BAB III

TINDAKAN PIDANA PENCEMARAN NAMA BAIK PADA JEJARING SOSIAL DI MEDIA INTERNET

A. Situs Jejaring Sosial

Kemajuan teknologi sangat potensial terhadap munculnya berbagai bentuk tindak pidana, internet dapat menjadi media yang memudahkan seseorang untuk melakukan berbagai tindak pidana berbasis teknologi informasi (*cybercrime*)

Kecanggihan teknologi komputer telah memberikan kemudahan-kemudahan terutama dalam membantu pekerjaan manusia, selain itu perkembangan teknologi komputer menyebabkan munculnya jenis kejahatan-kejahatan baru. Yaitu dengan memanfaatkan komputer sebagai modus operandi. Penyalahgunaan komputer dalam perkembangan menimbulkan permasalahan yang sangat rumit, diantaranya pembuktian atas suatu tindak pidana. Terlebih lagi penggunaan komputer untuk tindak pidana yang dilakukan tanpa menggunakan komputer (konvensional). Perbuatan atau tindakan, pelaku, alat bukti dalam tindak pidana biasa dapat dengan mudah diidentifikasi, tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer.[32]

Komputer dapat mempermudah suatu bentuk kejahatan yang konvensional seperti pencemaran nama baik pada media internet. Hal tersebut dilakukan dengan cara-cara baru sehingga tidak mudah untuk

[32]http://buletin.malsa.net.idjan 1001 Cybercrime / html, di akses pada tanggal 23 November 2009, pukul 13.00

dilakukan penyelidikan atau penyidikan seperti dalam tindak pidana biasa karena di dalam dunia maya (*cyberspace*) sulit untuk diketahui secara pasti suatu tindak pidana itu dilakukan.

Kendala-kendala tersebut tidak menyebabkan pelaku tindak pidana itu lolos begitu saja dari jeratan hukum. Selama ini banyak informasi yang diperoleh perihal banyaknya tindak pidana dengan menggunakan internet sebagai alat bantunya. Salah satu contoh kasus yaitu seperti terjadi pada Prita Mulyasari yang mengandung unsur pencemaran nama baik. Jenis kejahatan ini termasuk ke dalam kejahatan dengan modus operandi menggunakan fasilitas teknologi informasi. Bentuk kejahatan lainnya seperti pornografi dan perjudian melalui internet. Berdasarkan modus operandinya, *cybercrime* terdiri dari 2 jenis kejahatan yaitu :

1. Kejahatan yang sasaran / targetnya adalah fasilitas serta sistem teknologi komunikasi informasi.

   Para pelaku *cybercrime* menggunakan sarana ini untuk menyerang / merusak sarana teknologi informasi lainnya yang menjadi target. Pada posisi ini komputer / internet adalah alat sekaligus korban kejahatan. Kejahatan ini lebih dikenal dengan istilah *hacking* / *craking* yang menyerang program-program operasi jaringan komputer
2. Kejahatan umum / biasa yang difasilitasi oleh teknologi komunikasi informasi.

Jenis kejahatan ini sudah ada sebelum teknologi informasi bergerak menuju ke arah penyalahgunaan. Contohnya, penipuan kartu kredit, penyamaran, pencemaran nama baik, pornografi, dan sebagainya.

Banyak permasalahan hukum yang muncul ketika kejahatan di dunia maya (*cybercrime*) dapat diungkap oleh aparat penegak hukum, khususnya apabila dalam kejahatan tersebut terkait unsur-unsur asing, seperti pelakunya orang asing, korbannya orang asing atau tempat terjadinya (*locus delicti*) diluar negeri tetapi pengaruhnya dirasakan di Indonesia. Salah satu permasalahan hukum utama yang muncul bersamaan dengan terungkapnya kejahatan tersebut adalah masalah yurisdiksi hukum pidana (kriminal) suatu negara, termasuk kewenangan negara untuk menangkap, menahan, menuntut dan mengadili tersangka.

Layanan jejaring sosial yang populer di Indonesia dan memiliki jumlah pengguna yang lumayan banyak antara lain *friendster, myspace, facebook* dan *multiply.*[33]

1. *Friendster*.

   Friendster, yang ide penanamannya berasal dari nama *napste* adalah sebuah situs web jaringan sosial dimana seorang pengguna akan membuat identitas maya dan kemudian mengisi data dirinya untuk kemudian mendapatkan *account* di *friendster*. Dalam *friendster*, kita juga dapat melihat teman dari teman kita, selain melihat teman kita sendiri.

