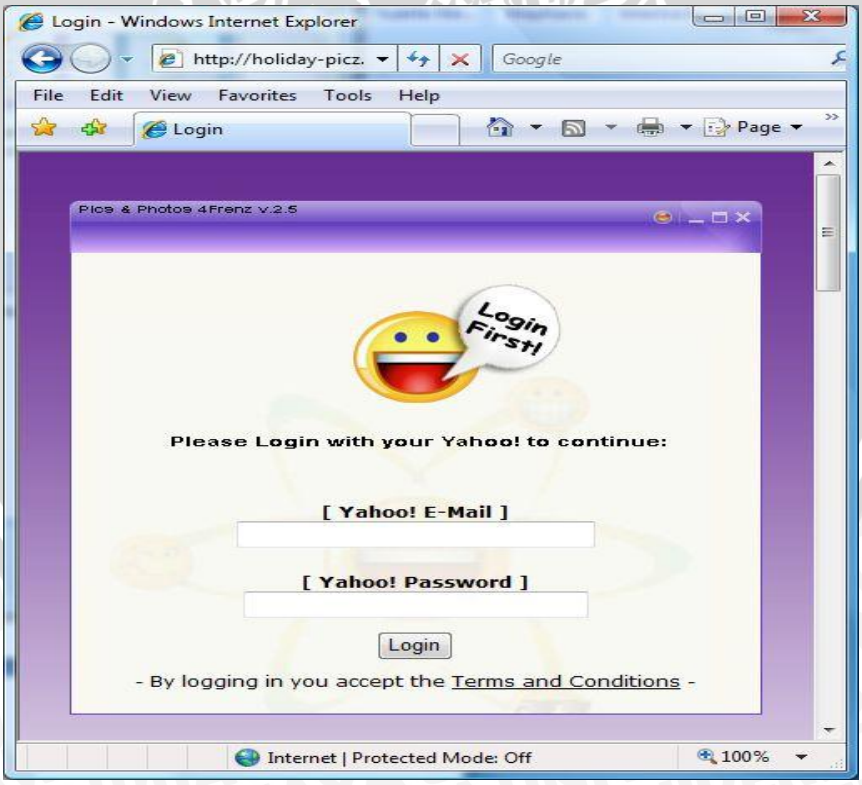


Sumber: Data Sekunder diolah, 2011

Namun setelah *hyperlink* tersebut diklik, bukannya gambar yang dimaksud yang keluar, tapi tampilan yang menyatakan ia harus *log in* kembali agar dapat mengakses gambar tersebut.

Gambar 4.4

Log In Palsu Setelah Hyperlink Diklik



Sumber: *Data Sekunder* diolah, 2011

Apabila korban terpancing pada jebakan tersebut, maka ia akan memasukkan *user id* beserta *password*-nya, dan tercapailah tujuan si pelaku.

Apabila disisipkan pada layanan *customer service online* sebuah perusahaan, maka pelaku juga akan menyisipkan sebuah program otomatis dimana pada setelah beberapa waktu berjalan, korban akan diberikan sebuah tampilan yang menyatakan bahwa koneksi terputus karena ada perbaikan jaringan, dan korban dipersilahkan mengisikan keluhannya tersebut pada suatu form isian. Di bawah ini akan dicontohkan phising pada suatu layanan *customer service online* pada sebuah perusahaan.

Gambar 4.5

Tampilan Awal Customer Service Online Palsu

Sumber: Data Sekunder diolah, 2011

Ini adalah tampilan awal pada sebuah *customer service online*. Tidak ada yang mencurigakan pada tampilan ini. Korban diminta memasukkan *user id* dan *password* terlebih dahulu. Dari sini

sebenarnya korban sudah masuk dalam jebakan pelaku. Tahapan berikutnya hanyalah kedok agar korban tidak merasa dijebak dalam phising.

Gambar 4.6

Customers Service Online Palsu Meminta Korban Menunggu

Welcome Tom! Please hold while we contact a representative. If a representative does not respond in a few seconds, then he/she is not available at this time.

Sumber: Data Sekunder diolah, 2011

Setelah *user id* dan *password* dimasukkan, muncullah tampilan berikutnya. *Customer service online* akan meminta korban menunggu beberapa saat untuk kemudian disambungkan dengan petugas yang berwenang.

Gambar 4.7

Customer Service Online Palsu Menyatakan

Telah Menyambungkan Korban Dengan Petugas

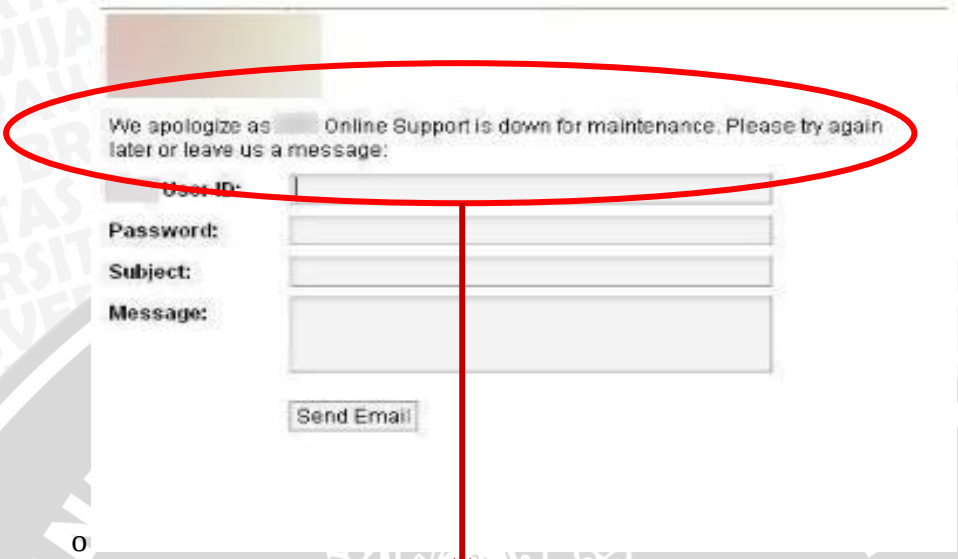
You are now speaking with Sonia Smith of Support Representative

Sumber: Data Sekunder diolah, 2011

Setelah korban menunggu beberapa saat, maka *customer service online* akan menyatakan bahwa korban telah tersambung kepada petugas yang berwenang, dan siap untuk menyampaikan keluhan, permasalahan atau pertanyaannya.

Gambar 4.8

Tampilan Akhir Customer Service Online Palsu



o

We apologize as online support is down for maintenance. Please try again later or leave us a message.

Sumber: Data Sekunder diolah, 2011

Namun setelah tersambung dengan petugas yang berwenang, mendadak tampilan berubah dengan alasan koneksi terputus karena adanya perbaikan. Korban dipersilahkan mengisikan keluhannya pada form yang telah dipersiapkan untuk kemudian ditindak lanjuti. Keluhan yang diisikan tentu saja tidak akan pernah ditindak lanjuti, karena dalam hal ini *customer service online* tersebut memang palsu.

3. Motif Melakukan Phising

a. Mencoba-Coba

Banyak kejahatan terjadi dengan diawali oleh rasa penasaran dan ingin tahu. Semakin ia penasaran, maka semakin ingin ia mencoba melakukannya. Beberapa kasus phising, atau bahkan kasus *cyber*

crime pada umumnya diawali dari coba-coba. Motif mencoba ini biasanya akan berlanjut pada motif ke-2, yaitu mempraktekkan ilmu. Adapun orang yang sekedar iseng, juga dapat dikategorikan dalam motif ini. Karena dari keisengan, akan melahirkan rasa penasaran. Dan rasa penasaran akan menimbulkan keinginan untuk mencoba. Kasus phising klikbca.com pada tahun 2001 adalah berawal dari rasa penasaran Steven Haryanto tentang seberapa aman sistem keamanan online banking Bank BCA.

b. Mempraktekkan Ilmu

Seperti disebutkan sebelumnya, bahwa rasa penasaran akan mendorong pelaku kejahatan untuk mencoba tindakan kejahatan tersebut. Semakin penasaran, maka semakin tertantang pula lah dia untuk melakukannya. Untuk menjawab rasa penasarannya, maka apapun akan dilakukan untuk mencari ilmu tentang bagaimana cara melakukannya.

Beberapa kasus *cyber crime* dilatarbelakangi oleh praktek ilmu. Mereka sebenarnya sadar bahwa perbuatannya melanggar hukum. Tetapi rasa penasaran yang besar rupanya tidak menghalangi mereka untuk mempraktekkan ilmunya. Tutorial yang sangat mudah sekali didapatkan serta mudah digunakan untuk para pemula semakin menguatkan motif ini. Hal ini didasarkan pada fakta bahwa sebagian pelaku *cyber crime* mendapatkan ilmu 'haram' tersebut melalui cara otodidak. Ini artinya bahwa mereka bukanlah orang yang berlatar belakang ilmu komputer atau pemrograman. Mereka hanyalah orang-

orang biasa yang mencoba menjadi bisa dengan cara belajar sendiri melalui bantuan tutorial.

Apabila orang tanpa latar belakang ilmu komputer dapat melakukan *cyber crime* (melalui otodidak), bagaimanakah orang dengan latar belakang ilmu komputer? Apakah mereka juga bisa menjadi pelaku *cyber crime*? Tentu saja jawabnya 'iya'. Sebenarnya mereka yang memiliki latar belakang ilmu komputer pada dasarnya lebih memiliki tanggung jawab moral untuk dapat menggunakan ilmunya pada jalan yang benar, sehingga ilmu tersebut tidak disalahgunakan. Namun kenyataannya ada saja oknum-oknum yang 'bandel' yang tidak memperhatikan kaidah tersebut. Sebaliknya, mereka malah mencari celah dan mencoba mengutak atik celah yang terbuka itu. Sebut saja Dani Firmansyah alias Xnuxer yang pernah mengacak-acak tampilan website KPU pada April 2004[37]. Ia adalah seorang konsultan TI di salah satu perusahaan di Indonesia. Wenas Agusetiawan alias hC yang melakukan aktivitas ilegal terhadap server dua buah perusahaan Singapura pada tahun 2000[38] hingga akhirnya ia ditangkap dan disidangkan di Singapura. Ia adalah seorang yang cukup menguasai teknik komputer, utamanya pemrograman.

