LAPORAN PENELITIAN

TENTANG

PENCEMARAN NAMA BAIK MELALUI INTERNET MENURUT UNDANG- UNDANG ITE(UNDANG- UNDANG NO 11 TAHUN 2008) Jo. Undang- Undang No 16 Tahun 2016

OLEH :

RATNA WATI SH,MH.

FAKULTAS HUKUM

UNIVERSITAS Dr. SOETOMO SURABAYA

SURABAYA 2020

LEMBAR PENGESAHAN

1. a. Judul Penelitian : Pencemaran nama baik melalui internet menurut undang- undang ITE
   b. Macam Penelitian : Yuridis Normatif.
   c. Katagori Penelitian : Penegakkan Hukum
2. Indentitas Peneliti :

a. Nama : Ratna Wati,SH.MH
b. Jenis Kelamin : Perempuan
c. Pangkat / Gol : Lektor / III.d
d. Jabatan Fungsional : Pengajar
e. Pekerjaan : Dosen Yayasan
f. Fakultas : Hukum

3. Jangka Waktu Penelitihan : 5 Bulan
4. Biaya yang di perlukan : Rp. 3.000.000
5. Sumber Dana : Mandiri

Mengetahui :

A.n Dekan Fakultas Hukum

Wakil Dekan I

DR. Noenik Soekorini,,SH,MH
NPP. 92.01.1.108

Surabaya, 29 Juli 2020

Peneliti

Ratna Wati, SH.MH
NPP. 97.01.1.259

Mengetahui :
Ketua Lembaga Penelitian
Universitas Dr.Soetomo Surabaya

DR. Fadjar Kurnia Hartadi, MP
NPP. 95.01.1.198

1

RINGKASAN

Pencemaran nama baik adalah satu/ sekumpulan data elektronik yang terdiri dari tulisan, suara, gambar, peta, rancangan, foto dan lain lain yang telah diolah sehingga didalamnya mengandung unsur penghinaan atau pencemaran nama baik seseorang. Hal ini merupakan kejahatan yang targetnya adalah seseorang yang akan dirugikan dimasyarakat. Sedangkan alat yang digunakan/ medianya adalah internet yang merupakan alat untuk kejahatan tersebut. Jenis kejahatan ini(pencemaran nama baik dilakukan oleh pelaku tindak pidana dalam dunia maya yang disebut dengan istilah *hacker hitam atau cracker)* hal tersebut diatur dalam undang- undang ITE(UU No. 11 Tahun 2008)

PRAKATA

Syukur Alhamdulilah penulis panjatkan kehadirat Allah SWT Yang Maha Kuasa, karena dengan berkah dan hidayah-Nya penelitihan berjudul **"PENCEMARAN NAMA BAIK MELALUI INTERNET MENURUT UNDANG- UNDANG ITE(UNDANG-UNDANG NO 11 TAHUN 2008) Jo. Undang- Undang No 16 Tahun 2016"** ini dapat penulis selesaikan .

Penelitihan ini saya lakukan untuk mengembangkan ilmu pengetahuan hukum pidana dan untuk menjelaskan tentang adanya kejahatan ini yang ada dan banyak terjadi di masyrakat,dan selalu ditutupi oleh mereka yang menjadi korban kejahatan ini, sebab jika terkuak, mereka akan merasa malu sebab pelakunya kadang adalah keluarga terdekat dari mereka, seperti ayah, saudara, kawan, tetangga dan sebagainya.

Penelitihan ini juga bisa sebagai pengetahuan bagi masyarakat, agar waspada terhadap kejahatan ini, dan mau melapor, jika pada keluarganya, sehingga pelaku bisa diproses secara hukum, dan diberi sanksi / pidana agar jerah / kapok, dan tidak mengulang perbuatannya, juga dibahas tentang perlindungan hukum bagin korbanya.

Semoga laporan ini bisa memberikan manfaat bagi masyarakat dan bisa menambah perkembangan ilmu hukum pidana.

Peneliti

Surabaya, Maret 2020

DAFTAR ISI

BAB I

PENDAHULUAN

A. Permasalahan: Latar belakang dan Rumusannya

Kejahatan telah diterima sebagai suatu fakta, baik pada masyarakat yang paling sederhana(primitive) maupun masyarakat yang modern, yang merugikan masyarakat. Kerugian yang ditimbulkan dapat berupa kerugian dalam arti material maupun immaterial. Kerugian material misalnnya korban kejahatan dan rusak atau musnahnya nama baik serta celaan yang diterima korban. Kerugian immaterial dapat berkurangnya atau hilangnya kepercayaan masyarakat terhadap dirinya dan lingkungan sekitar.[1]

Perkembangan teknologi telah memberikan nuansa baru bagi kehidupan manusia yang menyentuh semua aspek kehidupan. Teknologi, memberi kemudahan bagi masyarakat untuk melakukan aktivitas demi memenuhi kebutuhannya dan melakukan interaksi dengan manusia lainnya dimana pun berada. Teknologi selain membawa keuntungan seperti memberi kemudahan bagi masyarakat untuk melakukan aktivitasnya, juga menimbulkan kerugian- kerugian seperti maraknya kejahatan-kejahatan yang dilakukan melalui teknologi informasi. Teknologi juga memberikan pengaruh yang significant dalam pemahaman mengenai kejahatan terutama terhadap aliran- aliran dalam kriminologi yang menitikberatkan pada faktor manusia, baik secara lahir maupun psikologis.

[1] Agus Raharjo, *Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi.* Citra Aditya Bakti, Bandung, 2002, hal 29

Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu sendiri telah ada dan muncul sejak permulaan zaman sampai sekarang dan masa yang akan datang. Bentuk kejahatan yang adapun semakin hari semakin bervariasi. Suatu hal yang patut diperhatikan bahwa kejahatan sebagai gejala sosial sampai sekarang belum diperhitungkan dan diakui untuk menjadi suatu tradisi atau budaya, padahal jika dibandingkan dengan berbagai budaya yang ada, usia kejahatan tentu lebih tua. Kejahatan sebenarnya tumbuh dan berkembang dalam masyarakat, tidak ada kejahatan tanpa masyarakat. Betapapun kita mengetahui banyak tentang berbagai faktor kejahatan yang ada dalam masyarakat, namun yang pasti adalah kejahatan merupakan suatu bentuk perilaku manusia yang terus mengalami perkembangan sejajar dengan perkembangan masyarakat itu sendiri.[2]

Kejahatan merupakan perbuatan antisocial, tidak hanya terdapat pada masyarakat yang sedang berkembang, tetapi ada juga dalam masyarakat yang telah maju. Kejahatan tidak hanya didunia nyata(real), tetapi juga di dunia maya yang berbeda bentuknya dengan kejahatan konvesional, karena telah diperhalus sedemikian rupa. Keberadaan suatu kejahatan identik dengan keberadaan manusia itu sendiri meskipun ada kemungkinan bentuk atau tipe kejahatan dari tiap- tiap masyarakat berbeda.

