BAB I

PENDAHULUAN

A. Latar Belakang

Manusia adalah makhluk yang dianugerahi akal dan pikiran oleh Tuhan Yang Maha Esa. Pemikiran manusia senantiasa berkembang mengikuti pola perkembangan jaman. Dengan berkembangnya manusia, maka bekembang pula kebutuhannya. Karena pada dasarnya, keinginan manusia itu tidak terbatas, walaupun pada kenyataannya alat pemuas kebutuhannya yang terbatas. Oleh sebab itu, manusia dituntut untuk banyak melakukan berbagai terobosan dan inovasi untuk mencapai tingkat kepuasan maksimum dalam rangka pemenuhan kebutuhannya. Namun manusia selalu tidak pernah merasa puas. Melalui pengetahuannya, manusia selalu ingin terus melakukan inovasi yang lebih dan lebih jauh lagi. Hal inilah yang sering kita kenal sebagai perkembangan teknologi.

Perkembangan teknologi sejalan dengan perkembangan pengetahuan manusia. Dahulu, manusia hanya menggunakan peralatan seadanya dan sederhana untuk menunjang kehidupannya. Namun sekarang, peralatan-peralatan penunjang kehidupan manusia jauh lebih canggih dan lebih kompleks. Teknologi merupakan salah satu ciri khusus kemuliaan manusia bahwa dirinya tidak hidup dengan makanan semata. Teknologi adalah sebuah manifestasi langsung dari bukti kecerdasan manusia.[1]

Globalisasi adalah gejala perkembangan yang sangat pesat di segala bidang, hingga menyingkirkan batas geografis, ekonomi, dan budaya masyarakat,

[1] Aji Dedi Mulawarman, 2008, *Pengertian Teknologi (online)*, http://ajidedim. wordpress.com/teknologi-islami/technology/, (22 Februari 2011).

sehingga batas-batas wilayah suatu negara menjadi bias. Dalam era globalisasi sekarang ini, teknologi merupakan kunci utama dalam arus perkembangan jaman. Bahkan ada suatu ungkapan populer yang menyatakan bahwa dengan menguasai teknologi, berarti sama dengan menguasai dunia.

Informasi dan teknologi adalah suatu kesatuan yang tidak dapat dipisahkan dalam perkembangan dunia. Diciptakannya komputer dengan perkembangannya yang begitu pesat membawa kemudahan pada kehidupan manusia. Kemudian diciptakannya Internet yang kemudian berkembang dengan sangat pesat membawa dampak positif bagi manusia. Ditambah lagi dengan semakin meluasnya penggunaan Internet dalam kehidupan manusia, maka semakin bertambah cepat terjadinya pertukaran arus informasi dan teknologi dalam kehidupan manusia. Melalui media internet, kita dapat mengetahui kejadian penting yang terjadi, bahkan kejadian lima menit yang lalu yang terjadi di belahan bumi lainnya.

Keberadaan internet semakin memudahkan dan mempercepat arus perpindahan informasi dan teknologi yang sangat dibutuhkan manusia dalam era teknologi sekarang ini. Namun, elemen penting dalam internet sesungguhnya adalah keberadaan penyelenggara jasa internet, atau dalam bahasa Inggris sering disebut sebagai *Internet Service Provider* (ISP). ISP adalah perusahaan atau badan yang menyelenggarakan jasa sambungan Internet dan jasa lainnya yang berhubungan. Kebanyakan perusahaan telepon merupakan penyelenggara jasa Internet.[2]

---

[2] *Penyelenggara Jasa Internet (online),* http://id.wikipedia.org/wiki/Penyelenggara_jasa_Internet, (22 februari 2011)

Dengan gejala perkembangan teknologi di segala bidang yang semakin pesat, maka tidak menutup kemungkinan terjadinya perkembangan tindak kejahatan. Tindak kejahatan yang dilakukan tidak lagi menggunakan metode-metode konvensional. Namun digunakan metode-metode yang lebih canggih dan lebih efisien dalam melakukan tindak kejahatan. Hingga dikenalnya bentuk kejahatan dalam Internet atau dunia maya yang seringkali disebut sebagai *cyber crime*. *Cyber crime* merujuk pada suatu tindakan kejahatan yang berhubungan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer.[3] *Cyber crime* yang sering diidentikkan dengan *computer crime*, atau dalam bahasa Indonesia disebut sebagai tindak pidana komputer adalah setiap perbuatan melanggar hukum yang memerlukan pengetahuan tentang komputer untuk menangani, menyelidiki dan menuntutnya.[4] Widodo menyebutkan bahwa tindak pidana komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer.[5]