Bagaimana dalam kasus phising? Kasus klikbca.com yang cukup fenomenal yang terjadi pada tahun 2001 dilakukan oleh Steven Haryanto. Pada saat itu, Steven merupakan mahasiswa IT, yang nyata-nyata merupakan orang yang cukup 'melek' komputer. Ia juga paham

[37] Merry Magdalena & Mas Wigranto Roes Setyadi, *Cyberlaw, Tidak Perlu Takut*, Penerbit Andi, Yogyakarta, 2007, hal 94.
[38] *Ibid*, Hal 97.

bahwa tindakannya memang melanggar hukum. Tetapi ia melakukan tindakan tersebut karena memang hanya penasaran, sehingga ia akhirnya mencoba perbuatan tersebut. Namun patut diingat bahwa setelah Steven mengetahui kelemahan-kelemahan pada sistem *online banking* Bank BCA tersebut, ia tidak memanfaatkan celah itu demi kepentingan pribadinya. Sebaliknya, ia menyerahkan data-data tersebut kepada Bank BCA untuk kemudian dilakukan beberapa perbaikan.

c. Kriminal

Selain motif coba-coba dan praktek ilmu ada lagi motif yang cukup berbahaya, yaitu motif kriminal. Hal ini cukup jelas bahwa pelaku memang sengaja untuk melakukan tindakan tersebut, dan pelaku juga menghendaki hasil akhir dari perbuatannya tersebut.

Sebelumnya dijelaskan bahwa motif coba-coba diawali dari rasa penasaran. Setelah ia mencoba dan tahu, maka rasa penasaran itu pasti sudah terbayarkan. Manakala rasa penasaan itu sudah hilang, ia akan memutuskan untuk berhenti, atau melakukan tindakan yang lebih jauh lagi. Apabila ia memilih untuk berbuat lebih jauh lagi, terutama karena memanfaatkan situasi demi mencari keuntungan pribadi, maka motif pelaku sudah berubah menjadi motif kriminal. Perbuatan semacam ini tentu saja akan sangat merugikan pihak yang terbobol. Hal ini tentu saja akan berbeda manakala seseorang yang telah mencoba membobol suatu sistem keamanan sehingga ia mengetahui adanya celah pada sistem tersebut, kemudian ia memberikan

informasi, saran dan masukan kepada pengelola website itu untuk kemudian diadakan perbaikan agar tidak terjadi pembobolan. Tindakan semacam ini tentu saja tidak akan merugikan, tetapi menjadi sangat bermanfaat, terutama bagi pihak pengelola website.

Pada motif ini, pelaku umumnya merupakan orang yang sudah berpengalaman di bidangnya. Teknik yang digunakan pun juga sudah rapi dan sistematis, sehingga ia dapat melakukan perbuatannya dengan aman dan sulit dideteksi.

B. Ketentuan Hukum Pidana Di Indonesia Yang Dapat Digunakan Dalam Tindak Pidana Phising

Phising merupakan suatu bentuk kejahatan yang dilarang. Meskipun ia merupakan satu nama, tapi ternyata ia dapat dikelompokkan menjadi beberapa macam perbuatan. Pengelompokan ini didasarkan pada kemungkinan hasil akhir dari kejahatan phising yang dilakukan oleh pelaku. Walaupun begitu, antara perbuatan tersebut dapat dilakukan bersama-sama sebagai satu kesatuan, maupun berdiri sendiri. Namun pada umumnya perbuatan-perbuatan tersebut merupakan suatu kesatuan. Perbuatan tersebut antara lain: penipuan, pemalsuan surat, penerobosan, pencurian.

Dalam hukum pidana Indonesia, perbuatan-perbuatan yang dikategorikan dalam phising tersebut merupakan perbuatan pidana biasa yang diatur dalam Kitab Undang Undang Hukum Pidana (KUHP). Tetapi dengan kekhususan phising sebagai suatu tindak pidana dunia maya, maka sesuai dengan asas *lex specialis derogat lex generalis*, maka aturan yang digunakan bukan lagi ketentuan dalam KUHP, melainkan ketentuan dalam Undang Undang nomor 11 tahun 2008

tentang Informasi dan Transaksi Elektronik. Namun demikian, kepolisian dalam menindak kasus tindak pidana dunia maya ternyata tidak serta merta menggunakan ketentuan dalam UU ITE dan meninggalkan KUHP begitu saja. Kenyataannya, mereka masih tetap banyak berpedoman pada KUHP daripada UU ITE, dengan alasan dan pertimbangan tersendiri.[39]

Tabel 5.1

Peraturan Yang Digunakan pada Phising Dalam KUHP dan UU ITE

No.	Perbuatan	KUHP	UU ITE
1.	Penipuan (*fraud*)	Pasal 378	Pasal 28 ayat (1)
2.	Pemalsuan Surat	Pasal 263 ayat (1)	Pasal 35
3.	Penerobosan (*illegal access*)	-	Pasal 30 ayat (3)
4.	Pencurian (*theft*)	Pasal 362	Pasal 32 ayat (2)

Sumber: *Data Sekunder diolah*, 2011

1. Ketentuan Dalam KUHP

   a. Penipuan (*Fraud*)

   Disebut penipuan dalam phising, dimana pelaku berhasil memperdaya korban untuk percaya akan tipu muslihat pelaku. Hasil yang diharapkan dari tipu muslihat ini adalah diserahkannya *user id* dan *password* dari *internet banking* milik korban.

   Penipuan pada KUHP diatur pada pasal 378.

   Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu; dengan tipu muslihat, ataupun

[39] Wawancara bersama AKP Purnomo HS di Bareskrim Mabes Polri, tanggal 26 Mei 2011

rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama empat tahun.

Unsur penipuan menurut pasal 378 KUHP adalah:

1) Unsur obyektif
   a) Menggerakkan
   b) Orang lain
   c) Untuk menyerahkan suatu barang / benda
   d) Untuk memberi hutang
   e) Untuk menghapuskan piutang
   f) Dengan menggunakan daya upaya seperti
      1)) Memakai nama atau
      2)) Martabat palsu
      3)) Dengan tipu muslihat, dan
      4)) Rangkaian kebohongan
2) Unsur subyektif
   a) Dengan maksud
   b) Untuk menguntungkan diri sendiri atau orang lain
   c) Secara melawan hukum

Menggerakkan dapat didefinisikan sebagai perbuatan mempengaruhi atau menanamkan pengaruh pada orang lain, dimana obyek yang dipengaruhi adalah kehendak seseorang. Unsur menggerakkan orang lain berarti penggunaan tindakan-tindakan, baik berupa perbuatan-perbuatan maupun perkataan-perkataan yang

bersifat menipu.[40] Mengapa menggerakkan harus dengan cara-cara yang palsu dan tidak benar? Karena kalau menggerakkan dilakukan dengan cara yang sesungguhnya, cara yang benar dan tidak palsu, maka tidak mungkin kehendak korban akan menjadi terpengaruh, yang pada akhirnya ia menyerahkan benda, memberi hutang maupun menghapuskan piutang. Tujuan yang ingin dicapai petindak dalam penipuan hanya mungkin bisa dicapai dengan melalui perbuatan menggerakkan yang menggunakan cara-cara yang tidak benar.

Bila dikaitkan dengan phising, maka unsur menggerakkan orang lain terdapat pada saat pelaku mengirimkan e-mail palsu, atau pada saat pelaku menggunakan kedok tertentu (pada *phone phising*). Dengan menggunakan cara-cara tersebut, maka diharapkan korban akan percaya dan terperdaya, sehingga tujuan dari pelaku akan tercapai.

Menyerahkan suatu benda diartikan sebagai menyerahkan suatu barang berwujud. Namun pada perkembangannya, pengertian benda atau barang tidak hanya terbatas pada barang atau benda bergerak saja, tetapi juga termasuk barang tidak berwujud atau tidak bergerak.[41] Menyerahkan suatu benda tidak harus dilakukan sendiri secara langsung oleh korban kepada pelaku. Tetapi juga dapat dilakukan oleh korban kepada suruhan dari pelaku. Penyerahan barang merupakan akibat langsung dari upaya pelaku, sebagai akibat dari adanya unsur

[40] Tongat, *Hukum Pidana Materiil*, UMM Press, Malang, 2003, hal 73.
[41] *Ibid*, hal 18.

kesengajaan si pelaku. Oleh karena itu, perbuatan menyerahkan yang dilakukan oleh korban dan daya upaya dari pelaku harus merupakan suatu hubungan kausal.

Bila dikaitkan dengan phising, perbuatan menyerahkan benda ini terletak pada penyerahan *user id* dan *password*. Bukankah *user id* dan *password* merupakan suatu hal yang abstrak, yang tidak berwujud. Apakah dapat ia disebut sebagai barang, sehingga masuk dalam kualifikasi penyerahan barang? Seperti dijelaskan sebelumnya, pengertian benda telah mengalami perluasan. Sekarang pengertian benda bukan hanya sebatas pada benda berwujud saja, tetapi juga pada benda tidak berwujud. Konsepsi tentang barang menunjuk pada pengertian bahwa barang tersebut haruslah bernilai, tetapi tidak perlu bernilai secara ekonomis.[42] Sehingga dengan kriteria tersebut, *user id* dan *password* yang merupakan suatu informasi berharga dapat dikategorikan sebagai barang, karena pada dasarnya ia sangat bernilai, walaupun tidak bernilai secara ekonomis. Penyerahan *user id* dan *password* dalam phising merupakan akibat langsung dari tipu daya yang dilakukan pelaku. Sehingga jelas bahwa penyerahan dan tipu daya pelaku merupakan suatu hubungan yang bersifat kausal.

Dalam unsur memberikan hutang maupun menghapuskan piutang, berarti terdapat suatu hubungan perikatan antara korban dan pelaku. Memberikan hutang berarti pelaku menipu korbannya untuk seolah-olah membuat perikatan yang menyebabkan si korban

[42] *Ibid.*

membayar sejumlah uang tertentu. Sedangkan menghapus piutang berarti meniadakan perikatan yang sudah ada dari korban kepada pelaku, atau orang tertentu yang dikehendaki pelaku.

Penggunaan nama palsu, atau martabat palsu dimaksudkan untuk menyebutkan jati dirinya dalam suatu keadaan yang tidak benar, yang bertujuan untuk membuat korban percaya, sehingga dengan kepercayaan itu ia akan menyerahkan suatu barang atau memberikan hutang maupun menghapuskan piutang. Memakai nama palsu terjadi apabila pelaku menggunakan nama yang bukan namanya. Sedangkan penggunaan martabat palsu terjadi apabila pelaku menggunakan pangkat, atau jabatan, atau kedudukan yang bukan sebenarnya.

Dalam phising, penggunaan nama palsu ataupun martabat palsu dapat dijumpai pada isi e-mail palsu, maupun pada phone phising atau SMS phising. Dalam e-mail biasanya disebutkan bahwa pelaku atau pengirim adalah petugas suatu divisi dari bank tertentu. Sebagai contoh dalam pengiriman e-mail palsu yang terdapat pada gambar 4.2, pengirim mengaku sebagai petugas dari Privacy Department Bank Permata. Padahal ia sebenarnya tidak bekerja pada bank itu. Dan seringkali divisi dari bank yang diakuinya tersebut tidak pernah ada. Ataupun pada contoh kasus dalam *phone phising*, dimana pelaku mengaku sebagai direktur keuangan sebuah perusahaan yang kebetulan lupa *password* dan meminta informasi tersebut kepada bagian divisi teknologi informasi yang memang menyimpan informasi tersebut dalam databasenya. Pelaku jelas bukanlah direktur keuangan,

dan direktur keuangan yang sebenarnya juga tidak pernah menelpon divisi teknologi informasi.