Kecanggihan teknologi computer telah memberikan kemudahan- kemudahan, terutama dalam membantu pekerjaan manusia. Selain itu, perkembangan teknologi computer menyebabkan munculnya jenis- jenis kejahatan baru, yaitu melalui penyalahgunaan computer sebagai modus operandinya. Penyalahgunaan computer dalam perkembangannya menimbulkan permasalahan yang rumit, terutama erat

[2] ibid

kaitannya dengan proses pembuktian suatu tindak pidana. Apalagi penggunaan computer untuk tindak kejahatan itu memiliki karakteristik tersendiri atau berbeda dengan kejahatan yang dilakukan tanpa menggunakan computer. Perbuatan atau tindakan, pelaku, alat bukti maupun barang bukti dalam tindak pidana biasa dapat dengan mudah diidentifikasi, tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan computer.

Perkembangan lebih lanjut dari teknologi berupa computer network yang kemudian melahirkan suatu ruang komunikasi dan informasi global yang dikenal dengan internet. Kemudahan yang diperoleh melalui internet tentunya tidak menjadi jaminan bahwa aktivitas yang dilakukan di media tersebut adalah aman atau tidak melanggar norma. Dari permasalahan diatas, kita harus teliti dalam melihat fenomena sosial yang berkembang dalam masyarakat. Belum dianggap sebagai tindak pidana jika suatu perbuatan tidak secara tegas tercantum di dalam peraturan hukum pidana(KUHP) atau ketentuan pidana lainnya. Prinsip tersebut hingga sekarang dijadikan pijakan demi terjaminnya kepastian hukum. Dalam upaya mencapai kepastian, hukum pidana juga diupayakan untuk mencapai kesebandingan hukum. Sehingga hakim dan aparat penyidik tidak selalu berpegang pada asas legalitas saja.[3]

Kejahatan melalui penyalahgunaan teknologi informasi semakin banyak dilakukan. Jenis dan modus kejahatannya sendiri pun semakin berkembang. Disisi yang lain tingkat keberhasilan pengungkapan pelaku kejahatan dengan teknologi informasi ini masih sangat rendah. Hal ini tentunya sangat menghawatirkan masyarakat secara luas. Kerugian yang ditimbulkan akibat kejahatan ini tidak sedikit. Perkembangan kejahatan sampai saat ini semakin meningkat, termasuk adanya kemajuan teknologi computer tidaklah menyebabkan kejahatan itu semakin berkurang

[3] Edmon Makarim, *kompilasi hukum telematika.* Rajawali Pres, Jakarta, 2003. Hal 388

tapi justru sebaliknya. Kejahatan yang dilakukan makin canggih dan rumit, tidak seserdahana yang kita bayangkan. Dunia maya sebagai suatu perkembsngsn baru dalam sejarah peradaban manusia menyebabkan sulitnya dilakukan penegakan hukum sesuai tata cara yang berlaku.[4]

Salah satu kejahatan yang dilakukan dengan menyalahgunakan kecanggihan teknologi computer adalah melakukan akses secara tidak sah melalui pencurian kode akses terhadap jaringan computer seseorang yang mengakibatkan pencemaran nama baik. kode akses data jaringan computer yang diubah menggunakan perangkat lunak yang merupakan bagian dari kecanggihan jaringan computer dapat diakses dengan mudah tanpa diketahui oleh sang pemilik data tersebut.tindakan tersebut dapat berakibat mengandung unsur pencemaran nama baik sebab apabila terjadi tindakan tersebut ,ala data yang dapat diakses sewaktu- waktu bisa diubah, ditambahkan atau juga di tiadakan, seperti kasus yang dialami oleh Rektor Universitas Dr. Soetomo Surabaya atau bapak Ulul abab dimana *akount* atau data pribadi beliau yang terdapat di facebook pernah diakses oleh orang yang tidak dikenal dan tindakan tersebut berlanjut dengan adanya penulisan status/ pernyataan yang memiliki unsur pencemaran nama baik berdasar keterangan Dwi Cahyo, Staff IT Universitas Dr. Soetomo Surabaya. Kejahatan tersebut dalam hukum positif 2008 tentang Informasi dan Transaksi Elektronik yaitu setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Ketentuan yang diatur dalam *Convention on cyber crime* tanggal 23 november 2001 di kota budhapest Hongaria yang mana salah satu kualifikasi cyber crime menurut *convention on cybercrime* tersebut adalah *misuse of devices* yaitu

[4] Ibid. hal 419

penyalahgunaan perlengkapan computer, termasuk program computer, password computer, kode masuk.

Berdasarkan apa yang telah diuraikan pada latar belakang diatas, maka penulis merumuskan permasalahan sebagai berikut:

1. Bagaimana hukum Indonesia tentang cybercrime yang berupa akses tidak sah kode akses jaringan computer?
2. Bagaimana sanksi bagi pelaku akses secara tidak sah kode akses jaringan computer internet yang menyebabkan pencemaran nama baik?

BAB II

TINJAUAN PUSTAKA

A. Pengertian Cybercrime

Semakin tingginya kejahatan dengan menggunakan media internet sebagai sarananya pada saat ini yang meliputi berbagai jenis kejahatan contohnya seperti penipuan kartu kredit, penipuan perbankan, defacing, cracking, transaksi seks, judi online dan terorisme dengan korban yang sudah melintasi batas- batas territorial dari suatu wilayah Negara pada saat ini, merupakan salah satu permasalahan yang cukup rumit yang harus dihadapi oleh aparat penegak hukum dalam suatu wilayah Negara.

Perkembangan teknoligi jaringan computer global atau internet telah menciptakan dunia baru yang dinamakan *cyberspace*, sebuah dunia komunikasi berbasis computer yang menawarkan realitas yang baru yaitu realitas viritual. Istilah cyberspace muncul pertama kali dari novel William Gibson berjudul Neuromancer pada tahun 1984.[5] Istilah *cyberspace* pertama kali digunakan untuk menjelaskan dunia yang terhubung langsung(online) ke internet oleh Jhon Perry Barlow pada tahun 1990. Secara etimologis, istilah cyberspace sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir. Cambridge Advanced Learner Dictionary memberikan definisi cyberspace sebagai "*the internet considered as an imaginary area without limits where you can meet people and discover information*

[5] www.wikisource.com , cyberspace, akses dalam 14 Juni 2012

about any subject".[6] *The American Heritage Dictionary of English Language Fourth Edition* Mendefinisikan cyberspace sebagai "*the electronic medium of computer networks, in which online communication takes places."*[7]

Pengertian cybercrime tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet. Bruce sterling mendefinisikan *cyberspace* sebagai *the 'place' where a telephone converstation appears to occur*.

Perkembangan teknologi computer juga menghasilkan berbagai bentuk kejahatan computer di lingkungan cyberspace yang kemudian melahirkan istilah baru yang dikenal dengan *cybercrime, internet fraud* dan lain lain.