[33]Elisatris Gultom, Cyber law, Aspek Hukum Teknologi dan Informasi, PT. Refika Aditama, Bandung, 2005, hlm.23.

fitur yang disediakan *friendster* yaitu menampilkan foto, profile, testimonial atau komentar serta blog dan widget atau aplikasi-aplikasi *friendster* berfungsi sebagai alat berkomunikasi atau sebagai pengganti e-mail.

2. *Myspace*

   Myspace hampir mirip dengan *friendster*. Hanya fiturnya lebih lengkap. *myspace* sangat populer di Eropa dan Amerika sedangkan di indonesia penggunanya masih kurang di bandingkan dengan *friendster*.

3. *Facebook*

   Facebook juga mirip dengan *friendster* dan *myspace*, yang membedakannya dan membuatnya lebih menarik adalah aplikasi-aplikasi yang disediakan oleh facebook dan aplikasi-aplikasi yang dibuat sendiri. Lewat aplikasi itu bisa lebih akrab dengan teman-teman kita. Karena bisa digunaklan untuk sarana berinteraksi. Selain itu ada fitur chat yang sangat mudah digunakan.

4. *Multiply*

   Multiply memadukan layanan blog, file 1 media sharing dengan jejaring di dalamnya lebih terasa di bandingkan *friendster, facebook* ataupun *myspace*. Fitur-fitur yang disediakan multiply antara lain *sharing blog*, musik, foto, video, link dan lain-lain.

   Sharing tersebut dapat dibatasi aksesnya. Bisa hanya untuk jaringan atau siapa saja. Bisa juga untuk khusus orang-orang yang kita tunjuk.

Lewat sharing media tersebut sesama anggota mutiply bisa memberikan komentar, selama mereka diberikan akses.[34]

Sementara itu, pesatnya teknologi informasi melalui internet telah mengubah aktivitas-aktivitas kehidupan yang semula perlu dilakukan secara kontak fisik, kini dengan menggunakan media *ciberspace* aktivitas keseharian dapat dilakukan secara virtual atau maya. Masalah pelik yang dihadapi penegak hukum saat ini adalah bagaimana menjaring pelaku *cybercrime* yang mengusik rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku.

Pelaku tindak pidana dalam dunia maya sering disebut dengan istilah *hacker* hitam / *craker*.[35]

Hacker muncul pada awal tahun 196-an diantara para anggota organisasi mahasiswa *Tech Model Railroad Club* di Laboratorium Kecerdasan *Artifisial Massachusetts Institute Of Technology* (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka beroperasi dengan sejumlah komputer mainframe. Kata Hacker pertama kali muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik dari yang telah dirancang bersama. Kemudian pada tahun 1983. Analogi *hacker* semakin berkembang untuk menyebut seorang yang memiliki obsesi untuk semakin berkembang untuk menyebut seseorang yang memiliki obsesi untuk memahami dan menguasai sistem komputer.

---

[34]http://www.jejaringsosial.com. diakses pada tanggal 26 hari Kamis, pukul 19.00 WIB.

[35]Agus Raharjo, Cybercrime Pemahaman dan upaya Pencegahan Kejahatan Berteknologi, PT. Citra Aditya Bakti, Bandung, 2002, hlm.132.

Hacker adalah sebutan untuk mereka yang memberikan sumbangan yang bermanfaat kepada jaringan komputer, membuat program kecil dan membagikannya dengan orang-orang di internet. Para *hacker* biasanya melakukan penyusupan-penyusupan dengan maksud memuaskan pengetahuan dengan teknik. Perusahaan yang bergerak di dunia jaringan global (internet) juga memiliki *hacker*.

Cracker adalah sebutan untuk mereka yang masuk ke sistem orang lain dengan *cracker* lebih bersifat destruktif, biasanya di jaringan komputer, mem-bypass password atau lisensi program komputer, secara sengaja melawan keamanan komputer, mendeface (merubah halaman muka web) milik orang lain bahkan hingga men-delete data orang lain, mencuri data dan umumnya melakukan *cracking* untuk keuntungan sendiri, maksud jahat, atau karena sebab lainnya karena ada tantangan.