Cyber crime memiliki berbagai bentuk, jenis dan variasi. Bentuk *cyber crime* yang umum dan sering digunakan antara lain: *carding*, *hacking*, *cracking*, *defacing*, *spamming*, *malware*, dan *phising*. *Carding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. *Hacking* adalah kegiatan

---

[3] Dikdik M Arief Mansur dan Elisatris Gultom, *Cyber Law*, PT Refika Aditama, Bandung, 2005, hal 7.

[4] Abdul Wahid dan Muhammad Labib, *Kejahatan Mayatantra*, PT RefikaAditama, Bandung, 2005, hal 40.

[5] Widodo, *Sistem Pemidanaan Dalam Cyber Crime*, Laksbang Mediatama, Yogyakarta, 2009, hal 24.

menerobos program komputer milik orang/pihak lain. *Cracking* adalah hacking untuk tujuan jahat. *Defacing* adalah kegiatan mengubah halaman situs/*website* pihak lain. *Spamming* adalah pengiriman berita atau iklan lewat surat elektronik (*e-mail*) yang tak dikehendaki. *Malware* adalah program komputer yang mencari kelemahan dari suatu *software*. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau *operating system.*[6]

Phising adalah kegiatan memancing pemakai komputer di internet (*user*) agar mau memberikan informasi data diri pemakai (*username*) dan kata sandinya (*password*) pada suatu halaman web yang tampilannya sudah diatur sedemikian rupa sehingga mirip, bahkan sama persis dengan tampilan web aslinya. Kejahatan ini sebenarnya hanya memanfaatkan kelengahan dan kelalaian user dalam memasukkan alamat web yang dituju. *Phising* biasanya diarahkan kepada pengguna *online* banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya.[7]

Kasus *phising* populer yang terjadi di Indonesia dalam dunia perbankan adalah kasus klikbca.com yang dilakukan oleh Steven Haryanto, seorang hacker dan jurnalis pada majalah Master Web (alamat aslinya adalah www.klikbca.com, diubah menjadi klik-bca.com, kilkbca.com, clikbca.com, klickca.com dan klikbac.com) yang terjadi pada tahun 2001 dan bankmandiri.com (alamat aslinya adalah www.bankmandiri.com, diubah menjadi banknandiri.com yang apabila diakses akan langsung diarahkan pada alamat http://ib.banknandiri.com/retail) yang pernah terjadi pada tahun 2009. Namun, dalam beberapa kasus, phising

[6] Andrik Supriadi, 2010, *Hati Hati Kejahatan Internet (online)*, http://andriksupriadi.wordpress.com/2010/04/29/cyber-crime/, (22 Februari 2011).
[7] *Ibid.*

ternyata tidak hanya diarahkan kepada pengguna *online banking* saja. Beberapa pengguna jejaring sosial populer seperti Facebook pernah melaporkan adanya halaman web palsu yang diindikasikan sebagai sarana *phiser* (pelaku phising) untuk menjalankan kejahatannya. Tercatat pernah adanya alamat http://fesbook.byethost24.com/[8] serta http://www.facebook.com.profile.php.id.371233.cn[9] sebagai *fake log in* (halaman masuk palsu) pada Facebook yang sekarang sudah tidak dapat diakses lagi.

Berdasarkan data yang dihimpun oleh atlas.arbor.net, sebuah situs bagi pelaporan *cyber crime* di seluruh dunia, lebih dari sepuluh website populer di seluruh dunia telah digunakan sebagai media *phising* oleh *phiser*. PayPal, Facebook, dan eBay merupakan *website* yang paling sering digunakan sebagai media *phising*. Sedangkan untuk domain yang diketahui digunakan sebagai media *phising* terbanyak terletak pada domain yang telah di *hosting* oleh server di negara Amerika Serikat, Belanda, dan Jerman.