Unsur penggunaan tipu muslihat seringkali berkaitan dengan unsur rangkaian kebohongan. Tipu muslihat adalah perbuatan sedemikian rupa, sehingga perbuatan tersebut menimbulkan kepercayaan terhadap orang lain (yang ditipu). Sedangkan rangkaian kebohongan adalah rangkaian kata-kata dusta atau kata-kata yang bertentangan dengan kebenaran yang memberikan kesan seolah-olah apa yang dikatakan itu benar.

Dalam phising, penggunaan tipu muslihat dan rangkaian kebohongan merupakan suatu hal yang paling mendasar. Tanpa adanya tipu muslihat serta rangkaian kebohongan, maka hampir pasti kejahatan ini tidak akan terjadi. Tipu muslihat terlihat pada saat pelaku mengirimkan e-mail palsu. E-mail tersebut akan menimbulkan kepercayaan penerimanya, dalam hal ini korban. Hal ini disebabkan isi dari e-mail tersebut merupakan perwujudan atas rangkaian kebohongan. Isinya, pengirimnya, semuanya bohong. Rangkaian kebohongan dalam e-mail palsu tersebut seringkali dapat menyebabkan kesan kebenaran kepada penerimanya, sehingga akan menggerakkan korbannya untuk menyerahkan barang, dalam hal ini *user id* dan *password* yang sangat berharga. Demikian juga pada *phone phising* maupun SMS phising. Kata-kata pelaku untuk meyakinkan korbannya merupakan suatu rangkaian kebohongan.

Unsur dengan maksud merujuk pada adanya suatu kesengajaan. Dalam pasal 378 KUHP, kesengajaan atau maksud ditujukan untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Berkaitan dengan maksud, yang dalam hal ini ditujukan untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, maka untuk itu harus dibuktikan:

1) Bahwa maksud pelaku memang demikian adanya, artinya pelaku memang mempunyai maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum.
2) Kesengajaan harus ditujukan pada menguntungkan diri, juga ditujukan pada unsur lain di belakangnya, seperti unsur melawan hukum, menggerakkan, menggunakan nama palsu dan lain sebagainya.
3) Dengan perbuatan yang dilakukannya itu, pelaku tahu bahwa ia melakukan perbuatan yang melawan atau bertentangan dengan hak orang lain.

Menguntungkan diri sendiri atau orang lain berarti menambah baik bagi dirinya sendiri maupun bagi orang lain, dari kekayaan semula. Bertambahnya kekayaan tidak perlu benar-benar terjadi. Tetapi cukup apabila dapat dibuktikan bahwa maksud pelaku adalah untuk menguntungkan diri sendiri atau orang lain.

Dalam phising, maksud menguntungkan diri sendiri atau orang lain secara melawan hukum merupakan motif utama. Karena tanpa adanya maksud menguntungkan diri sendiri atau orang lain secara

melawan hukum, perbuatan phising tidak akan terwujud. Maksud berarti adanya kesengajaan. Sehingga, pelaku memang menghendaki perbuatannya demi menguntungkan diri sendiri atau orang lain. Pelaku juga tahu dan sadar bahwa perbuatannya itu telah melanggar hak-hak orang lain. Pelanggaran hak dalam phising dapat dilihat dengan timbulnya kerugian baik materiil, maupun imateriil. Kerugian materiil dapat berupa kerugian harta benda yang dapat diukur dengan uang. Misalnya ketika korban mendapati rekening kartu kreditnya telah habis dibobol oleh pelaku. Sedangkan kerugian imateriil berupa kerugian yang tidak dapat diukur oleh uang, tetapi ia pada dasarnya telah mengalami suatu kerugian. Misalnya ketika korban berselancar di dunia maya, kemudian menerima suatu e-mail palsu yang kemudian mengarahkannya ke sebuah website phising. Walaupun ia belum pasti mengalami kerugian keuangan, tetapi ia telah mengalami kerugian waktu, akibat e-mail tersebut.

Unsur melawan hukum berarti perbuatan tersebut bertentangan dengan hukum. Unsur melawan hukum berkaitan erat dengan unsur-unsur lainnya. Hal ini disebabkan karena unsur-unsur sebelumnya harus ditujukan pada unsur melawan hukum. Sebelum melakukan atau setidak-tidaknya ketika memulai perbuatan menggerakkan, pelaku telah memiliki kesadaran dalam dirinya bahwa menguntungkan diri sendiri atau orang lain dengan melakukan perbuatan itu adalah melawan hukum. Melawan hukum di sini tidak semata-mata diartikan sekedar dilarang oleh undang-undang atau melawan hukum formil.

Tetapi harus diartikan secara luas yaitu bertentangan dengan apa yang dikehendaki masyarakat. Karena unsur melawan hukum ini dicantumkan dalam rumusan tindak pidana, maka harus dibuktikan dalam persidangan. Yang harus dibuktikan adalah pelaku mengerti maksud menguntungkan diri sendiri atau orang lain dengan menggerakkan orang lain dengan cara tertentu dan seterusnya sesuai dalam rumusan penipuan tersebut merupakan suatu hal yang dicela masyarakat.

b. Pemalsuan Surat

Pemalsuan surat dalam phising hanya dapat terjadi untuk perbuatan phising yang dimulai dengan pengiriman e-mail palsu saja. Disebut perbuatan pemalsuan surat, ketika pelaku mengirimkan e-mail palsu kepada korban, dimana e-mail tersebut seolah-olah adalah asli dan tidak dipalsu.

Pemalsuan surat dalam KUHP diatur pada pasal 263 ayat (1).

Barangsiapa membuat secara tidak benar atau memalsu surat yang dapat menimbulkan sesuatu hak, perikatan atau pembebasan hutang, atau yang diperuntukkan sebagai bukti dari sesuatu hal, dengan maksud untuk memakai atau menyuruh orang lain pakai surat tersebut seolah-olah isinya benar dan tidak dipalsu, diancam, jika pemakaian tersebut dapat menimbulkan kerugian, karena pemalsuan surat, dengan pidana penjara paling lama enam tahun.

Unsur pemalsuan surat menurut pasal 263 ayat (1) KUHP adalah:

1) Unsur obyektif:
   a) Membuat secara tidak benar atau memalsu
   b) Surat
   c) Yang dapat menimbulkan suatu hak

d) Perikatan

e) Pembebasan hutang

f) Diperuntukkan sebagai bukti dari sesuatu hal

g) Seolah-olah isinya benar dan tidak dipalsu

2) Unsur subyektif:

a) Dengan maksud

b) Memakai atau

c) Menyuruh orang lain pakai

Perbuatan membuat ditujukan pada objek perbuatan, yaitu dalam hal ini adalah surat. Membuat secara tidak benar atau memalsu berarti bermacam-macam hal. Apakah itu palsunya subyek perbuatan, ataupun palsunya obyek perbuatan. Palsunya subyek perbuatan, berarti orang yang membuat adalah orang yang palsu. Palsu dalam artian, ia bukanlah orang yang berwenang untuk membuat. Sedangkan palsunya obyek, berarti dalam benda tersebut memuat hal-hal yang bohong, menyesatkan, dan bukan sebenarnya.

Dalam phising, perbuatan membuat secara tidak benar atau memalsu yaitu pada penggunaan e-mail palsu. Palsunya e-mail berarti dua hal, yaitu palsunya orang yang membuat ataupun palsunya informasi yang termuat di dalamnya. Palsunya orang yang membuat, berarti ia memang bukanlah orang yang berhak untuk membuat e-mail tersebut. Ia tidak berhak, karena memang bukan bagian tugasnya untuk membuat e-mail itu. Sedangkan palsunya informasi yang terkandung di dalamnya, berarti isi e-mail tesebut memuat hal-hal

bohong dan menyesatkan. Umumnya perbuatan memalsu dalam phising adalah baik orang yang membuat dan isinya adalah sama-sama palsu.

Surat merupakan objeknya perbuatan membuat secara tidak benar atau memalsu. Menurut pandangan umum, yang disebut surat adalah sarana komunikasi untuk menyampaikan informasi tertulis oleh suatu pihak kepada pihak lain, yang membutuhkan perangko dan amplop sebagai alat ganti bayar jasa pengiriman. Namun pada perkembangannya, yang disebut surat juga mengalami perkembangan. Seiring dengan dikenalnya internet, maka dikenal surat elektronik atau e-mail (*electronic mail*). E-mail pada dasarnya adalah sama dengan surat konvensional, yaitu sebagai sarana untuk menyampaikan informasi tertulis kepada pihak lain. Hanya saja dalam e-mail tidak membutuhkan perangko dan amplop sebagai sarana pengiriman. Pengiriman e-mail hanya membutuhkan alamat e-mail yang dituju serta adanya koneksi internet.

Dalam phising, pengertian surat bukanlah surat dalam pengertian konvensional. Hal ini disebabkan karena perbuatan phising sangat erat kaitannya dengan dunia maya, sehingga jelas bahwa pengertian surat yang dimaksud bukanlah surat konvensional. Surat di sini adalah surat dalam dunia maya, yaitu e-mail (*electronic mail*).

Unsur yang dapat menimbulkan suatu hak mengisyaratkan telah timbul suatu hubungan perikatan antara korban dan pelaku. Ataupun belum terdapat suatu hubungan perikatan, tetapi dengan adanya surat

tersebut maka akan melahirkan suatu hak tertentu. Perikatan adalah suatu hubungan hukum antara satu pihak dengan pihak yang lain. Suatu perikatan akan menimbulkan suatu hak di satu sisi dan kewajiban di sisi lainnya. Pembebasan hutang berarti pelepasan kewajiban debitur untuk membayarkan pelunasan hutang kepada kreditur. Dalam pembebasan hutang, kehendak untuk membebaskan hutang berasal dari kreditur. Kesemua unsur tersebut, yaitu menimbulkan suatu hak, perikatan dan pembebasan hutang tidak harus selalu dimaknai secara sempit, yaitu hubungan antara pelaku dan korban saja. Tetapi dapat pula dimaknai secara meluas, yaitu korban dengan orang lain yang dikehendaki oleh pelaku.

Unsur diperuntukkan sebagai bukti dari suatu hal berkaitan erat dengan pembuktian dalam persidangan. Menurut ketentuan pasal 184 ayat (1) KUHAP, surat merupakan alat bukti yang sah dalam persidangan. Adapun tidak digunakan sebagai alat bukti dalam persidangan, maka yang dimaksud ‘sebagai bukti’ dapat merupakan bukti telah melakukan suatu hal, misalnya bukti pembayaran.