Collin Berry C. Menjelaskan istilah *Cybercrime* sebagai berikut:

"*Term" "cyber-crime" is young and created by combination of two words: cyber and crime. The term "cyber" means the cyber- space (terms "viritual space", "viritual world" are used more often in literature and means (according to the definition in "new hacker vocabulary"by Eric S. Raymond) the informational space modeled through computer, in which defined types of object or symbols images of information exist- the place where computer program work and data processed."*

Computer crime dan *Cybercrime* merupakan dua istilah yang berbeda sebagaimana dikatakan oleh Nazura Abdul Manap sebagai berikut:

"Defined broadly, "computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as crime committed using a computer as a tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who unauthorisedly transfers a

[6]Dictionary.cambridge.org akses 7 juni 2012
[7] Bartleby.com akkses 7 juni 2012

costumer's money to a domant account for his own interset or a person without permission has obtained acces to other person's computer directly to download information, which in the first place, are confidental. These situations require direct access by the hacker to the victim's computer. There is no internet line involved, or only limited networking used such as the Local Area Network (LAN). Whereas, Cyber-crimes are crimes committed virtually through Internet online. This means that the crimes committed could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refer computer crimes as cybercrimes or vice versa, since they have some impact in law."[8]

Sebagian besar dari perbuatan *cybercrime* dilakukan oleh seseorang yang sering disebut dengan *cracker.* Berdasarkan catatan Robert H'obbes' Zakon, seorang internet Evangelist, *hacking* yang dilakukan oleh *cracker* pertama kali terjadi pada tanggal 12 Juni 1995 terhadap the spot dan 12 agustus 1995 terhadap *cracker move page.* Berdasar catatan itu pula, situs pemerintah Indonesia pertama kali mengalami serangan *cracker* pada tahun 1997 sebanyak lima kali.[9]

Kegiatan *hacking* atau *cracking* yang merupakan salah satu bentuk cybercrime tersebut telah membentuk opini umum para pemakai jasa internet bahwa cybercrime merupakan suatu perbuatan yang merugikan bahkan amoral. Para korban menganggap atau memberi stigma bahwa cracker adalah penjahat. Perbuatan *cracker* juga telah melanggar hak-hak pengguna jasa internet sebagaimana digariskan dalam The Declaration of the right of netizens yang disusun oleh Ronda Hauben.[10]

[8] Manap, Nazura Abdul, Anita Abdul Rahim, and Hossein Taji. "Cyberspace identity theft: The conceptual framework." *Mediterranean Journal of Social Sciences* 6, no. 4 (2015).
[9] Agus Raharjo, op. Cit. Hal 35-39
[10] Ibid, hal 44

Berdasarkan pemikiran JoAnn L. Miller yang membagi kategori *white collar crime* menjadi empat kategori, yaitu meliputi *organizational occupational crime, government occupational crime, professional occupational crime* dan *individual occupational crime* maka Agus Raharjo berpendapat bahwa cybercrime dapat dikatakan sebagai *white collar crime* dengan kriteria berdasarkan kemampuan profesionalnya.[11]

David I. Brainbridge mengingatkan bahwa pada saat memperluas hukum pidana, harus ada kejelasan tentang batas- batas pengertian dari suatu perbuatan baru yang dilarang sehingga dapat dinyatakan sebagai perbuatan pidana dan juga dapat dibedakan dengan misalnya sebagai suatu perbuatan perdata.[12]

B. Akses Secara Tidak Sah Terhadap Kode Akses Jaringan Komputer

Perkembangan teknologi informasi yang sangat pesat di Indonesia, menuntut masyarakat untuk dapat menyesuaikan diri dengan perubahan yang terjadi sebagai dampat dari kemajuan teknologi informasi tersebut. teknologi informasi dan komunikasi telah mengubah perilaku dan pola hidup masyarakat secara global, perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas dan menyebabkan perubahan sosial budaya, ekonomi dan pola penegakan hukum yang secara significant berlangsung secara cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena disalah satu sisi teknologi informasi tersebut telah memberi kontribusi bagi peningkatan kesajahteraan kemajuan dan peradaban manusia, sedangkan disisi lainnya teknologi informasi juga menjadi sarana yang sangat efektif untuk melakukan perbuatan melawan hukum. Banyaknya penyedia

[11] Ibid, hal 50-51
[12] David I. Brainbridge. *Computer dan hukum,* sinar grafika. Jakarta. 1993. Hal 155

internet dan semakin terjangkaunya biaya untuk mengakses internet pada saat ini menimbulkan banyak terjadi penyalahgunaan sarana internet oleh seseorang yang tidak bertanggung jawab dimana internet dijadikan sebagai sarana untuk menguntungkan diri sendiri tanpa menghiraukan batas- batas hak orang lain. Salah satu penyalahgunaan yang terjadi yaitu melakukan akses terhadap data seseorang dalam jaringan computer secara melawan hukum atau tidak sah itu sendiri adalah perbuatan seseorang dengan menggunakan software khusus yang diaplikasikan pada computer yang terhubung dengan internet sehingga computer itu dapat memantau aktifitas seseorang yang sedang menggunakan internet, dengan tujuan untuk mendapatkan data pribadi pengguna internet diantaranya username dan password dari akun pribadi seseorang dalam internet.

Pada dasarnya setiap kegiatan atau aktifitas manusia telah diatur oleh hukum. Hukum dipersempit pengertiannya menjadi peraturan perundang- undangan yang dibuat oleh Negara, begitu pula aktifitas kejahatan maya yang menjadikan internet sebagai sarana utamanya. Dalam kaitan dengan teknologi informasi khususnya dunia maya, peran hukum adalah melindungi pihak- pihak yang lemah terhadap eksploitasi dari pihak yang kuat atau berniat jahat, disamping itu hukum dapat pula mencegah dampak negative dari ditemukannya suatu teknologi baru.

Undang- undang nomer 11 tahun 2008 tentang informasi dan transaksi elektronik itu sendiri disusun sedemikian rupa sebagai upaya pemerintah dalam pengakuan transaksi elektronik dan dokumen elektronik dalam kerangka hukum perikatan dan hukum pembuktian, sehingga kepastian hukum transaksi elektronik dapat terjamin, kemudian sebagai bentuk dari upaya penegakkan hukum menyangkut tindakan- tindakan yang termasuk kualifikasi pelanggaran hukum terkait penyalahgunaan teknologi informasi disertai sanksi pidananya.

Pengaturan yang menyangkut akses- akses secara tidak sah dalam jaringan computer atau internet tertuang dalam pasal 30 ayat undang- undang nomer 11 tahun 2008 tentang informasi dan transaksi elektronik tersebut yaitu:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan

Pasal tersebut diatas merupakan landasan hukum atau perlindungan hukum bagi para pengguna internet dari tindakan akses illegal yang dilakukan oleh seseorang yang dengan sengaja dan tanpa hak untuk mengakses masuk terhadap informasi elektronik atau dokumen elektronik pribadi milik orang lain secara melawan hukum. Dalam aksinya, pelaku mempunyai tujuan tertentu contohnya yaitu untuk mendapatkan informasi rahasia pengguna internet seperti username dan password akun pengguna internet.