B. Akibat Hukum Yang Timbul Dari Tindak Pidana Pencemaran Nama Baik di Media Internet

Kejahatan dalam dunia maya (*cybercrime*) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempergunakan media internet sebagai alat bantu. Jenis-jenis kejahatan yang termasuk dalam kategori (*cybercrime*) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempergunakan media internet sebagai alat bantu. Jenis-jenis kejahatan yang termasuk dalam kategori *cybercrime* diantaranya.[36]

[36]Didik M. Arief Mansur dan Elistris Gustom, Cyber law Aspek Hukum Informasi Refika Aditama, Bandung, 2005, hlm.26.

1. Tindak pidana yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
    a. *Ilegal acces* (akses secara tidak sah terhadap sistem komputer), yaitu dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem kompetr yang dihubungkan dengan sistem komputer lain. *Macking* merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi.
    b. *Data interperence* (mengganggu data komputer), yaitu dengan sengaja melakukan perbuatan merusak, menghapus, memerosotkan (*Deterioration*), mengubah atau menyembunyikan (*supression)* data komputer tanpa hak perbuatan menyebarkan virus komputer merupakan salah satu dari jenis kejahatan ini sering terjadi.
    c. *System interference* (mengganggu sistem komputer), yaitu dengan sengaja dan tanpa hak melakukan gangguan terhadap fungsi sistem komputer dengan cara memasukkan, memancarkan merusak, menghapus, memerosotkan, mengubah, atau menyembunyikan data komputer. Perbuatan menyebarkan program virus komputer dan e-mail *Bombings* (surat elektronik

berantai) merupakan bagian dari jeni kejahatan ini yang sangat sering terjadi.

d. *Ilegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem komputer, dan atau jaringan operasional komputer yang bukan diperuntukan bagi kalangan umum, dari atau melalui sistem komputer, termasuk di dalamnya gelombang elektromagnetik yang dipancarkan dari suatu sistem komputer yang membawa sejumlah data, perbuatan dilakukan dengan maksud tidak baik, atau berkaitan dengan suatu sistem komputer yang dihubungkan dengan sistem komputer lainnya.

e. *Data Theft* (mencuri data) yaitu kejahatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. Indentifity merupakan salah satu dari jenis kejahatan ini sering diikuti dengan kejahatan penipuan (*Fraud*). Kejahatan ini juga sering diikuti dengan kejahatan data leakage.

f. *Data leakage and espionage* (membocorkan data dan memata-matai) yaitu kegiatan memata-matai dan atau membocorkan data rahasia baik berupa rahasia negara, rahasia perusahaan, atau data lainnya tidak diperuntukkan bagi umum, kepada orang lain, suatu badan atau perusahaan lain, atau negara asing.

g. *Misase of devices* (menyalahgunakan peralatan komputer) yaitu dengan sengaja dan tanpa hak, memproduksi, menjual, berusaha memperoleh untuk digunakan di impor, di edarkan atau cara lain untuk kepentingan itu, peralatan, termasuk program komputer, password di komputer, kode akses, atau data semacam itu, sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain.

2. Tindak pidana yang menggunakan komputer sebagai alat kejahatan :
   a. *Credit Card Fraud* (penipuan kartu kredit);
   b. *Bank Fraud* (penipuan terhadap Bank);
   c. *Service Offered Fraud* (penipuan melalui penawaran suatu jasa);
   d. *Identity Theft and Fraud* (pencurian identitas dan penipuan);
   e. *Computer – Related Fraud* (penipuan melalui komputer);
   f. *Computer – Related Foigery* (pemalsuan melalui komputer);
   g. *Computer – Related Betting* (Perjudian melalui komputer);
   h. *Computer – Related Extortion and Threats* (pemerasan dan penipuan melalui komputer).
3. Tindak pidana yang berkaitan dengan isi atau muatan data atau sistem komputer :
   a. *Child pornography* (pornografi anak);

b. *Intfringements of copy right and related rights* (pelanggaran terhadap hak cipta dan hak-hak terkait);

c. *Drug traffickers* (peredaran narkob), dan lain-lain.

Internet adalah suatu media yang dapat menyatukan media audio, visual, telekomunikasi bahkan dapat mengkonversikan kedua media tersebut.[37] Pengguna media internet yang dirasakan sangat efisien, efektif dan juga ekonomis telah memberikan dampak tersendiri bagi perkembangan kehidupan. Masyarakat sangat membutuhkan penggunaan internet saat ini. Akan tetapi selain memberikan dampak positif, internet juga mengambil peran dalam memberikan dampak-dampak yang negatif yaitu dalam perkembangan kejagatan. Penyalahgunaan sarana internet, bagi para pelaku kejagatan ataupun orang-orang yang tidak bertanggung jawab adalah media komunikasi. Jadi bukan sekedar kecanggihan fiturnya yang diperlukan. Lebih dari itu, kekuatan strategi komunikasilah yang menjadi dasar utamanya.