Seolah-olah isinya benar dan tidak dipalsu mengandung makna telah terdapat suatu upaya yang bersifat manipulatif dari pelaku terhadap objek perbuatan. Adanya kata ‘seolah-olah isinya benar’ mengandung arti bahwa objek tersebut mengandung sebuah kebohongan dan kepalsuan.

Memakai berarti peruntukan obyek adalah bagi dirinya pelaku sendiri. Sedangkan menyuruh orang lain pakai berarti peruntukan

obyek adalah bagi orang selain dirinya pelaku. Kata ‘menyuruh’ berarti adanya sebuah perintah. Pengertian perintah di sini tidak harus selalu dimaknai dengan perintah secara langsung, tetapi juga termasuk perintah secara tidak langsung.

Dalam phising, pemalsuan e-mail ditujukan kepada orang lain. Tidak mungkin apabila e-mail yang palsu itu ditujukan untuk dirinya sendiri, karena sasaran phising adalah orang lain. E-mail palsu yang dikirimkan kepada korbannya seolah-olah adalah perintah dari pelaku kepada korbannya. Memang isi e-mail tersebut bukan merupakan perintah secara langsung. Isi e-mail adalah sebuah informasi yang palsu. Tetapi apabila dicermati lagi, informasi palsu tersebut sebenarnya adalah sebuah perintah secara tidak langsung dari pelaku kepada korbannya untuk melakukan apa yang diinstruksikan dalam e-mail tersebut. E-mail yang berisi pesan “diharap untuk melakukan log in melalui hyperlink ini”, sejatinya sama saja dengan perintah pelaku kepada korbannya sambil mengatakan, “kliklah hyperlink ini, kemudian log in lah”.

c. Pencurian

Dalam phising, pencurian dapat berarti bermacam-macam hal. Pertama, ia mencuri isi dari rekening korban. Setelah pelaku berhasil mendapatkan *user id* dan *password* online banking pelaku, kemudian ia mengambil sebagian atau seluruh uang yang tersimpan dalam rekening korban. Kedua, ia mencuri identitas korban (*identity theft*). Ia

tidak mencuri isi dari rekening korban, tetapi menggunakan identitas tersebut untuk keperluan lain yang menguntungkan pelaku.

Pencurian dalam KUHP diatur pada pasal 362.

> *Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimilik secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau denda paling banyak enam puluh rupiah.*

Unsur pencurian menurut pasal 362 KUHP adalah:

1) Unsur obyektif:
   a) Mengambil
   b) Suatu barang
   c) Yang seluruhnya atau sebagian milik orang lain
2) Unsur subyektif:
   a) Dengan maksud
   b) Untuk memiliki barang / benda tersebut untuk dirinya sendiri
   c) Secara melawan hukum

Unsur mengambil bermakna sebagai setiap perbuatan untuk membawa atau mengalihkan suatu barang ke tempat lain. Awalnya perbuatan mengambil merujuk pada perbuatan yang menggunakan sentuhan tangan. Tetapi perkembangannya, pengertian mengambil mengalami perluasan. Termasuk dalam perbuatan mengambil yaitu perbuatan untuk mengalihkan atau memindahkan suatu barang dengan berbagai cara. Perbuatan dapat disebut sebagai mengambil, manakala perpindahan barang telah terjadi.

Mengambil dalam phising terletak pada saat telah didapatkannya *user id* dan *password* korban oleh pelaku. Hal ini berlaku bagi pencurian identitas pada phising. Dengan *user id* dan *password* yang sudah berada dalam genggaman pelaku, ia dapat dianggap sebagai pemilik akun tersebut. Ketika ia sudah melakukan *log in*, maka ia dapat dengan bebas untuk menggunakan identitas tersebut untuk melakukan apa saja yang ia kehendaki. Pada pencurian rekening, perbuatan mengambil terjadi ketika ia telah melakukan *log in* ke dalam akun rekening korban. Setelah masuk ke dalam rekeningnya, kemudian ia mengambil beberapa atau seluruh uang yang tersimpan dalam rekening tersebut. Akan dipindahkan kemana bukanlah merupakan persoalan, karena berpindahnya uang tersebut sudah memenuhi unsur mengambil.

Unsur suatu barang pada kualifikasi pasal ini sama seperti halnya dengan pengertian barang pada pasal lainnya. Barang yang dimaksud merupakan barang dalam pengertian barang bergerak maupun barang tidak bergerak. Barang yang dapat menjadi objek pencurian adalah barang yang mempunyai pemilik. Sehingga apabila barang tersebut tidak dimiliki oleh siapapun, atau barang tersebut telah dibuang oleh pemiliknya, maka tidak dapat menjadi objek pencurian.

Barang pada phising merujuk pada uang. Uang tersebut merupakan uang yang terdapat dalam rekening orang lain, dalam hal ini rekening korban. Besarnya nilai barang yang menjadi objek phising dapat diketahui dari besarnya uang yang telah tercuri oleh

pelaku. Pada pencurian identitas, barang yang dimaksud adalah akun itu sendiri. Didapatkannya *user id* dan *password* hanyalah sarana untuk mempermudah mendapatkan akun korban.

Unsur seluruhnya atau sebagian milik orang lain mengandung pengertian, bahwa barang yang diambil itu haruslah barang yang dimiliki baik seluruhnya atau sebagian oleh orang lain. Sehingga harus memiliki pemilik, karena barang yang tidak bertuan tidak dapat menjadi objek pencurian. Sebagian atau seluruhnya milik orang lain juga mengandung makna bahwa tidak menjadi syarat apakah barang tersebut milik orang lain secara keseluruhan. Pencurian tetap ada, walaupun barang tersebut milik orang lain dan sebagian milik pelaku itu sendiri.

Dikaitkan dalam pencurian pada phising, seluruhnya atau sebagian milik orang lain berarti dua hal. Pertama, pencurian terhadap uang yang memang merupakan milik orang lain. Dalam hal ini pelaku mengambil, baik sebagian ataupun seluruh uang yang tersimpan dalam rekening korban. Sedangkan yang kedua, pelaku dan korban sebenarnya merupakan pemilik bersama dari rekening tersebut. Demi keuntungan pribadinya, pelaku mengambil semua uang dalam rekening tersebut.

Unsur memiliki untuk dirinya sendiri pada dalam rumusan pasal 362 KUHP merupakan terjemahan dari kata *zich toeeigenen*, yang sebenarnya memiliki makna lebih luas daripada memiliki. Namun oleh banyak ahli lebih diartikan sebagai menguasai. Hal ini

disebabkan apabila seseorang mengambil suatu barang milik orang lain secara melawan hukum, maka tidak secara otomatis hak kepemilikan itu beralih pada yang mengambil barang tersebut. Karena pada hakikatnya, hak milik itu tidak dapat beralih dengan cara melawan hukum. Ia belum memiliki barang yang diambilnya, tetapi baru menguasai barang tersebut, yaitu bahwa orang tersebut bertindak seolah-olah sebagai pemilik barang.[43] Disamping alasan tersebut, orang yang mengambil barang itu belum tentu bermaksud untuk memilikinya sendiri. Bisa saja orang tersebut bermaksud untuk memberikannya kepada orang lain.

Dalam phising, setelah pelaku berhasil *log in* ke dalam rekening korban, maka pelaku dapat dikatakan telah menguasai rekening tersebut. Sebagai orang yang menguasai, maka ia dapat berlaku seolah-olah pemilik rekening, termasuk berbuat apa saja terhadap isi rekening tersebut.

2. Ketentuan Dalam UU ITE

a. Penipuan

Dalam UU ITE, penipuan diatur pada pasal 28 ayat (1).

Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

Unsur penipuan menurut pasal 28 ayat (1) UU ITE adalah:

1) Unsur obyektif:

a) Menyebarkan berita bohong dan menyesatkan

[43] *Ibid*, hal 20.

b) Mengakibatkan kerugian konsumen dalam transaksi elektronik

2) Unsur subyektif:

a) Dengan sengaja, dan

b) Tanpa hak

Menyebarkan berita bohong berarti perbuatan menyebarluaskan berita yang bohong dan tidak benar. Dengan ditambahnya unsur menyesatkan pada rumusan pasal, maka penyebaran berita tersebut sarat akan tipu muslihat maupun rangkaian kebohongan. Dengan adanya tipu muslihat maupun rangkaian kebohongan, maka pelaku sebenarnya berusaha untuk menggerakkan korbannya untuk melakukan suatu hal tertentu. Sehingga, unsur menyesatkan berarti sebuah usaha untuk menggerakkan korbannya untuk melakukan suatu hal tertentu.

Pada phising, perbuatan menyebarkan berita bohong dan menyesatkan terlihat pada pengiriman e-mail palsu dan pengiriman SMS phising. Menurut pandangan umum, berita adalah segala sesuatu yang memuat informasi. E-mail palsu maupun SMS phising berisi tentang suatu informasi yang palsu yang ditujukan kepada korbannya. Sehingga isi e-mail palsu maupun isi SMS phising dapat disebut sebagai berita yang dimaksudkan pada rumusan pasal. Isi e-mail maupun SMS yang memuat hal palsu tersebut merupakan suatu tipu muslihat yang bertujuan untuk menggerakkan hati korban untuk

melakukan sesuatu seperti yang diharapkan oleh pelaku, yaitu menyerahkan *user id* dan *password*.

Unsur mengakibatkan kerugian konsumen dalam transaksi elektronik berarti kerugian merupakan hasil paling akhir dari perbuatan pelaku kejahatan. Berdasarkan bunyinya pasal, maka kerugian di sini merujuk pada kerugian materiil, karena hanya disyaratkan tentang kerugian yang terjadi dalam transaksi elektronik saja. Yang dimaksud dengan transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan / atau media elektronik lainnya.

Dalam phising, kerugian merupakan suatu hasil akhir. Kerugian baru dapat dialami setelah dibarengi dengan perbuatan lainnya, yaitu pencurian. Apabila tindakan pelaku hanya sebatas pada penipuan yang mengakibatkan didapatkannya *user id* dan *password* saja, pelaku belum mencuri isi rekeningnya, maka korban belum dapat dikatakan mengalami kerugian. Karena kerugian yang dimaksud adalah kerugian yang bersifat materiil, maka besarnya kerugian tentu saja harus dapat diukur dengan uang. Kerugian ini biasanya terlihat setelah korban mendapati bahwa dirinya secara tidak sadar telah terjerat dalam phising. Pada kasus phising yang umumnya melibatkan instansi keuangan seperti perbankan, kerugian akan tampak secara jelas pada hilangnya sejumlah uang pada rekening korban. Hilangnya uang tersebut bukanlah karena suatu sebab yang dikehendaki, melainkan disebabkan karena dicurinya isi rekening tersebut oleh pelaku phising.