Terdapat beberapa unsur yang terkandung pada pasal 30 ayat 1 undang- undang nomer 11 tahun 2008 tentang informasi dan transaksi elektronik tersebut diantara yaitu:

a. Setiap orang
b. Dengan sengaja
c. Tanpa hak atau melawan hukum

d. Melakukan akses

e. Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun.

Akses secara melawan hukum terhadap data pribadi pengguna internet yang dilakukan seseorang merupakan suatu kesengajaan dari seseorang yang tidak mempunyai hak dengan maksud untuk menguntungkan diri sendiri. Unsur mengguntungkan diri sendiri atau orang lain secara melawan hukum mengandung arti bahwa keuntungan dengan kepatutan dalam pergaulan masyarakat. Unsur lain dari tindakan akses illegal terhadap data pribadi pengguna internet adalah setiap orang, kata setiap orang menunjukan siapa saja orang yang apabila orang tersebut memenuhi semua unsur dari tindakan akses illegal secara sengaja dan tanpa hak, maka ia dapat disebut pelaku akses secara illegal.

Mengakses masuk data pribadi pengguna internet dalam suatu situs tertentu dalam internet secara melawan hukum dilakukan dengan berbagai cara diantaranya, melalui tindakan penyadapan maupun monitoring terhadap system computer dengan tujuan mendapatkan username dan password. Username dan password tersebut merupakan suatu bentuk dari informasi elektronik atau dokumen elektronik dimana username dan password berbentuk suatu tulisan terdiri dari huruf, tanda, angka atau kode akses yang telah diolah dan memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Berdasarkan rumusan unsur- unsur diatas, maka perbuatan yang dilakukan oleh pelaku akses illegal sudah memenuhi unsur objektif dan unsur subjektif sebagaimana yang telah tertulis pada pasal 30 ayat 1 undang- undang nomer 11 tahun 2008 tentang informasi dan transaksi elektronik. Dengan demikian pasal 30 ayat 1

undang- undang nomer 11 tahun 2008 tentang informasi dan transaksi elektronik dapat diterapkan terhadap tindak pidana akses secara melawan hukum.

C. Mengenai pencemaran nama baik menurut KUHP

Berbicara tentang pencemaran nama baik, berkaitan dengan suatu kata penghinaan. Pada dasarnya penghinaan adalah menyerang nama baik dan kehormatan seseorang, dalam hal ini bukan dalam arti seksual sehingga orang itu merasa dirugikan. Objek atau sasaran pencemaran nama baik dapat digolongkan menjadi

1. Terhadap pribadi perorangan
2. Terhadap kelompok atau golongan
3. Terhadap suatu agama
4. Terhadap orang yang sudah meninggal
5. Terhadap para pejabat yang meliputi pegawai negri, kepala Negara atau wakilnya dan pejabat perwakilan asing

Dilihat dari cara melakukan pencemaran nama baik menurut kitab undang- undang hukum pidana KUHP terdapat beberapa pembagian yaitu:

1. Secara lisan, yaitu pencemaran nama baik yang diucapkan atau dilakukan secara oral
2. Secara tertulis, yaitu pencemaran nama baik yang dilakukan melalui tulisan

Yang dimaksud dengan menghina yaitu menyerang kehormatan dan nama baik seseorang. Kehormatan yang diserang hanya mengenai kehormatan tentang nama baik, bukan dalam lapangan seksuil. Penghinaan dalam KUHP ada 6 macam yaitu

1. Menista secara lisan
2. Menista dengan surat/ tertulis

3. Memfitnah
4. Penghinaan ringan
5. Mengadu secara memfitnah
6. Tuduhan secara memfitnah

Semua penghinaan di atas hanya dapat dituntut apabila ada pengaduan dari orang yang menderita/ dinista/ dihina, kecuali bila penghinaan itu dilakukan terhadap seorang pegawai negri pada waktu sedang menjalankan pekerjaannya secara sah.

Obyek dari penghinaan tersebut harus manusia perorangan, maksudnya bukan instansi pemerintah, pengurus suatu perkumpulan, segolongan penduduk dan lain-lain, berdasarkan pasal 310 ayat 1 KUHP, penghinaan yang dapat dipidana harus dilakukan dengan cara menuduh seseorang telah melakukan perbuatan tertentu, dengan maksud tuduhan itu akan tersiar(diketahui orang banyak). Perbuatan yang dituduhkan tidak perlu suatu perbuatan yang boleh dihukum seperti mencuri, menggelapkan, berzina dan sebagainya. Perbuatan tersebut cukup perbuatan biasa yang sudah tentu merupakan perbuatan yang memalukan, misalnya menuduh bahwa seseorang telah berselingkuh. Dalam hal ini bukan perbuatan yang boleh dihukum, akan tetapi cukup memalukan bagi yang berkepentingan bila diumumkan. Tuduhan tersebut harus dilakukan dengan lisa, apabila dilakukan dengan tulisan atau gambar, maka penghinaan itu dinamakan menista/ menghina dengan surat(secara tertulis) dan dapat dikenakan pasal 310 ayat 2 KUHP.

Penghinaan menurut pasal 310 ayat 1 dan 2 di atas dapat dikecualikan apabila tuduhan atau penghinaan itu dilakukan untuk membela kepentingan umum atau terpaksa membela diri. Patut atau tidaknya pembelaan umum dan pembelaan diri yang diajukan oleh tersangka terletak pada pertimbangan hakim. Untuk kejahatan

memfitnah Pasal 311 KUHP, tidak perlu dilakukan di muka umum, telah cukup apabila dapat dibuktikan bahwa ada maksud untuk menyiarkan tuduhan tersebut. Apabila itu berupa suatu pengaduan yang berisi fitnah yang diisukan kepada pembesar/ pejabat yang berwajib, maka dapat dikenakan pidana pasal 317 KUHP.

Menurut muladi, bahwa yang dapat melaporkan pencemaran nama baik seperti tercantum dalam pasal 310 dan 311 KUHP adalah pihak yang diserang kehormatannya, direndakan martabatnya sehingga namanya menjadi tercela di depan umum. Namun, tetap ada pembelaan bagi pihak yang dituduh melakukan pencemaran nama baik apabila menyampaikan informasi ke public. Penyampaian informasi itu ditujukan untuk kepentingan umum, atau untuk membela diri atau untuk mengungkapkan kebenaran, sehingga orang yang menyampaikan informasi secara lisan atau tertulis diberi kesempatan untuk membuktikan bahwa tujuannya itu benar. Kalau tidak dapat membuktikan kebenarannnya itu namanya penistaan atau fitnah.[13]

Seperti yang telah diuraikan sebelumnya pasal- pasal dalam Bab XVI Buku II KUHP tersebut hanya mengatur penghinaan atau pencemaran nama baik terhadap seseorang, sedangkan penghinaan atau pencemaran nama baik terhadap instansi pemerintah, pengurus suatu perkumpulan atau segolongan penduduk, maka diatur dalam pasal- pasal khusus, yaitu:

1. Penghinaan terhadap Presiden dan Wakil Presiden(Pasal 134 dan pasal 137 KUHP), pasal- pasal ini telah dibatalkan atau dinyatakan tidak berlaku lagi oleh makamah konstitusi
2. Penghinaan terhadap kepala Negara asing (Pasal 142 dan pasal 143 KUHP)

[13] www.hukumonline.com ancaman pencemaran nama baik mengintai. Diakses pada 16 maret 2009

3. Penghinaan terhadap segolongan penduduk/ kelompok/ organisasi(Pasal 156 dan pasal 157 KUHP)
4. Penghinaan terhadap pegawai agama (Pasal 177 KUHP)
5. Penghinaan terhadap kekuasaan yang ada di Indonesia (Pasal 207 dan pasal 208 KUHP)

Selain itu pencemaran nama baik juga diatur dalam undang- undang nomor 32 tahun 2002 tentang penyiaram dan undang- undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Pasal 36 ayat 5 undang- undang nomor 32 tahun 2002 menyebutkan bahwa:

Isi siaran dilarang :

a. bersifat fitnah, menghasut, menyesatkan dan/atau bohong;
b. menonjolkan unsur kekerasan, cabul, perjudian, penyalah-gunaan narkotika dan obat terlarang; atau
c. mempertentangkan suku, agama, ras, dan antargolongan.

Unsur- unsur yang terdapat dalam pasal tersebut adalah:

1. Isi siaran

   Isi siaran adalah segala sesuatu yang berhubung dengan materi siaran yang disiarkan oleh stasiun televise sebagai lembaga penyiaran
2. Dilarang

   Dilarang merupakan tindakan yang tidak boleh dilakukan oleh lembaga penyiaran
3. Bersifat fitnah, menghasut, menyesatkan dan/atau bohong

Bersifat, menghasut, menyesatkan dan/atau bohong adalah materi siaran bersifat menyebarkan informasi yang tidak benar sehingga akan menimbulkan dampak yang negative bagi masyarakat

4. Menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang

   Menonjolkan unsur kekeraasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang adalah materi siaran yang didalamnya mengandung perbuatan- perbuatan tersebut yang secara tidak langsung atau pun secara langsung akan mengubah pola hidup dan perilaku masyarakat sebagai pengguna informasi

5. Mempertentangkan suku, agama, ras dan antargolongan

   Mempertentangkan suku, agama, ras dan antargolongan adalah materi siaran yang bersifat adu domba atau melakukan profokasi yang akan menimbulkan perpecahan diantara suku, agama, ras dan antargolongan

Pasal 27 ayat 3 Undang- undang nomor 11 Tahun 2008 menyebutkan bahwa Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

Unsur- unsur yang terdapat dalam pasal tersebut adalah:

1. Setiap orang

   Orang adalah orang perseorangan, baik antar warga Negara Indonesia, warga Negara asing ataupun badan hukum

2. Dengan sengaja dan tanpa hak

Dengan sengaja dan tanpa hak adalah tindakan yang dilakukan oleh pelaku kejahatan telah direncanakan atau diniatkan terlebih dahulu dan tanpa sepengetahuan dari orang yang berhak

3. Mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya

   Mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya adalah tindakan yang dilakukan oleh pelaku kejahatan supaya dapat diketahui olej orang banyak

4. Informasi elektronik yang memiliki muatan penghinaan dan atau pencemaran nama baik

   Informasi elektronik yang memiliki muatan penghinaan dan atau pencemaran nama baik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, elektronik data interchange, surat elektronik, telegram, teleks, telekopi atau sejenisnya, huruf, tanda, akses, kode akses, symbol yang telah diolah sehingga didalamnya mengandung usnur penghinaan atau pencemaran nama baik seseorang

D. Pelaku dalam tindak pidana pencemaran nama baik melalui akses yang melawan hukum

Kemajuan teknologi sangat potensial terhadap munculnya berbagai bentuk tindak pidana, internet dapat menjadi media yang memudahkan seseorang untuk melakukan berbagai tindak pidana yang berbasiskan teknologi informasi. Berdasarkan modus operandinya, cybercrime terdiri dari dua jenis kejahatan.

1. Kejahatan yang sasarannya adalah fasilitas serta system teknologi komunikasi informasi. Para pelaku cybercrime menggunakan sarana ini untuk menyerang

atau merusak sarana teknologi informasi lainnya yang menjadi target. Pada posisi ini kompuer/ internet adalah alat sekaligus korban kejahatan. Kejahatan ini dikenal dengan istilah hacking/crackinh yang menyerang program-program operasi jaringan computer

2. Kejahatan umum/biasa yang difasilitasi leh teknologi informasi bergerak menuju kea rah penyalahgunaan. Contohnya, penipuan kartu kredit, pengancaman, pencemaran nama baik, pornografi dan sebagainya

Selama ini banyak informasi yang diperoleh perihal banyaknya tindak pidana dengan menggunakan internet sebagai alat bantunya. Salah satu contoh kasusu yang terjadi pada kasus pada Rektor Universitas Dr. Soetomo Surabaya dimana ekoun pribadi beliau diakses secara tidak sah oleh orang yang tidak diketahui yang mengandung unsur pencemaran nama baik sebab pelaku menuliskan beberaapa status yang merugikan pemilik ekoun. Jenis kejahatan ini termasuk dalam kejahatan dengan modus operandi menggunakan fasilitas teknologi informasi. Bentuk kejahatan lainnya seperti pornografi dan perjudian melalui internet

Pelaku tindak pidana dalam dunia maya sering disebut dengan istilah hacker/cracker.[14] Peretas muncul pada awal tahun 1960-an di antara 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 berkutat dengan sejumlah komputer mainframe. Kata bahasa Inggris "hacker" pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki

[14] Agus raharjo. Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi. Citra Aditya Bakti. Bandung, 2002 hal 132

keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama.

Kemudian pada tahun 1983, istilah hacker mulai berkonotasi negatif. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok criminal komputer The 414s yang berbasis di Milwaukee, Amerika Serikat. 414 merupakan kode area local mereka. Kelompok yang kemudian disebut hacker tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan- Kettering hingga computer milik Laboratorium Nasional Los Alamos. Satu dari pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Perkembangan selanjutnya muncul kelompok lain yang menyebut-nyebut diri sebagai peretas, padahal bukan. Mereka ini (terutama para pria dewasa) yang mendapat kepuasan lewat membobol komputer dan mengakali telepon (phreaking). Peretas sejati menyebut orang-orang ini cracker dan tidak suka bergaul dengan mereka. Peretas sejati memandang cracker sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. Peretas sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi peretas. Para peretas mengadakan pertemuan tahunan, yaitu setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan peretas terbesar di dunia tersebut dinamakan Def Con. Acara Def Con tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas peretasan.