C. Penghinaan dan Pencemaran Nama Baik

Larangan content yang memiliki muatan penghinaan dan / atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) ini sebenarnya adalah berusaha untuk memberikan perlindungan atas hak-hak individu maupun institusi, dimana penggunaan setiap informasi melalui media yang menyangkut data pribadi seseorang atau institusi harus dilakukan atas persetujuan orang/institusi yang bersangkutan.

[37]Budi Agus Riswandi, Hukum dan Internet di Indonesi, VII Pers, Yogyakarta 2003, hlm 15.

Bila seseorang menyebarluaskan suatu yang data pribadi seseorang melalui media internet, kdalam hal ini blog, tanpa seijin orang yang bersangkutan, dan bahkan menimbulkan dampak negatif bagi orang yang bersangkutan, kmaka selain pertanggungjawaban perdata (ganti kerugian) sebagaimana diatur dalam KUHP Pasal 26 Undang-undang ITE, maka Undang-undang ITE akan memberikan sanksi pidana bagi pelakunya.

Selain pasal poidana pencemaran nama baik dalam Undang-undang ITE tersebut, kitab-kitab undang hukum pidana juga mengatur tentang pidana penghinaan dan pencemaran nama baik. Pasal-pasal pidana mengenai penghinaan dan pencemaran nama baik ini memang sudah lama berada dalam dunia hukum.

Berdasarkan Pasal 310 KUHP dan pasal 27 ayat (3) UU ITE tersebut di atas, untuk dapat dikategorikan sebagai tindak pidana pencemaran nama baik, maka harus dibuktikan unsur-unsur sebagai berikut :[38]

- Adanya kesengajaan;
- Tanpa hak (tanpa izin);
- Bertujuan untuk menyerang nama baik atau kehormatan;
- Agar diketahui oleh umum.

Kejahatan maya antara (cybercrime) merupakan kejahatan modern yang muncul seiring dengan berkembangnya ilmu pengetahuan dan teknologi. Kejahatan di dunia maya mempunyai karakteristik yang berbeda dengan kejahatan-kejahtan konvensional yang terdapat dalam kitab undang-undang hukum pidana (KUHP).

[38]Ibid, hlm. 192

Pada dasarnya tindak pidana pencemaran nama baik adalah tindak pidana konvensional biasa. Akan tetapi berbeda halnya apabila tindak pidana pencemaran nama baik ini menggunakan teknologi canggih seperti perangkat lunak pada sebuah komputer yang terceptanya tindak pidana pencemaran nama baik itu sendiri. Seperti pada kasusnya Prita Mulyasari, menyebarkan e-mail kepada 10 orang temannya yang berisikan keluhannya terhadap rumah sakit tersebut. E-mail tersebut kemudian menyebar luas ke mailing list. Berita ini sangat menggemparkan para pembaca media cetak maupun elektronik, bagaikan magnitude yang tersebar secara on-line untuk mempublikasikan tentang surat pembaca yang ditulis oleh Prita Mulyasari. Tak kurang dari 10.000 *Facebooker* mendukung pembebasannya. Demikian juga keluhannya yang ditulis Prita Mulyasari dalam e-mail nya itu, isinya hanya menggambarkan pengalamannya bersinggungan dengan RS Omni Internasional. Kasus Prita Mulyasari harus menjadi pelajaran bagi masyarakat, khususnya para pengguna blog dan sejenisnya agar lebih berhati-hati dalam berkoneksi di dunia internet.

Kemajuan teknologi komputer, teknologi informasi dan teknologi komunikasi menimbulkan suatu tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari perkembangan tersebut tidak lepas dari sifatnya yang khas sehingga

membawa persoalan baru yang agak rumit untuk dipecahkan, berkenaan dengan masalah penanggulangannya.

Perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya dimana kepolisian merupakan lembaga aparat penegak hukum yang memegang peranan penting di dalam penegakan hukum, sebab tanpa adanya hukum yang mengatur dan lembaga yang menegakkan maka dapat menimbulkan kekacauan di dalam perkembangannya. Dampak negative tersebut menimbulkan suatu kejahatan yang dikenal dengan nama "*cybercrime*" yang tentunya harus di antisipasi dan ditanggulangi.