Unsur dengan sengaja merupakan unsur kesengajaan pelaku untuk melakukan perbuatan. Sedangkan unsur tanpa hak berarti pelaku sebenarnya bukan seseorang yang berhak untuk melakukan perbuatan, yaitu menyebarkan berita. Tidak berhaknya pelaku disebabkan karena pelaku memang secara nyata bukanlah orang yang berhak atau berwenang menyebarkan berita tersebut.

Tidak berhaknya pelaku dalam menyebarkan berita pada phising dapat dilihat dari alamat ataupun nama atau jabatan pengirim e-mail. Apabila terdapat unsur kebohongan atau kepalsuan, maka jelas bahwa pengirim bukanlah seseorang yang berhak atau berwenang mengirimkan e-mail tersebut.

b. Pemalsuan surat

Dalam UU ITE, pemalsuan surat diatur pada pasal 35.

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 pemalsuan surat menurut pasal 35 UU ITE adalah:

1) Unsur obyektif:
    a) Manipulasi
    b) Penciptaan
    c) Perubahan
    d) Penghilangan
    e) Pengrusakan
    f) Informasi elektronik dan / atau dokumen elektronik

g) Agar dianggap seolah-olah data yang otentik

2) Unsur subyektif:

a) Sengaja, dan

b) Tanpa hak

c) Melawan hukum

Manipulasi adalah proses rekayasa dengan melakukan penambahan, penghilangan atau pengkaburan terhadap sebagian atau keseluruhan sebuah fakta. Penciptaan adalah proses menjadikan sesuatu dari yang sebelumnya tidak ada menjadi ada. Perubahan adalah proses penambahan atau pengurangan sebagian atau keseluruhan suatu hal. Penghilangan adalah proses menghilangkan sesuatu dari yang sebelumnya ada menjadi tidak ada. Sedangkan pengrusakan adalah proses merubah nilai sesuatu dari yang sebelumnya baik menjadi buruk. Kesemua bentuk perbuatan tersebut ditujukan pada obyeknya perbuatan, yang dalam hal ini adalah informasi elektronik dan / atau dokumen elektronik.

Dalam phising, perbuatan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan ditujukan pada e-mail. Pada penciptaan, pelaku menciptakan sebuah e-mail yang sebelumnya tidak ada, kemudian dikirimkan kepada korbannya. Isi e-mail palsu tersebut mengacu pada e-mail asli. Hal ini dapat juga e-mail asli yang telah dimanipulasi ataupun dirubah isinya, sehingga menjadi palsu. Pemanipulasian atau perubahan bukan pada isi pesan e-mailnya, tetapi pada hyperlink yang disediakan. Apabila hyperlink e-mail asli akan

menuju pada website perbankan yang memang benar-benar asli, maka hyperlink pada e-mail yang telah dipalsukan ini akan menuju pada website palsu yang telah disiapkan oleh pelaku.

Informasi elekronik dan / atau dokumen elektronik merupakan objek dari perbuatan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan yang dilakukan oleh pelaku. 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* dan sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Sedangkan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan / atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas 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.

Informasi elektronik dan / atau dokumen elektronik yang dimaksud dalam perbuatan ini adalah e-mail. E-mail berisi informasi, yang dapat berwujud tulisan, gambar, suara. Informasi dalam e-mail yang telah termanipulasi akan menggiring alam pemikiran korban

sehingga tujuan pelaku tercapai, yaitu korban menganggap bahwa e-mail tersebut adalah asli dan otentik. Sehingga korban akan mengikuti saja perintah pelaku seperti yang diinstruksikan dalam e-mail.

Unsur agar dianggap seolah-olah data yang otentik, mengandung pengertian terdapat suatu perbuatan dari pembuat perbuatan untuk mempermainkan alam pikiran korbannya sehingga korban menganggap bahwa data tersebut adalah otentik. Bentuk perbuatan itu dirumuskan secara limitatif dalam unsur sebelumnya, yaitu manipulasi, penciptaan, perubahan, penghilangan, dan pengrusakan.

Pelaku phising akan berusaha sedemikian rupa sehingga e-mail akan tampak seperti aslinya. Dengan e-mail yang tampak seperti aslinya, maka korban tidak akan curiga dan menganggap bahwa e-mail tersebut adalah asli dan otentik. Dengan demikian, maka tujuan pelaku dalam perbuatan ini akan tercapai.

c. Penerobosan

Penerobosan berarti perbuatan pelanggaran terhadap sesuatu yang sebenarnya dilarang, ditutup, atau tidak boleh dimasuki. Seperti halnya penerobosan rambu dilarang masuk pada rambu lalu lintas. Sebenarnya pengguna jalan dilarang melewati jalan tersebut. Tetapi karena menerobos, ia tetap saja melewati jalan tersebut. Sama halnya pada pengertian penerobosan pada phising. Penerobosan dalam phising terjadi ketika setelah pelaku berhasil mendapatkan *user id* dan *password* korban, ia kemudian melakukan *log in* ke dalam akun tersebut.

Dalam UU ITE, penerobosan diatur pada pasal 30 ayat (3).

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

Unsur penerobosan menurut pasal 30 ayat (3) UU ITE adalah:

1) Unsur obyektif:
   a) Mengakses
   b) Komputer dan / atau
   c) Sistem elektronik
   d) Dengan cara apapun, dengan:
      1)) Melanggar
      2)) Menerobos
      3)) Melampaui
      4)) Menjebol
   e) Sistem keamanan
2) Unsur subyektif:
   a) Sengaja, dan
   b) Tanpa hak, atau
   c) Melawan hukum

Unsur mengakses bermakna melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan. Mengakses dapat dimaknai sebagai perbuatan memasuki suatu sistem elektronik untuk kemudian berinteraksi di dalamnya. Perbuatan mengakses ditujukan pada obyek perbuatan, yaitu komputer dan / atau sistem komputer.

Dalam penerobosan pada phising, perbuatan mengakses terjadi ketika pelaku berhasil melakukan *log in* ke dalam akun korban setelah memperoleh *user id* dan *password* terlebih dahulu. Yang diakses dalam hal ini adalah data yang tersimpan pada sistem elektronik suatu perusahaan perbankan, atau *server*.

Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan. Sedangkan sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan / atau menyebarkan informasi elektronik. Perbedaan antara keduanya yaitu apabila komputer merupakan suatu alat yang menjalankan fungsi sederhana, sedangkan sistem elektronik merupakan serangkaian perangkat yang menjalankan fungsi yang lebih kompleks.

Yang diakses dalam perbuatan penerobosan pada phising adalah sistem elektronik milik suatu bank, atau yang sering disebut sebagai *server*. Pada *server* tersebut termuat segala macam data atau informasi yang berhubungan dengan korban, termasuk akun rekening korban. Dengan diaksesnya *server*, maka akun rekening korban akan segera ditemukan. Setelah berhasil ditemukan, maka pelaku dapat segera melakukan *log in* ke dalam akun tersebut.

Unsur dengan cara apapun berarti yang dimaksudkan adalah segala cara yang dapat dimungkinkan untuk dilakukan. Tetapi

kemudian diperjelas dengan memberikan rumusan perbuatan yang seperti apa yang dimaksud dalam undang-undang. Perbuatan tersebut antara lain melanggar, menerobos, melampaui, dan menjebol. Keempat perbuatan tersebut pada dasarnya adalah sama, yaitu perbuatan melewati sesuatu yang telah telah dibatasi. Hanya saja dalam pengertian menjebol, perbuatan disertai dengan aksi yang terkesan merusak.

Penerobosan dalam phising dilakukan dengan cara yang lain dari yang dirumuskan dalam rumusan pasal. Pelaku hanya melakukan *log in* secara biasa, seolah-olah ia adalah korban, sang pemilik akun tersebut. Sesuai dengan asas legalitas, perbuatan pelaku yang semacam ini tidak memenuhi unsur perbuatan, karena tidak ada kesesuaian dengan wujud perbuatan yaitu melanggar, menerobos, melampaui, atau menjebol. Namun demikian, harap diingat bahwa terdapat kata "dengan cara apapun". Hal ini berarti segala cara yang dimungkinkan untuk dilakukan, termasuk cara-cara diluar ketentuan undang-undang. Sehingga dengan demikian, pelaku akan tetap terjerat sekalipun cara yang digunakannya diluar yang ditentukan dalam undang-undang.

Sistem keamanan adalah sistem yang membatasi akses komputer atau melarang akses ke dalam komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan. Sistem keamanan berfungsi untuk melindungi data

yang terdapat pada komputer dari orang-orang yang tidak berhak untuk mengaksesnya.

Log in pada suatu akun dapat dipandang sebagai salah satu bentuk sistem pengamanan secara sederhana. Fungsi *log in* adalah untuk membatasi suatu informasi dari orang-orang yang tidak berhak untuk mengaksesnya. Yang berhak untuk mengakses adalah sang pemilik aslinya. Dengan pelaku melakukan *log in*, maka pelaku sudah dapat disebut menerobos sistem pengaman.

d. Pencurian

Dalam UU ITE, pencurian diatur pada pasal 32 ayat (2).

> *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.*

Unsur pencurian menurut pasal 32 ayat (2) UU ITE adalah:

1) Unsur obyektif:
    a) Memindahkan atau mentransfer
    b) Informasi elektronik dan / atau dokumen elektronik
    c) Kepada sistem elektronik orang lain yang tidak berhak
2) Unsur subyektif:
    a) Dengan sengaja, dan
    b) Tanpa hak, atau
    c) Melawan hukum

Memindahkan berarti merubah suatu kedudukan dari satu tempat ke tempat yang lain. Dalam dunia maya, yang dapat dipindahkan bukanlah suatu benda yang nyata dan kasat mata. Melainkan

merupakan suatu informasi yang tidak tampak secara kasat mata yang disebut dengan data. Disebut memindahkan atau mentransfer, berarti perbuatan tersebut sudah atau sedang dilakukan oleh pelaku.

Pemindahan dalam kaitannya pada pencurian dalam phising adalah ketika pelaku memindahkan isi dari suatu informasi dalam rekening. Isi suatu rekening tentu saja adalah sejumlah uang yang tersimpan. Sehingga, pemindahan terjadi ketika pelaku memindahkan sebagian atau seluruhnya isi rekening korban ke suatu rekening yang telah ditentukan oleh pelaku. Bisa saja rekening tujuan pada pentransferan itu adalah milik pelaku, atau rekening milik orang lain yang ikut bekerja sama dengan pelaku. Atau bila pada kasus phising yang menggunakan kartu kredit, pemindahan berarti pemindahan kedudukan uang yang semula berada pada rekening korban menjadi suatu bentuk lain yang dikehendaki pelaku. Atau dengan kata lain, penggunaan sejumlah uang korban yang digunakan untuk kepentingan pelaku.