Hacker adalah sebutan untuk mereka yang memberikan sumbangan yang bermaanfaat kepada jaringan computer, membuat program kecil dan membagikannya dengan orang- orang di internet. Para hacker biasanya melakukan penyusupan-

penyusupan dengan maksud memuaskan pengetahuan dan Teknik. Perusahaan-perusahaan yang bergerak di dunia jaringan global juga memiliki hacker. Tugasnya yaitu untuk menjaga jaringan dari kemungkinan pengrusakan oleh pihak luar atau yang disebut cracker, menguji jaringan dari kemungkinan lubang yang menjadi peluang para *cracker* merusak jaringannya, contoh perusahaan asuransi dan *auditing "Price Waterhouse".* Yang memiliki tim hacker yang disebut dengan tiger team. Mereka bekerja untuk menguji system sekuriti klien mereka. Cracker adalah sebutan untuk mereka yang masuk ke system orang lain dan cracker bersifat lebih destruktif, biasanya di jaringan komputer, mem-bypass password atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-deface (merubah halaman muka web) milik orang lain bahkan hingga men-delete data orang lain, mencuri data.

Pada umumnya melakukan cracking untuk keuntungan sendiri, maksud jahat, atau karena sebab lainnya karena ada tantangan. Pada perkembangannya, hacker memiliki tingkatan sebagai berikut:

1. ***Elite***

   Memiliki ciri-ciri seperti mengerti sistem operasi luar dalam, sanggup mengkonfigurasi dan menyambungkan jaringan secara global, melakukan pemrogramman setiap harinya, effisien dan trampil, menggunakan pengetahuannya dengan tepat, tidak menghancurkan data-data, dan selalu mengikuti peraturan yang ada. Tingkat Elite ini sering disebut sebagai 'suhu'.

2. ***Semi Elite***

   Memiliki ciri-ciri seperti lebih muda dari golongan elite, mempunyai kemampuan dan pengetahuan luas tentang komputer, mengerti tentang sistem operasi (termasuk lubangnya), kemampuan programnya cukup untuk mengubah program eksploit.

3. ***Developed Kiddie***

   Memiliki ciri- ciri seperti umurnya masih muda (ABG) dan masih sekolah, mereka membaca tentang metoda hacking dan caranya di berbagai kesempatan, mencoba berbagai sistem sampai akhirnya berhasil dan memproklamirkan kemenangan ke lainnya, umumnya masih menggunakan Grafik User Interface (GUI) dan baru belajar basic dari UNIX tanpa mampu menemukan lubang kelemahan baru di sistem operasi

4. Script Kiddie

   Memiliki ciri- ciri seperti eperti developed kiddie dan juga seperti Lamers, mereka hanya mempunyai pengetahuan teknis networking yang sangat minimal, tidak lepas dari GUI, hacking dilakukan menggunakan trojan untuk menakuti dan menyusahkan hidup sebagian pengguna Internet.

5. ***Lamer***

   Memiliki ciri- ciri seperti tidak mempunyai pengalaman dan pengetahuan tapi ingin menjadi hacker sehingga lamer sering disebut sebagai ‘wanna-be’ hacker, penggunaan komputer mereka terutama untuk main game, IRC, tukar menukar software prirate, mencuri kartu kredit, melakukan hacking dengan menggunakan software trojan, nuke dan DoS, suka menyombongkan diri melalui IRC channel, dan sebagainya. Karena banyak kekurangannya untuk mencapai elite, dalam perkembangannya mereka hanya akan sampai level developed kiddie atau script kiddie saja.

Hacker secara harafiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup atau melakukan perusakan melalui komputer15 . Hacker dapat juga didefinisikan sebagai orangorang yang gemar mempelajari seluk-beluk sistem komputer dan bereksperimen dengannya16. Penggunaan istilah hacker

terus berkembang seiring dengan perkembangan internet, tetapi terjadi pembiasan makna kata. Hacker yang masih menjunjung tinggi atau memiliki motivasi yang sama dengan perintis mereka, hacker-hacker MIT disebut hacker topi putih (white hat hackers). Mereka masih memegang prinsip bahwa meng-hack adalah untuk tujuan meningkatkan keamanan jaringan internet. Hacker dalam pengertian yang kedua adalah mereka yang dengan kemampuan yang dimiliki melakukan kejahatan, baik pencurian nomor kartu kredit sampai perusakan situs atau website milik orang lain. Hacker ini selalu berperan dengan hacker topi putih yang menyebut mereka dengan istilah cracker (hacker hitam).

Sampai saat ini sering terdapat kekeliruan dalam menuliskan istilah yang tepat untuk mereka yang melakukan tindak pidana dunia maya. Istilah yang sering digunakan oleh media cetak dan elektronik adalah hacker, padahal yang tepat adalah cracker. Hacker, sebutan untuk mereka yang menggunakan keahliannya dalam hal computer untuk melihat, menemukan, dan memperbaiki kelemahan system keamanan dalam system computer ataupun dalam software. Hasil pekerjaan mereka biasanya dipublikasikan luas dengan harapan system atau software yang didapati memiliki kelemahan dalam hal keamanan dapat disempurnakan di masa dating. Sementara cracker memanfaatkan kelemahan- kelemahan pada system atau software untuk melakukan tindak kejahatan.

Selain pelaku, pihak-pihak yang terkait dengan tindak pence,aran nama baik melalui akses illegal, juga terdapat korban. Berbicara tentang kejahatan, maka kita secara tidak langsung berbicara tentang korban dari kejahatan tersebut. Para kriminolog sepakat, bahwa kejahatan merupakan produk dari masyarakat. Selama masyarakat masih mengadakan interaksi satu sama lain, selama itupula kejahatan akan tetap muncul. Ada korban, ada kejahatan dan sebaliknya, ada kejahatan ada

korban. Rangkaian kata ini menyatakan, apabila terdapat korban kejahatan, jelas terjadi suatu kejahatan. Kejahatan sebagaimana didefiniskan oleh Arif Gosita tersebut adalah kejahatan dalam arti luas. Kejahatan dalam arti luas tidak hanya yang dirumuskan dalam undang-undang, tetapi juga tindakan yang menimbulkan penderitaan dan tidak dapat dibenarkan serta dianggap jahat oleh masyarakat. Kejahatan dalam arti sempit adalah Mijsdriff atau crime yang merupakan bagian dari tindak pidana atau delict.[15]

[15] http://te-effendi-pidana.blogspot.com/2009/03/korban-tindak-pidana-narkoba.html diakses pada tanggal 07 april 2010

BAB III

TUJUAN DAN MANFAAT PENELITIAN

A. Tujuan penelitian

1. Untuk mengkaji dan memahami hukum yang berlaku di Indonesia mengenai cybercrime(tentang akses secara tidak sah kode jaringan computer
2. Untuk mendapatkan kejelasan mengenai sanksi hukum terhadap pelaku yang mengakses secara tidak sah kode jaringan computer yang menimbulkan pencemaran nama baik

B. Manfaat Penelitian

1. Untuk mengembangkan ilmu hukum pidana
2. Untuk memahami peranan masyarakat dan pemerintah dalam upaya menanggulangi kejahatan cyber.