Tabel 1.1

Website Yang Sering Digunakan Sebagai Media Phising

Website	Jumlah kasus
PayPal	5.161
Facebook	1.770
Ebay	1.597

Sumber: *Data Sekunder diolah*, 2011

[8] masihnewbie21, 2011, *[awas]penyebaran phising melalui chat facebook!!! (online)*, http://www.kaskus.us/showthread.php?t=6606545, (22 Februari 2011).

[9] Eko Pramuyanto, 2008, *Facebook Phising (online)*, http://maseko.com/2008/01/03/facebook-phishing/, (22 Februari 2011).

Tabel 1.2

Server Di Negara Yang Sering Digunakan Sebagai Media Phising

Negara	Jumlah kasus
Amerika Serikat	60.902
Belanda	7.569
Jerman	4.705

Sumber: *Data Sekunder diolah*, 2011

Phising merupakan bentuk *cyber crime* jenis baru. Sebelum diundangkannya Undang Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, praktis tidak ada satu aturan baku yang dapat menjerat pelaku tindak pidana komputer, utamanya pelaku phising. Namun ternyata setelah diundangkannya Undang Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pun, masih dirasa belum mencukupi untuk menjerat pelaku *phising*. Hal ini disebabkan karena belum dicantumkannya definisi *phising* dalam undang-undang tersebut. Undang undang nomor 11 tahun 2008 hanya mencantumkan unsur-unsur serta kualifikasi *cyber crime* secara umum melalui pasal 28 ayat (1) dan pasal 35. Kedua pasal tersebut tidak membedakan apakah *cyber crime* itu termasuk dalam kategori *carding*, *hacking*, *cracking*, *defacing*, *spamming*, *malware* atau *phising*, padahal kualifikasi perbuatannya jelas berbeda.

Di negara lain, cybercrime sudah menjadi sesuatu permasalahan yang cukup serius. Hal ini ditandai dengan diaturnya secara khusus mengenai pembatasan tanggung jawab Penyedia Jasa Internet dan berbagai peraturan yang mengatur tentang cybercrime itu sendiri. Di Amerika Serikat misalnya, sudah dikeluarkan *Digital Millenium Copyright Act* yang memberikan batasan tentang

sejauh mana penyelenggara jasa internet dapat dipertanggung jawabkan apabila terjadi pelanggaran kasus cybercrime dalam hal pelanggaran hak cipta. Demikian juga dengan Eropa yang mengeluarkan *European E-Commerce Directive*, Jerman dengan *Information and Communication Services Act*-nya, *Digital Copyrights Act 2000* milik Australia, dan Singapura dengan *Electronic Transaction Act 1998*-nya. Selain dikeluarkannya peraturan-peraturan tersebut, juga dibentuk suatu institusi tersendiri yang secara khusus menangani kasus cybercrime. Di Amerika Serikat misalnya, telah dibentuk *Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Departement of Justice*. Institusi ini memiliki situs web yang memberikan informasi tentang cybercrime. Dikeluarkannya peraturan atau bahkan dibentuknya institusi khusus ini dilatar belakangi oleh suatu anggapan bahwa Internet atau jaringan komputer sudah dianggap sebagai infrastruktur yang perlu mendapat perhatian khusus.

Era globalisasi dan teknologi informasi membawa pengaruh terhadap munculnya berbagai bentuk kejahatan yang sifatnya baru. *Phising* merupakan bentuk baru dari *cyber crime* yang semakin banyak terjadi di dunia maya. Hal ini sebagian besar disebabkan oleh kurangnya kewaspadaan masyarakat sebagai pengguna internet, sebagai akibat dari rendahnya pengetahuan masyarakat akan sistem keamanan di dunia maya. Hal ini diperparah dengan minimnya aturan hukum dalam melindungi masyarakat sebagai pengguna internet maupun untuk menjerat pelaku phising sebagai pemilik domain. Untuk itu, perlu adanya penanggulangan secara cepat dan akurat. Atas pertimbangan inilah, maka penulis tertarik untuk mengangkat masalah KAJIAN YURIDIS

PERTANGGUNGJAWABAN PIDANA PENYEDIA JASA INTERNET DAN PEMILIK DOMAIN SITUS PHISING.

B. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka inti permasalahan dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Peraturan hukum apa saja dalam sistem hukum pidana di Indonesia yang dapat digunakan untuk menjerat pelaku phising?
2. Bagaimana pertanggungjawaban pelaku sebagai pemilik website (domain) dalam hukum pidana?
3. Bagaimana bentuk pertanggungjawaban ISP sebagai penyedia jasa internet sekaligus sebagai penyedia halaman web (*web hosting*) yang memuat konten phising dalam hukum pidana?

C. Tujuan Penelitian

Berkaitan dengan permasalahan di atas, maka tujuan dari penulisan skripsi ini adalah:

1. Untuk mengetahui dan menganalisis peraturan hukum apa saja dalam sistem hukum positif Indonesia yang dapat digunakan untuk menjerat pelaku phising
2. Untuk mengetahui dan menganalisis pertanggungjawaban pemilik website (domain) dalam hukum pidana

3. Untuk mengetahui dan menganalisis bentuk pertanggungjawaban ISP sebagai penyedia jasa internet sekaligus sebagai penyedia halaman web (*web hosting*) yang memuat konten phising dalam hukum pidana

D. Manfaat Penelitian

Penulisan skripsi ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Secara Teoritis

   Memberikan kontribusi bagi perkembangan ilmu hukum pidana, khususnya berkaitan dengan masalah pertanggungjawaban pidana bagi pemilik website (domain) yang berisi konten phising

2. Secara Praktis

   a. Bagi Penulis

      Untuk menambah wawasan mengenai jenis-jenis perbuatan yang dikategorikan sebagai tindak pidana komputer serta menambah pengetahuan tentang bentuk tanggung jawab pemilik website (domain) yang berisi konten phising sehubungan dengan pertanggungjawaban dalam hukum pidana.

   b. Bagi Pemilik Website (Domain) maupun ISP

      Sebagai masukan dan kontribusi pemikiran bagi para pemilik website maupun penyedia jasa internet atau ISP (*Internet Service Provider*) agar lebih memperhatikan isi website miliknya atau yang dibawahinya.

c. Bagi Masyarakat

Untuk menambah wacana pengetahuan kepada masyarakat dan memberikan gambaran mengenai jenis-jenis kejahatan di internet yang bersifat terselubung, sehingga masyarakat dapat lebih berhati-hati dalam mengakses internet.

E. Sistematika Penulisan

Adapun sistematika penulisan yang disusun oleh penulis dalam skripsi antara lain:

BAB I PENDAHULUAN

Pada bab ini penulis menguraikan tentang latar belakang permasalahan, rumusan permasalahan, tujuan penulisan, metode penelitian, serta sistematika penulisan.

BAB II KAJIAN PUSTAKA

Pada bab ini penulis menguraikan tinjauan umum mengenai pidana, tinjuan umum mengenai bentuk pertanggungjawaban, tinjauan umum mengenai internet, serta tinjauan umum mengenai phising.

BAB III METODE PENELITIAN

Pada bab ini penulis membahas mengenai jenis metode pendekatan yang digunakan peneliti dalam melakukan penelitian, jenis dan sumber data di dapat dan digunakan peneliti dalam melakukan penelitan, metode penelusuran

bahan hukum, teknik analisa bahan hukum dan definisi konseptual.

BAB IV HASIL DAN PEMBAHASAN

Bab ini memuat uraian sekaligus merupakan analisis terhadap penelitian yang dilakukan meliputi kategori tindak pidana komputer dan tinjauan yuridis penggunaan halaman website (domain) sebagai media phising, bentuk pertanggungjawaban pidana bagi pemilik website (domain) yang menggunakan halaman webnya sebagai media phising, serta bentuk pertanggungjawaban ISP sebagai penyedia jasa layanan.

BAB V PENUTUP

Bab ini merupakan bab yang berisi tentang kesimpulan dan saran yang dapat penulis berikan kepada pihak-pihak yang terkait dengan permasalahan dalam skripsi ini.