Pencurian pada phising adalah pencurian tentang isi dari informasi elektronik dan / atau dokumen elektronik. Suatu akun akan memuat informasi tentang seberapa banyak uang yang tersimpan pada rekening tersebut. Sehingga, disebut pencurian apabila telah berpindah isi dari informasi akun rekening korban, dalam hal ini adalah sejumlah uang tertentu.

Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah,

menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan / atau menyebarkan informasi elektronik. Dengan ditambahnya kata 'kepada yang tidak berhak', maka mengandung pengertian bahwa pemindahan informasi elektronik dan / atau dokumen elektronik merupakan perbuatan yang dilarang. Dilarangnya perbuatan tersebut karena pemindahan ditujukan pada orang yang memang tidak memiliki hak untuk menerima informasi elektronik dan / atau dokumen elektronik tersebut.

Pada pencurian dalam phising, informasi elektronik dan / atau dokumen elektronik merujuk pada akun nasabah, dalam hal ini milik korban. Informasi elektronik dan / atau dokumen elektronik itu tersimpan pada sistem elektronik yang umumnya disebut *server*. *Server* adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan atau *network operating system*. *Server* juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat pencetak (*printer*), dan memberikan akses kepada *workstation* anggota jaringan[44]. Pendeknya, server adalah sebuah sistem jaringan komputer raksasa yang menyediakan fasilitas-fasilitas tertentu bagi anggota jaringannya. Perbuatan pemindahan

[44] Hadi Wibowo, 2010, *Komputer Server – Pengertian, Jenis dan Fungsi Server (online)*, http://adibowo.com/komputer-server-pengertian-jenis-dan-fungsi-server/, (5 April 2011).

informasi elektronik dan / atau dokumen elektronik ke sistem informasi milik orang lain yang tidak berhak terjadi ketika pelaku memindahkan informasi elektronik dan / atau dokumen elektronik yang tersimpan pada server bank ke dalam sistem informasi miliknya sendiri. Dengan berpindahnya informasi elektronik dan / atau dokumen tersebut ke dalam sistem informasinya, maka ia dapat mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan / atau menyebarkan informasi elektronik yang ia dapatkan tersebut.

Apabila diperhatikan dengan seksama, unsur-unsur pada phising mirip dengan unsur-unsur yang terdapat pada *cybercrime* jenis lainnya, yaitu carding. Carding adalah suatu bentuk kejahatan menggunakan kartu kredit orang lain untuk dibelanjakan tanpa sepengetahuan pemiliknya.[45] Keduanya sama-sama memiliki persamaan yaitu memiliki unsur pencurian. Bedanya apabila phising selain menggunakan unsur pencurian juga menggunakan unsur penipuan. Sedangkan carding tidak menggunakan unsur penipuan sama sekali. Penipuan pada phising tampak jelas pada penipuan tampilan (*visual deception*) yang digunakan untuk memperdaya korbannya. Dalam phising, pelaku kejahatan berbuat secara pasif. Artinya, pelaku cukup menunggu korban terjaring dengan sendirinya. Sebaliknya dalam carding, pelaku berbuat secara aktif. Artinya, pelaku aktif melakukan cara-cara tertentu sehingga dapat membobol kartu kredit seseorang.

[45] Ade Ary Sam Indradi, *Carding: Modus Operandi, Penyidikan dan Penindakan*, Pensil, Jakarta, 2006, hal 4.

C. Pertanggungjawaban Pelaku Phising Sebagai Pemilik Website (Domain)

Untuk dapat dipertanggungjawabkannya seorang pelaku kejahatan, maka ia harus memiliki unsur kesalahan. Kesalahan merupakan ukuran pengenaan pidana, yang pada hakikatnya menempatkan kesalahan sebagai batas pengenaan pidana. Kesalahan merupakan ukuran yang paling menentukan dalam memutuskan bentuk dan lamanya pidana yang tepat bagi seorang pembuat tindak pidana.[46]

Untuk dapat dipersalahkannya seorang pelaku tindak pidana, maka ia harus memenuhi kualifikasi sebagai orang yang dapat dipersalahkan. Untuk dapat disebut sebagai orang yang bersalah, maka ia harus memenuhi unsur kesalahan dalam melakukan perbuatan yang disalahkan itu, yaitu dengan melanggar aturan yang berlaku. Pelaku dalam tindak pidana phising adalah pemilik *domain*. Sebagai pemilik domain, ia bertanggungjawab sepenuhnya atas isi dan materi yang terkandung dalam website. Sehingga dengan demikian, apabila terdapat suatu tindak pidana phising, maka yang harus disalahkan serta dimintai pertanggungjawaban pertama kali adalah sang pemilik domain, atau pelaku itu sendiri.

Seperti dijelaskan sebelumnya, bahwa phising dapat terbagi menjadi beberapa macam perbuatan yang dilarang dalam peraturan perundangan. Perbuatan itu antara lain: penipuan, pemalsuan surat, penerobosan, pencurian.

Penipuan pada phising dikenai aturan pasal 28 ayat (1) UU ITE. Dengan dipenuhinya unsur-unsur pada pasal 28 ayat (1) UU ITE, maka pelaku dapat dikenai pidana penipuan, dan dapat dikenai sanksi pidana yang berlaku. Ketentuan

[46] Chairul Huda, *Dari 'Tiada Pidana Tanpa Kesalahan' Menuju Kepada 'Tiada Pertanggungjawaban Pidana Tanpa Kesalahan'*, Prenada Media, Jakarta, 2006, hal 142.

bagi yang melanggar pasal 28 ayat (1) UU ITE diatur pada pasal 45 ayat (2) UU ITE.

> *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).*

Pemalsuan surat pada phising dikenai aturan pasal 35 UU ITE. Dengan dipenuhinya unsur-unsur pada pasal 35 UU ITE, maka pelaku dapat dikenai pidana pemalsuan surat, dan dapat dikenai sanksi pidana yang berlaku. Ketentuan bagi yang melanggar pasal 35 UU ITE diatur pada pasal 51 ayat (1) UU ITE.

> *Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan / atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).*

Penerobosan pada phising dikenai aturan pasal 30 ayat (3) UU ITE. Dengan dipenuhinya unsur-unsur pada pasal 30 ayat (3) UU ITE, maka pelaku dapat dikenai pidana penerobosan, dan dapat dikenai sanksi pidana yang berlaku. Ketentuan bagi yang melanggar pasal 30 ayat (3) UU ITE diatur pada pasal 46 ayat (3) UU ITE.

> *Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan / atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).*

Pencurian pada phising dikenai aturan pasal 32 ayat (2) UU ITE. Dengan dipenuhinya unsur-unsur pada pasal 32 ayat (2) UU ITE, maka pelaku dapat dikenai pidana pencurian, dan dapat dikenai sanksi pidana yang berlaku. Ketentuan bagi yang melanggar pasal 32 ayat (2) UU ITE diatur pada pasal 48 ayat (2) UU ITE.

> *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).*

Seperti disebutkan sebelumnya, phising apabila dijabarkan terdiri dari beberapa macam perbuatan yang masing-masing dapat saling berkaitan maupun berdiri sendiri. Apabila perbuatan tersebut berdiri sendiri, maka jelas bagi hakim untuk menjatuhkan hukuman bagi pelaku, yaitu seperti yang tercantum dalam rumusan pasal. Akan tetapi permasalahan timbul ketika perbuatan tersebut merupakan suatu perbuatan yang saling berkaitan dan berkelanjutan. Bagaimana hakim menentukan hukuman yang tepat dan memenuhi unsur keadilan bagi pelaku phising? Mengingat pada umumnya dalam kasus phising, perbuatan tersebut merupakan perbuatan yang saling berkaitan.

Dalam hukum pidana dikenal adanya perbarengan tindak pidana (*concursus* atau *samenloop*). Yang dimaksud dengan perbarengan adalah terjadinya dua atau lebih tindak pidana oleh satu orang dimana tindak pidana yang dilakukan pertama kali belum dijatuhi pidana, atau antara tindak pidana yang awal dengan tindak pidana berikutnya belum dibatasi oleh suatu putusan hakim.[47] Perbarengan dalam tindak pidana dibagi menjadi tiga macam, yaitu:

1. Perbarengan peraturan (*concursus idealis* atau *eendaadse samenloop*)
2. Perbuatan berlanjut (*voorgezette handeling*)
3. Perbarengan perbuatan (*concursus realis* atau *meerdaadse samenloop*)

Perbarengan peraturan adalah satu perbuatan yang melanggar banyak aturan. Contohnya seorang laki-laki memperkosa seorang perempuan yang dilakukannya di pinggir jalan raya. Ia melanggar dua aturan sekaligus, yaitu

[47] Adami Chazawi, *Pelajaran Hukum Pidana bagian 2*, PT RajaGrafindo Persada, Jakarta, 2007, hal 109.

memperkosa dan melanggar kesusilaan di muka umum. Perbuatan berlanjut adalah satu rangkaian perbuatan yang terdiri dari beberapa macam perbuatan yang dapat berdiri sendiri, dimana masing-masing perbuatan tersebut timbul dari satu kehendak dasar. Kehendak dasar terbentuk sebelum melakukann tindak pidana yang pertama kali, yang kemudian berlanjut pada tindak-tindak pidana lainnya. Satu kali kehendak dasar diputuskan, maka kehendak itu terus ditujukan pada semua tindak pidana yang akan dilakukan kemudian. Contohnya seorang teknisi di perusahaan perakitan radio yang memutuskan untuk memiliki satu radio dengan mencuri dari perusahaan dimana dia bekerja. Diputuskan caranya yaitu dengan mencuri komponen-komponen yang diperlukan sedikit demi sedikit untuk dirakit menjadi sebuah radio. Apabila komponen-komponen tersebut telah lengkap, maka ia akan merakitnya sendiri menjadi sebuah radio. Ia tidak mencuri sebuah radio karena pencurian tersebut akan segera diketahui, dan hal itu tentu saja tidak diinginkannya. Perbarengan perbuatan adalah beberapa perbuatan yang melanggar banyak aturan, dimana masing-masing perbuatan tersebut tidak saling berkaitan dan berdiri sendiri. Contohnya dalam satu hari, seorang penjahat melakukan bermacam-macam tindak pidana. Pagi hari ia mencopet dompet seseorang di terminal. Siang hari ia menganiaya seorang pria di pasar. Sore hari ia mencabuli seorang anak dibawah umur. Malam hari ia merampok sebuah rumah mewah. Semua perbuatan penjahat itu tidak memiliki keterkaitan, dan dapat berdiri sendiri sebagai beberapa bentuk perbuatan.