BAB IV

METODE PENELITIAN

A. Pendekatan masalah

Dalam penulisan ini, penulis menggunakan pendekatan yuridis normative artinya permasalahan yang ada diteliti berdasarkan peraturan perundang- undangan No. 11 Tahun 2008 tentang ITE yang berlaku di Indonesia dan literatur- literatur yang ada kaitannya dengan permasalahan serta untuk mencari jawaban dari permasalahan tersebut.

B. Sumber bahan hukum

Sumber bahan hukum primer yaitu segala peraturan perundang- undangan yang mengatur tentang tindak cybercrime melalui facebook di Indonesia antara lain

1. Kitab undang- undang hukum pidana
2. Undang- undang No. 11 Tahun 2008 Tentang informasi dan transaksi elektronik

Sedangkan sumber bahan hukum sekunder merupakan sumber bahan yang diperoleh melalui studi kepustakaan dengan mempelajari literatur ataupun internet yang ada kaitannya dengan permasalahan yang diangkat.

C. Pengumpulan dan pengolahan bahan hukum

Dalam penelitian ini, peneliti mengumpulkan bahan hukum yang berhubungan dengan **cybercrime pada pencemaran nama baik melalui internet menurut hukum di**

Indonesia kemudian bahan tersebut di kelompokkan sesuai dengan permasalahan yang diangkat baru kemudian di susun untuk menjadi sumber bahan hukum yang dapat dipertanggung jawabkan.

D. Analisis bahan hukum

Setelah data terkumpul maka peneliti melakukan analisis bahan hukum, pembahasannya dilakukan secara deskripsi analitis, yaitu membuat deskripsi mengenai situasi-situasi atau kejadian- kejadian atas masalah yang diteliti berdasarkan penelitian kepustakaan. Bahan hukum yang diperoleh dari bahan kepustakaan tersebut dipisah- pisahkan untuk diperiksa kembali, diatur atau disistematisasi sesuai pembahasan penelitian, selanjutnya bahan kepustakaan dilakukan interprestasi analisis, dimana analisis dilakukan sesuai metode kualitatif, kemudian ditarik suatu kesimpulan.

BAB V

HASIL DAN LUARAN

A. Ketentuan hukum pidana terhadap tindak pidana teknologi informasi

Globalisasi teknologi infomasi yang telah mengubah dunia ke era cybercrime dengan sarana internet yang menghadirkan cyberspace dengan realitas viritualnya menawarkan kepada manusia berbagai harapan dan kemudahan akan tetapa dibalik itu, timbul berupaka kejahatan yang berupa cybercrime baik system jaringan computer itu sendiri yang menjadi sarana untuk melakukan kejahatan tentunya jika kita melihat bahwa informasi itu sendiri telah menjadi komonditi maka upaya untuk melindungi asset tersebut.

Kebijakan sebagai upaya untuk melindungi informasi membutuhkan suatu pengkajian yang sangat mendalam menyangkut aspek sosiologis, filosofis, yuridis dan sebagainya. Teknologi informasi sekarang ini sangat strategis dan berdampak luas terhadap aktifitas kehidupan manusia, oleh karena itu dibutuhkan peratura perundang-undangan yang dapat menanggulangi terhadap kejahatan teknologi informasi.

Peraturan teknologi informasi agar di terima masyarakat harus mempertimbangkan semua aspirasi (struktur, infrastruktur, kepakaran, dan infrasiainternational) dan berbagai kepentingan harus di selaraskan dan di serasikan pembentukan peraturan perundang- undangan di dunia cybercrime. Berpangkal pada

keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum sebagai norma hukum akan bersifat mengikat bagi tiap- tiap individu untuk tunduk dan mengikuti segala kaidah- kaidah yang terkandung didalamnya.

Sebelum diundangkannya UU No 11 tahun 2008 tentang informasi dan transaksi elektronik yang mengatur khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan cybercrime tidak ada kekosongan hukum ini terjadi jika digunakan metode penafsiran yang dikenal dengan ilmu hukum dan ini mestinya dipegang oleh apparat penegak hukum dalam menghadapi perbuatan-perbuatan yang melanggar hukum dan berdimensi baru yang secara khusus belum diatur undang- undang

Upaya penafsiran cybercrime ke dalam undang- undang yang terkait dengan perkembangan teknologi informasi telah dilakukan oleh penegak hukum dalam menangani cybercrime selama ini sebelum UU ITE di undangkan ada beberapa ketentuan hukum positif yang dapat diterapkan dengan keberanian untuk melakukan trobosan hukum dengan menafsirkan hukum yang berkaitan dengan teknologi khususnya kejahatan yang berkaitan dengan internet.

Dalam menangani kasus kejahatan dalam dunia maya terdapat pasal- pasal dalam KHUP yang mengkriminalisasikan cybercrime dengan menggunakan metode interprestasi ektensif pasal- pasal yang ada dalam KUHP yang mengakibatkan pencemaran nama baik dan sanksi hukum adalah Sebagian berikut

1. Pasal 310 ayat 1 menyebutkan bahwa Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena

pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

2. Ayat 2 Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.
3. Ayat 3 Tidak merupakan pencemaran atau pencemaran tertulis, jika perbuatan jelas dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri.
4. Pasal 311 ayat 1 Jika yang melakukan kejahatan pencemaran atau pencemaran tertulis dibolehkan untuk membuktikan apa yang dituduhkan itu benar, tidak membuktikannya, dan tuduhan dilakukan bertentangan dengan apa yang diketahui, maka dia diancam melakukan fitnah dengan pidana penjara paling lama empat tahun.

Berdasarkan penjabaran diatas telah jelas disebutkan bahwa KUHP menyebutkan sanksi pidana, agar dapat menimbulkan efek jera dalam penggunaan yang salah dalam penggunaan jejaring social yang dapat merugikan orang lain.

B. Undang- undang No. 36 tahun 1999 tentang telekomunikasi

Menurut definisi yang termuat dalam undang- undang telekomunikasi ini yang dimaksud dengan telekomunikasi adalah setiap pencemasan, pengiriman dan atau penerimaan dari setiap infomasi dalam bentuk tanda- tanda, isyarat, gambar, suara dan bunyi melalui system kawat, optic, radiao atau system electromagnetic lainnya adalah setiap alat- alat perlengkapan yang digunakan dalam bertelekomunikasi dan yang

dimaksud dengan jaringan telekomunikasi adalah perangkat telekomunikasi dan kelengkapannya yang digunakan dalam bertelekomunikasi.

Alasan dikeluarkannya undang- undang telekomunikasi dalam penjelasan umum undang- undang tersebut menyatakan bahwa penyelenggaraan telekomunikasi nasional menjadi bagian dari system perdagangan global. Pengaruh globalisasi dan perkembangan teknologi komunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaaan dan cara pandang terhadap telekomunikasi.

Internet merupakan salah satu bentuk media telekomunikasi elektronik yang terdiri dari computer dan dilengkapi dengan perlengkapan tertentu sehingga memungkinkan untuk melakukan komunikasi dengan berbagai pihak di cyberspace penyalahgunaan internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan undang- undang ini.

