SISTEM PEMBUKTIAN CYBER CRIME DALAM TINDAK PIDANA PENCEMARAN NAMA BAIK MELALUI MEDIA SOSIAL

SKRIPSI

Disusun untuk memperoleh gelar Sarjana Hukum

Oleh
EDELWEISS PREMAULIDIANI PUTRI
15.0201.0091

PROGRAM STUDI ILMU HUKUM
FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH MAGELANG
2019

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Semakin berkembangnya penggunaan internet dan teknologi informasi sebagai media untuk bertransaksi dan berkomunikasi elektronik, maka akan semakin menjadikan kita akan lebih mudah dan cepat. Di sisi lain, juga memunculkan dampak yang besar terhadap meningkatnya kejahatan di dunia cyber. Keamanan Informasi dan Transaksi Elektronik (ITE) dan Kejahatan ITE selalu beradu dalam berbagai persoalan terkait dengan Informasi dan Transaksi Elektronik (ITE).

Sesuai dengan penjelasan pada UU ITE, Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Penyebab perubahan itu akibat masyarakat yang lebih banyak menggunakan ITE, dan hukum atau peraturan yang kurang mejerat para pelaku kejahatan tersebut sehingga banyak munculnya kejahatan seperti cybercrime atau kejahatan melalui jaringan internet adanya cybercrime telah menjadi ancaman stabilitas bagi negara, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan menggunakan teknologi komputer khususnya internet.

Teknologi informasi juga dapat merubah perilaku masyarakat, bahkan sekarang Teknologi Informasi saat ini menjadi pedang bermata dua buat kita karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum sehingga banyak perbuatan pidana terlepas dari jerat hukum.

Perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas sehingga menyebabkan perubahan sosial yang sangat cepat pada masyarakat. Sesuai dengan catatan Polda Metro Jaya Jakarta Selatan, kejahatan dunia cyber hingga pertengahan 2018 mencapai 1.603 kasus. Arga mengatakan kasus tersebut meliputi pencemaran nama baik, hate speech, spam, penyalahgunaan jaringan teknologi informasi, dan carding. Data dari Asosiasi Kartu Kredit Indonesia (AKKI) menunjukkan, sejak tahun 2003 hingga kini, angka kerugian akibat kejahatan kartu kredit mencapai Rp 30 milyar per-tahun (Ahmadjayadi, 2008). Menurut Wakil unit serse Bidang Monitoring dan Keamanan Jaringan ID-SIRTII/CC, Arga mengatakan saat ini kasus pelanggaran cyber crime tahun 2018 hingga awal oktober telah mencapai sekitar 1.603 kasus.Jumlah ini terus meningkat tiap tahunnya mencapai 100 persen. Di 2015 hanya 200 kasus setahun, 2016 naik 225 kasus, 2017 menjadi 199 kasus. (http://www.reskrimsus.metro.polri.go.id.di unduh Rabu 26 september 2018 Pukul 21.00 WIB)

Undang-Undang ITE ini dimaksudkan untuk menjawab permasalahan hukum yang seringkali dihadapi yaitu terkait dengan penyampaian informasi,

komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.namun kenyataan saat ini adalah ketidakmampuan sistem hukum konvensional dalam mengantisipasi dan menangani kasus kejahatan didunia maya. Hal ini di dasari oleh beberapa hal, misalnya persoalan tentang kegiatan dunia maya yang tidak dapat dibatasi oleh teritorial suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun.

Melihat kondisi tersebut, Didik M. Arief Mansur dan Alisatris Gultom menyatakan bahwa ketiadaan undang-undang yang menjadi penyebab tidak dapat dihukumnya pelaku kejahatan tidak dapat dibiarkan berlarut-larut, karena apabila hal ini tidak segera diselesaikan akan menimbulkan keresahan di masyarakat dan pada akhirnya hukum akan kehilangan wibawanya. Selanjutnya dinyatakan, ironis memang, pada saat kejahatan didunia maya (*cyber crime*) semakin meningkat jumlahnya, ternyata masih banyak pelaku yang tidak dapat diadili akibat ketiadaan undang-undang. Akibatnya, sangat wajar apabila kejahatan didunia maya (cyber crime) semakin meningkat dari waktu ke waktu.