Perbarengan yang dimungkinkan dalam phising adalah perbuatan berlanjut (*voorgezette handeling*). Hal ini disebabkan karena perbuatan-perbuatan pada phising merupakan perbuatan yang saling berkaitan, dimana perbuatan-

perbuatan tersebut timbul dari satu kehendak dasar, yaitu pencurian. Untuk mewujudkan pencurian, maka pelaku akan melakukan pemalsuan surat, kemudian dilanjutkan pada penipuan, penerobosan, hingga berujung pada pencurian.

Sistem penjatuhan pidana pada perbuatan berlanjut yaitu menggunakan sistem hisapan (*absorbsi stelsel*). Absorbsi stelsel berarti hanya dipidana terhadap salah satu dari aturan pidana itu, dan jika di antara aturan-aturan pidana itu berbeda-beda ancaman pidananya, maka yang dikenakan adalah terhadap aturan pidna yang terberat ancaman pidana pokoknya. Apabila satu perbuatan itu masuk dalam aturan pidana umum yang sekaligus masuk dalam aturan pidana khusus, maka yang dikenakan adalah terhadap aturan pidana khusus itu saja[48]. Sistem hisapan pada perbuatan berlanjut dibedakan antara sistem hisapan yang umum dan yang khusus. Sistem hisapan yang umum berlaku pada dua kemungkinan, yaitu:

1. Dalam hal perbuatan berlanjut yang terdiri dari beberapa tindak pidana (sejenis) yang diancam dengan pidana pokok yang sama, maka yang diterapkan adalah satu aturan pidana saja (tanpa pemberatan).
2. Dalam hal perbuatan berlanjut yang terdiri dari beberapa tidak pidana (sejenis) yang diancam dengan pidana pokok yang tidak sama beratnya, maka yang diterapkan adalah aturan pidana yang memuat ancaman pidana pokok yang paling berat (tanpa pemberatan).

Sedangkan yang dimaksud dengan sistem hisapan yang khusus, yaitu hanya berlaku khusus dalam pidana yang disebutkan dalam undang-undang. Sistem hisapan yang khusus hanya berlaku pada dua hal, yaitu:

[48] *Ibid,* hal 124.

1. Dalam hal pembuat dipersalahkan karena melakukan tindak pidana pemalsuan uang yang sekaligus digunakannya, atau dalam hal pembuat dipersalahkan karena melakukan tindak pidana perusakan mata uang yang sekaligus digunakannya, maka diterapkan satu aturan pidana saja, tanpa pemberatan.
2. Dalam hal pembuat melakukan kejahatan yang dirumuskan dalam pasal-pasal: 364, 373, 379, dan 407 ayat (1), sebagai perbuatan berlanjut dan jumlah kerugian yang ditimbulkannya melebihi Rp 250,00 maka hanya dijatuhkan satu pidana saja.

Sistem penjatuhan pidana dalam phising menggunakan sistem hisapan yang umum. Menurut ketentuan dalam hisapan umum, maka terjadi dua kemungkinan. Apakah digunakannya satu aturan karena memuat pidana pokok yang sama, ataukah digunakannya aturan yang terberat karena memuat pidana pokok yang berbeda. Dari keempat perbuatan dalam phising, tidak ada satupun perbuatan yang memiliki pidana pokok yang sama. Sehingga, kemungkinan yang paling masuk akal yang dapat diberikan pada pelaku phising menurut sistem hisapan yang umum, yaitu digunakannya aturan yang terberat. Dari keempat perbuatan yang mungkin dilakukan dalam phising, perbuatan pemalsuan suratlah yang memiliki pidana pokok yang paling berat, yaitu pidana penjara maksimum dua belas tahun dan / atau denda maksimum Rp 12.000.000.000,00. Namun demikian, yang berhak menjatuhkan seberapa lamanya hukuman penjara dan / atau denda bagi pelaku adalah hakim, melalui proses persidangan. Hakim dalam menjatuhkan hukuman bagi pelaku tentunya akan membuat bermacam-macam

pertimbangan, sehingga akan menjatuhkan hukuman yang tepat dan tentunya memenuhi rasa keadilan.

D. Pertanggungjawaban ISP Sebagai Penyedia Jasa Internet

Dalam pembahasan sebelumnya, telah dijelaskan bahwa orang tidak dapat langsung berselancar dalam dunia maya. Untuk dapat berselancar ke dalam dunia maya, harus ada pihak perantara yang menjembatani antara pengguna dan dunia maya. Pihak perantara itu disebut dengan ISP (*Internet Service Provider*) atau dalam Bahasa Indonesia disebut sebagai PJI (Penyelenggara Jasa Internet). Penyelenggara jasa internet memberikan jasa untuk menyambungkan pengguna dengan dunia maya, disamping jasa-jasa lain yang disediakan. Kedudukan penyelenggara jasa internet dalam hal ini adalah penting dan vital dalam kaitannya dengan dunia maya.

Kejahatan pada dunia maya merupakan perbuatan orang-orang yang tidak bertanggungjawab yang telah menyalahgunakan fasilitas yang disediakan oleh penyelenggara jasa internet. Pelaku kejahatan dalam dunia maya dapat mempertanggungjawabkan perbuatannya secara hukum melalui peraturan perundang-undangan yang ada. Peraturan perundang-undangan yang khusus mengatur mengenai kejahatan dalam dunia maya adalah Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Apabila pelaku kejahatan dunia maya dapat dipertanggungjawabkan secara hukum, bagaimana dengan pihak penyelenggara jasa internet? Dapatkah penyelenggara jasa internet turut dipidanakan apabila pelanggannya terbukti bersalah melakukan kejahatan dunia maya? Mengingat penyelenggara jasa internet dianggap mampu mengawasi

lalu lintas pertukaran informasi yang terjadi dalam jaringannya, serta mengambil tindakan pencegahan yang dianggap perlu.

Untuk menjawab persoalan tersebut, maka harus diingat bahwa pemidanaan baru dapat terjadi apabila orang yang melakukan tindak pidana dapat dipertanggungjawabkan (asas tiada pidana tanpa kesalahan atau *Geen Straf Zonder Schuld*). Sehingga, yang dapat dipertanggungjawabkan hanyalah orang yang memiliki unsur kesalahan. Unsur kesalahan meliputi kemampuan bertanggung jawab, adanya bentuk kesalahan, dan tidak adanya alasan pemaaf. Unsur kesalahan yang utama dan sangat menentukan adalah adanya bentuk kesalahan, dimana bentuk kesalahan itu berupa kesengajaan atau kelalaian.

Penyedia jasa internet merupakan sebuah subjek hukum yang berbentuk korporasi. Karena bentuknya yang korporasi, maka pembebanan pertanggungjawaban menggunakan sistem pertanggung jawaban korporasi, dimana pertanggung jawaban ada pada pengurus korporasi, baik secara *vicarious liability* maupun *strict liability*. *Vicarious liability* merupakan tanggung jawab yang dibebankan kepada seseorang terhadap perbuatan orang lain atas dasar hubungan hukum antara mereka. Sedangkan *strict liability* adalah tanggung jawab mutlak, yang berarti bahwa seseorang dianggap bertanggung jawab secara hukum terhadap kerugian walaupun orang tersebut tidak memiliki niat untuk melakukan kesalahan, tetapi pada dasarnya ia bersalah karena adanya suatu pelanggaran kewajiban.

Kesengajaan berarti adanya suatu niatan atau kehendak untuk melakukan perbuatan. Niat tersebut tentunya akan segera diwujudkan melalui perbuatan-perbuatan yang menghasilkan suatu tindak kejahatan. Sedangkan kelalaian

merupakan suatu kesengajaan perbuatan dimana hasilnya tidak dikehendaki karena kurangnya kehati-hatian ataupun ketiadaan pemikiran sama sekali. Adanya kesengajaan atau kelalaian harus dibuktikan agar memenuhi syarat adanya kesalahan.

Tiadanya alasan pemaaf berarti tiadanya suatu alasan yang dapat memafkan perbuatan. Alasan pemaaf meliputi ketidakmampuan bertanggung jawab, pembelaan terpaksa yang melampaui batas, dan menjalankan perintah jabatan yang tidak sah dengan itikad baik. Agaknya tidak sulit untuk menentukan ada atau tidaknya alasan pemaaf dalam kaitannya dengan kesalahan. Apalagi penyelenggara jasa internet merupakan sebuah korporasi, dimana alasan pemaaf umumnya hanya terdapat pada subjek hukum manusia saja.

Penyedia jasa internet merupakan perusahaan yang memberikan jasa dan layanan. Sebagai penyedia jasa, mereka membuat suatu ketentuan layanan (*terms of condition*) mengenai pembatasan tanggung jawab. Diantaranya adalah bahwa penyedia jasa internet tidak bertanggung jawab atas isi dari situs pelanggan yang ditempatkan dalam server penyedia jasa internet yang bersangkutan, baik sebagian maupun seluruhnya dan penyedia jasa internet tidak bertanggung jawab atas kerugian dalam bentuk apapun yang diderita pelanggan maupun pihak ketiga lainnya, termasuk dan tidak terbatas pada kehilangan kesempatan untuk mendapatkan keuntungan, kehilangan informasi yang disebabkan oleh hal-hal yang terjadi karena penggunaan layanan yang bukan diakibatkan oleh penyelenggara jasa internet. Dengan ketentuan ini, maka penyedia jasa internet tidak bertanggung jawab terhadap isi dan materi dari setiap website (*domain*) yang menjadi kewajibannya untuk disiarkan pada pengguna. Dengan adanya

ketentuan tersebut maka isi dan materi yang disampaikan oleh setiap website (*domain*) menjadi tanggung jawab pemilik website (*domain*).[49] Sehingga pihak penyedia jasa internet dalam hal ini tidak dapat turut dipidanakan apabila terdapat salah satu pengguna jasanya terbukti melakukan tindak pidana kejahatan dalam dunia maya. Kecuali apabila mereka terbukti turut serta dalam kejahatan tersebut, maka pihak penyedia jasa internet dapat dimintai pertanggungjawabannya secara pidana.[50]

Bahwa kata 'terbukti' harus menjadi fokus pembahasan dalam kaitannya dengan perbuatan penyelenggara jasa internet pada kejahatan dunia maya. Sehingga dengan demikian, ada suatu kesengajaan dari penyedia jasa internet untuk melakukan perbuatan. Maka dalam hal ini siapakah yang harus membuktikan? Pasal 15 ayat (2) Undang-Undang nomor 36 tahun 1999 tentang Telekomunikasi menyatakan:

> *Penyelenggara telekomunikasi wajib memberikan ganti rugi sebagaimana dimaksud pada ayat (1), kecuali penyelenggara telekomunikasi dapat membuktikan bahwa kerugian tersebut bukan diakibatkan oleh kesalahan dan atau kelalaiannya.*

Dengan adanya ketentuan tersebut, maka kewajiban untuk melakukan pembuktian ada di tangan penyelenggara jasa, dalam hal ini adalah penyedia jasa internet. Dengan dikeluarkannya *terms of condition* oleh penyedia jasa internet yang menyatakan bahwa mereka tidak bertanggung jawab terhadap isi dan materi dari website yang dihostingnya dan ketentuan pasal 15 ayat (2) UU Telekomunikasi, maka akan melahirkan suatu hubungan yang kontradiktif,

---

[49] Yunie Chandra Wardhani, *Pertanggungjawaban Pidana bagi Pemilik Website (Domain) yang Menayangkan Gambar-Gambar Porno di Internet*, Skripsi tidak diterbitkan, Malang, Fakultas Hukum Universitas Brawijaya, 2007, hal 66.