Jika dikaitkan dengan kejahatan- kejahatan di internet yang marak terjadi seperti hacking, carding, pencemaran dan bentuk- bentuk kejahatan yang lainnya yang berhubungan dengan cybercrime sebagai berikut:

1. Dalam pasal 21

   Menyebutkan bahwa Penyelenggara telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan, atau ketertiban umum

2. Pasal 50 junti pasal 22

   Barangsiapa melanggar ketentuan sebagaimana dalam pasal 22 di pidana dengan pidana penjara paling lama 6 tahun atau denda paling banyak RP. 600.000.000. Maksud dari pasal 50 mengkriminalitaskab terhadap perbuatan

tanpa hak, tidak sah atau memanipulasi mengakses ke jaringan telekomunikasi khusus

3. Pasal 55 junto pasal 38

   Barangsiapa yang melanggar ketentuan sebagaimana maksud dalam pasal 38 di pidana dengan pidana paling lama 6 tahun atau denda paling banyak Rp. 600.000.000 maksud dari pasal 55 mengkriminalisasikanperbuatan yang dapat menimbulkan gangguan fisik elektro magnetic terhadap penyelenggaraan Telekomunikasi pasal 55 junto pasal 38 berkaitan dengan kerahasiaan

C. Sanksi hukum menurut undang- undang No 11 tahun 2008

Pasal 27 ayat 3 Undang- undang nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik. Aparat penegak hukum menggunakan pasal tersebut untuk mendakwa seseorang yang dianggap mencemarkan diri pribadi orang lain dalam ranah internet. Bunyi pasal tersebut adalah sebagai berikut

"Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik."

Pasal 27 ayat 3. Juncto

"Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)"(Pasal 45 ayat 1 UU ITE)

Di dalam pasal 27 ayat 3 UU ITE terdapat 2 unsur, yaitu unsur objektif dan unsur subjektif

a. Pasal 45 UU ITE

   Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)

b. Pasal 36 UU ITE

   Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

c. Pasal 51 ayat 2 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 Rp12.000.000.000,00 (dua belas miliar rupiah).

D. Ketentuan KUH Perdata terhadap pencemaran Nama Baik

1. Pasal 1372 KUH Perdata menegaskan bahwa tuntutan perdata tentang hal penghinaan adalah bertujuan mendapat penggantian kerugian serta pemulihan dan kehormatan nama baik
2. Pasal 1373 KUH Perdata menyatakan Selain itu, orang yang dihina dapat menuntut pula supaya dalam putusan juga dinyatakan bahwa perbuatan yang telah dilakukan adalah perbuatan memfitnah. Jika ia menuntut supaya

dinyatakan bahwa perbuatan itu adalah fitnah, maka berlakulah ketentuan-ketentuan dalam Pasal 314 Kitab Undang-undang Hukum Pidana tentang penuntutan perbuatan memfitnah. Jika diminta oleh pihak yang dihina, putusan akan ditempelkan di tempatkan di tempat umum, dalam jumlah sekian lembar dan tempat, sebagaimana diperintahkan oleh Hakim atas biaya si terhukum.

3. Pasal 1374 KUH Perdata Tanpa mengurangi kewajibannya untuk memberikan ganti rugi, tergugat dapat mencegah pengabulan tuntutan yang disebutkan dalam pasal yang lalu dengan menawarkan dan sungguh-sungguh melakukan di muka umum di hadapan Hakim suatu pemyataan yang berbunyi bahwa Ia menyesali perbuatan yang telah ia lakukan, bahwa Ia meminta maaf karenanya, dan menganggap orang yang dihina itu sebagai orang yang terhormat.

BAB VI
KESIMPULAN DAN SARAN

A. Kesimpulan

1. Perlindungan hukum atas kejahatan yang terjadi dalam jejaring sosial, internet dalam system dapat dipandang sebagai suatu Langkah maju, dimana pemerintah Indonesia telah mengesahkan. Suatu peraturan perundang-undangan yang secara khsusu mengatur seluruh kegiatan dalam dunia maya khususnya bagi permasalahan yang menyangkut cybercrime yaitu undang-undang no 11 tahun 2008 tentang informasi dan transaksi elektronik. Dengan disahkannya undang- undang tersebut membawa angin segar khususnya polri untuk menghadang laju kejahatan para cracker yang semakin banyak bermunculan di dunia cyber.
2. Perbuatan melanggar hukum yang dilakukan orang, individu dalam dunia maya adalah pencemaran nama baik dan kehormatan seseorang. Sehingga seseorang tersebut dirugikan, hal tersebut dapat diadukan dan selanjutnya dalam hal ini delik aduan yang mengacu pada pasal 310 ayat 2 KHUP tentang pencemaran nama baik, selain daripada itu juga diatur dalam undang- undang nomor 32 tahun 2002 tentang penyiaran dan undang- undang no 11 tahun 2008 tentang informasi dan transaksi elektronik.

B. Saran

1. Lembaga peradilan wewenangnya di perluas dengan mencakup segala Tindakan yang merupakan pelanggaran hak- hak pribadi orang dalam penggunaan system jejaring social baik itu pelanggaran yang bersifat

procedural atau bersifat administratif. Selain wewenangnya diperluas putusan peradilan juga diberi kekuatan memaksa bagi pelaksanaan putusannya dan tidak sekedar bersifat diktaktor tetapi juga bersifat comdenatoir, sehingga putusan peradilan dapat menjadi bentuk perlindungan bagi para pengguna teknologi internet yang benar- benar efektif dalam system peradilan di Indonesia.

2. Peraturan perundang- undangan di Indonesia tentang ITE harus lebih disempurnakan lagi dan diperluas cakupannya agar memberi kemudahan bagi para penegak hukum dalam melaksanakan tugasnya dan memberi rasa aman

Daftar Pustaka

Agus Raharjo, Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi. Citra Aditya Bakti, Bandung, 2002

Bartleby.com akkses 7 juni 2012

David I. Brainbridge. Computer dan hukum, sinar grafika. Jakarta. 1993. Hal 155

Dictionary.cambridge.org akses 7 juni 2012

Edmon Makarim, kompilasi hukum telematika. Rajawali Pres, Jakarta, 2003. Hal 388

http://te-effendi-pidana.blogspot.com/2009/03/korban-tindak-pidana-narkoba.html diakses pada tanggal 07 april 2010

Manap, Nazura Abdul, Anita Abdul Rahim, and Hossein Taji. "Cyberspace identity theft: The conceptual framework." Mediterranean Journal of Social Sciences 6, no. 4 (2015).

www.hukumonline.com ancaman pencemaran nama baik mengintai. Diakses pada 16 maret 2009

www.wikisource.com , cyberspace, akses dalam 14 Juni 2012

Maskun, M. (2012). CYBER CRIME SUATU PENGANTAR

Arief, B. N. (2005). Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana Edisi Revisi. Citra Aditya Bakti, Bandung.

UU ITE no 11 tahun 2008

KUH PERDATA

KUH PIDANA

UU No 36 Tahun 1999 tentang telekomunikasi