Sejalan dengan hal diatas, Sutanto dkk menyatakan bahwa persoalan hukum yang muncul bukan hanya akibat adanya suatu kegiatan yang merugikan pihak lain dalam lingkup yang kecil. Berbagai kasus telah mengindikasikan tingkat kejahatan yang dilakukan sudah sedemikian luas,

mulai dari kasus pencemaran nama baik, hingga isu-isu yang menimbulkan masalah regional, bahkan global misalnya isu terorisme.

Esensi Undang-Undang Informasi dan Transaksi Elektronik melingkupi seluruh transaksi berbasis elektronik seperti komputer serta jaringan dan memiliki kekuatan hukum. Undang-Undang ITE dipersepsikan sebagai cyberlaw di Indonesia, yang diharapkan bisa mengatur segala urusan dunia internet (cyber), termasuk didalamnya memberi hukuman terhadap pelaku cybercrime guna melindungi masyarakat dari kejahatan di dunia maya.(Wahono, 2008)

Pada akhirnya, tepat apa yang dikemukakan oleh Ahmad M. Ramli dkk, bahwa kegiatan *cyber* meskipun bersifat virtual tetapi dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis, terhadap ruang *cyber* sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi konvensional untuk dijadikan obyek dan perbuatan. Sebab, jika cara ini ditempuh maka akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan *cyber* adalah kegiatan *virtual* tetapi berdampak sangat nyata meskipun alat uktinya bersifat elektronik. Oleh karena itu, subyek pelakunya harus dikualifikasikan pula sebagai telah melakukan perbuatan hukum secara nyata. Perkembangan terbaru dalam hukum pidana (khususnya hukum acara pidana) sebetulnya telah berupaya untuk mengakomodasi perkembangan teknologi informasi ini. Misalnya, dalam UU No. 20 tahun 2001 jo. UU. No.31 tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi telah memasukkan alat bukti

elektronik sebagai alat bukti yang sah, dalm bentuk “petunjuk”. Hal ini diatur dalam pasal 26 A dengan menyatakan sebagai berikut:

Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam pasal 188 ayat (2) undang-undang No. 8 tahun 1981 tentang Hukum acara pidana, khususnya untuk tindak pidana korupsi juga diperoleh dari :

1. Alat bukti yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpansecara elektronik dengan alat optikatau yang serupa dengan itu; dan
2. Dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang diatas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka atau perforasi yang memiliki makna.

Kemudian dalam penjelasan pasal demi pasalnya disebutkan bahwa yang dimaksud dengan “ disimpan secara elektronik” misalnya data yang disimpan dalam mikro film, compact disk read only memory (CD-ROM) atau write once read many (WORM).

Sedangkan yang dimaksud dengan “alat optik atau yang serupa dengan itu” adalah tidak terbatas pada data penghubung elektronik (elektronic data interchage), surat elektronik (e-mail), telegram, teleks, dan faksmili.

Ketentuan tersebut mengisyaratkan secara eksplisit akan pengakuan secara hukum atas perkembangan penyalahgunaan teknologi informasi.

Khususnya penyalahgunaan internet. Dengan kata lain, perkembangan teknologi komputer dan internet dapat dijadikan sebagai sarana untuk melakukan kejahatan. Sarana itulah yang diakui oleh UU No. 20 tahun 2001 sebagai salah satu alat bukti yang sah.

Namun demikian, permasalahan akan muncul tatkala undang-undang tersebut merujuk pada KUHAP sebagai acuan dalam penyidikan, penuntutan maupun pemeriksaan dipengadilan. Hal itu disebabkan dalam KUHAP diatur bahwa alat bukti yang sah hanya meliputi :

1. Keterangan Saksi
2. Keterangan Ahli
3. Surat
4. Petunjuk; dan
5. Keterangan Terdakwa.

Sehubungan dengan itu, banyak kalangan yang mengusulkan bahwa KUHAP juga perlu direvisi. Disesuaikan pengaturan alat buktinya dengan perkembangan teknologi informasi, sebagaimana yang telah diatur dalam UU tindak pidana korupsi, maupun undang-undang yang lainnya, yang telah memasukkan data elektronik sebagai alat bukti.