[50] Wawancara bersama AKP Purnomo HS di Bareskrim Mabes Polri, tanggal 26 Mei 2011.

dimana pertentangan tersebut terkesan lebih menguntungkan penyedia jasa internet daripada masyarakat umum sebagai pengguna internet.

Memang maksud dikeluarkannya ketentuan layanan (*terms of condition*) adalah sebagai dasar untuk melindungi hak-hak penyelenggara jasa dari kemungkinan terjadinya kesewenang-wenangan konsumen. Tetapi nyatanya, ketentuan layanan yang demikian itu malah terlalu menguntungkan penyelenggara jasa sendiri. Penyelenggara jasa dapat berdalih bahwa tidak mungkin mengawasi semua aktivitas atau lalu-lintas arus pertukaran informasi yang terjadi dalam server mereka. Bahwa keuntungan dan biaya pengeluaran atas pengawasan sangat tidak berimbang, sehingga pengawasan tidak dilakukan karena tingginya biaya pengeluaran. Serta beragam dalih lainnya. Tetapi kemudian ternyata ketentuan layanan yang demikian itu dieksploitasi demi kepentingan penyelenggara jasa dengan membiarkan saja segala macam aktivitas yang terjadi dalam server mereka, termasuk membiarkan aktivitas kejahatan dalam dunia maya.

Undang-undang melalui ketentuan pasal 15 ayat (2) UU Telekomunikasi memberikan kesempatan seluas-luasnya untuk membuktikan bahwa penyelenggara jasa tidak bersalah. Tetapi ketentuan layanan yang mereka buat terkesan tidak mau untuk ikut bertanggung jawab apabila terjadi suatu permasalahan. Logikanya, bagaimana mereka mau membuktikan apabila mereka sudah menyatakan bahwa tidak mau turut dipertanggungjawabkan terlebih dahulu. Dengan adanya aturan yang demikian, maka seakan-akan hanya kepentingan penyedia jasa yang didahulukan, sementara kepentingan konsumen tidak dihiraukan. Dengan adanya ketimpangan ini, maka perlu diadakan perbaikan dalam rumusan perundangan sehingga antara peraturan perundangan dan

penyelenggara jasa dapat berjalan selaras. Dengan adanya perbaikan, diharapkan peraturan yang ada tidak lagi terkesan berat sebelah, sehingga rasa keadilan pun tercapai.

Terlepas dari hubungan yang timpang tersebut, undang undang telah menyatakan bahwa kewajiban pembuktian ada di tangan penyelenggara jasa, yaitu penyedia jasa internet. Apabila terbukti bersalah, maka penyedia jasa internet dapat dipertanggung jawabkan secara pidana. Terbukti bersalahnya penyedia jasa internet dapat berarti dua kemungkinan, apakah penyedia jasa internet berperan sebagai pelaku tunggal, dalam artian ia tidak bekerja sama dengan pihak lain, ataukah ia bekerja bersama-sama dengan pihak lain (pidana penyertaan).

Penyedia jasa internet sebagai pelaku tunggal, berarti ia melakukan perbuatannya sendiri, tanpa adanya kerja sama dengan pihak lain. Karena penyedia jasa internet berbentuk korporasi, maka pengertian berbuat sendiri tanpa adanya kerja sama dengan pihak lain adalah perbuatan itu dilakukan hanya dalam kalangan perusahaan itu saja, tanpa adanya unsur dari luar perusahaan tersebut. Dengan bentuknya sebagai perusahaan, maka pembebanan pertanggungjawaban menggunakan asas pertanggungjawaban korporasi, yaitu pengurus perusahaan yang wajib bertanggung jawab.

Apabila penyedia jasa internet bekerja bersama-sama dengan pihak lain, maka perbuatannya masuk ke dalam ranah pidana penyertaan. Pidana penyertaan merupakan perbuatan pidana yang melibatkan lebih dari satu peserta. Penyertaan adalah pengertian yang meliputi semua bentuk turut serta / terlibatnya orang atau orang-orang baik secara psikis maupun fisik dengan melakukan masing-masing

perbuatan sehingga melahirkan suatu tindak pidana.[51] Karena dalam penyertaan melibatkan lebih dari satu peserta, maka tentu saja pembebanan pertanggungjawabannya pun berbeda. Dikenal dua macam sistem pembebanan pertanggungjawaban dalam doktrin hukum pidana, yaitu:

1. Setiap orang yang terlibat bersama-sama dalam tindak pidana dipandang dan dipertanggungjawabkan secara sama dengan pembuat pidana, tanpa dibedakan baik atas perbuatan yang dilakukannya atau apa yang ada dalam batinnya
2. Masing-masing orang yang terlibat dalam tindak pidana dipandang dan dipertanggungjawabkan berbeda, yang berat-ringannya sesuai dengan bentuk dan luasnya wujud perbuatan masing-masing peserta

Sistem pembebanan yang pertama dianut dan diterapkan di negara Inggris. Sedangkan sistem pembebanan yang kedua dianut dan diterapkan di negara Jerman. Indonesia menggunakan sistem campuran. Ini maksudnya antara kedua sistem tersebut digunakan. Pelaksana perbuatan dibebani tanggung jawab yang sama, sedangkan pembantu perbuatan dibebani tanggung jawab yang berbeda, sesuai dengan peranannya dalam perbuatan, dimana biasanya lebih ringan daripada pelaksana perbuatan.

Bentuk penyertaan diterangkan dalam pasal 55 dan 56 KUHP. Pasal 55 KUHP menerangkan tentang golongan yang disebut sebagai pembuat (*mededader*), sedangkan pasal 56 KUHP menerangkan tentang golongan yang disebut sebagai pembuat pembantu (*medeplichtige*). Yang disebut sebagai pembuat adalah mereka yang melakukan (*plegen*), menyuruh melakukan (*doen*

[51] Adami Chazawi, *Pelajaran Hukum Pidana bagian 3*, PT RajaGrafindo Persada, Jakarta, 2005, hal 73

plegen), turut serta melakukan (*mede plegen*), dan sengaja menganjurkan (*uitlokken*). Sedangkan yang disebut sebagai pembuat pembantu (*medeplichtige*) adalah mereka yang memberikan bantuan pada saat pelaksanaan kejahatan, atau memberikan kesempatan, sarana atau keterangan untuk melakukan kejahatan.

Mereka yang melakukan (orangnya disebut pembuat pelaksana atau *pleger*) adalah orang yang melakukan perbuatan, dimana perbuatannya telah memenuhi unsur pidana, sehingga melahirkan suatu tindak pidana. Untuk menjadi seorang pembuat pelaksana, maka harus ada keterlibatan peserta lainnya, baik secara psikis maupun secara fisik.

Mereka yang menyuruh melakukan (orangnya disebut pembuat penyuruh atau *doen pleger*) adalah orang yang memerintahkan orang lain untuk berbuat, seakan-akan orang tersebut adalah alat dalam tangannya. Orang yang diperintahkan tersebut harus berbuat tanpa adanya kesengajaan, tanpa adanya kealpaan, maupun tanpa adanya tanggung jawab, disebabkan oleh suatu hal yang tidak diketahuinya, disesatkan, atau karena kekerasan.

Mereka yang turut serta melakukan (orangnya disebut pembuat peserta atau *medepleger*) adalah setiap orang yang sengaja berbuat untuk melakukan suatu tindak pidana, dimana pada masing-masing peserta terdapat suatu bentuk kerja sama yang dikehendaki, dan bagi masing-masing peserta telah sama-sama melaksanakan tindak pidana yang dimaksud.

Mereka yang sengaja menganjurkan (orangnya disebut pembuat penganjur atau *uitlokker*) adalah orang yang memberi atau menjanjikan sesuatu, dengan menyalahgunakan kekuasaan atau martabat, memberi kesempatan, sarana atau keterangan, sengaja menganjurkan orang lain untuk melakukan perbuatan.

Terbentuknya kehendak orang yang dianjurkan untuk melakukan tindak pidana adalah akibat langsung oleh digunakannya upaya-upaya penganjuran oleh pembuat penganjur (*psychische causaliteit*). Sehingga dengan demikian orang yang dianjurkan adalah orang yang memiliki kemampuan bertanggung jawab.

Mereka yang disebut sebagai pembuat pembantu adalah orang yang sengaja memberi bantuan pada waktu kejahatan dilakukan, atau yang sengaja memberi kesempatan, sarana atau keterangan untuk melakukan kejahatan. Pemberian bantuan ditujukan untuk sekedar mempermudah atau memperlancar pelaksanaan kejahatan saja. Bentuk pembantuan yaitu pembantuan sebelum pelaksanaan kejahatan dan pembantuan saat pelaksanaan kejahatan. Pembantuan baik sebelum maupun pada saat pelaksanaan kejahatan diwujudkan melalui pemberian kesempatan, sarana, ataupun keterangan. Perbuatan dalam pembantuan dapat berupa pembantuan aktif dan pembantuan pasif. Pembantuan aktif adalah bentuk pembantuan dengan melakukan perbuatan aktif. Sedangkan pembantuan pasif adalah pembantuan dengan tidak melakukan perbuatan aktif, tetapi dengan tidak melakukan perbuatan aktif, orang itu telah melanggar suatu kewajiban hukumnya.

Penyedia jasa internet apabila benar-benar terbukti bersalah, baik ia bertindak sebagai pelaku tunggal, bersama-sama dengan pihak lain (penyertaan), maupun berlaku sebagai pembantu, jelas dapat dikenai sanksi pidana. Ketentuan yang mengatur tentang sanksi pidana bagi penyedia jasa internet apabila terbukti bersalah adalah pasal 52 ayat (4) UU ITE.

> *Dalam hal tindak pidana sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.*

Ketentuan tersebut berlaku bagi semua macam jenis penyertaan. Khusus untuk pembantuan, maka juga digunakan ketentuan dalam pasal 57 ayat (1) KUHP.

> *Dalam hal pembantuan, maksimum pidana pokok terhadap kejahatan dikurangi sepertiga.*