Dalam upaya menghindari adanya ketidakadilan bagi korban maka diperlukan kemampuan dan keberanian aparat penegak hukum untuk melakukanpenemuan hukum. Hal ini dapat dilakukan dengan menerapkan merode interprestasi (penafsiran) hukum sebelum adanya payung hukum

yang memadai. Sehingga, diharapkan tidak akan terjadi kekosongan hukum dalam menuntut dan mengadili para pelaku cyber crime di indonesia.

Berdasarkan latar belakang diatas, menarik minat penulis untuk mengetahui lebih dalam mengenai kendala yuridis pembuktian dalam tindak pidana Informasi dan Transaksi Elektronik. Adapun Judul penelitian ini ***"SISTEM PEMBUKTIAN CYBER CRIME DALAM TINDAK PIDANA PENCEMARAN NAMA BAIK MELALUI MEDIA SOSIAL"***

B. Rumusan Masalah

1. Apakah hal-hal yang dapat dijadikan alat bukti dalam tindak pidana pencemaran nama baik?
2. Apakah hambatan penyidik dalam menemukan barang bukti untuk mengungkap tindak pidana tersebut?
3. Apa upaya penyidik untuk mengatasi hambatan tersebut?

C. Tujuan Penelitian

Berdasarkan hal tersebut, tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk mengetahui alat bukti dalam tindak pidana pencemaran nama baik
2. Untuk mengetahui kendala apa saja yang dihadapi pengadilan dalam menanggulangi cyber crime, serta kendala-kendala Aparat Kepolisian dalam melakukan proses penyidikan terkait dengan pengumpulan alat-alat bukti kejahatan dunia maya (cyber crime)
3. Untuk mengetahui upaya-upaya yang dapat dilakukan oleh Aparat Kepolisian dalam melakukan proses pembuktian pada para pelaku tindak

pidana cyber crime. Mengingat sulitnya proses pemidanaan terkait dengan sedikitnya alat bukti dalam tindak pidana tersebut.

D. Manfaat Penelitian

Hasil penelitian ini diharapkan dapat bermanfaat baik bagi peneliti, masyarakat, maupun bagi ilmu pengetahuan.

1. Bagi Peneliti

   Hasil penelitian ini diharapkan dapat menambah wawasan dan pengetahuan khususnya mengenai tindak pidana yang dijerat dalam Undang-Undang Informasi dan Transaksi Elektronik dan memberikan arahan kepada penulis untuk melangkah ke jalur profesional dan derajat pendidikan selanjutnya, serta untuk memenuhi syarat guna mencapai derajat sarjana pada Fakultas Hukum Universitas Muhammadiyah Magelang.

2. Bagi Masyarakat

   Hasil dari penelitian ini, diharapkan dapat memberikan pengetahuan lebih tentang hukum diindonesia, karena selama ini masyarakat cenderung tidak peduli selama dirinya tidak dirugikan. Sebenarnya, secara tidak langsung masyarakat awam juga ikut dirugikan, dengan adanya kerugian yang dialami oleh negara baik secara materiil maupun moril.

3. Bagi para pelaku cyber crime

   Bagi pelaku kejahatan komputer, bahwa kejahatan yang mereka lakukan dapat dijerat dengan pidana yang cukup berat, karena pihak yang dirugikan

cukup banyak, termasuk negara-negara di dunia. Oleh karena itu dibutuhkan banyak pengetahuan bagi mereka tentang hukum di Indonesia.

4. Bagi Pemerintah (kepolisian, dinas sosial, dan Kejaksaan Negeri)

   Perlu adanya suatu bentuk sosialisasi hukum dan pelaksanaannya secara menyeluruh dan merata, khususnya pada kalangan muda yang bergelut dibidang yang memiliki intensitas tinggi dengan hal-hal yang mendekati perbuatan melawan hukum, serta adanya pemberian struktur keamanan lebih pada segala mediasi yang mendukung terjadinya tindak pidana cyber crime, agar dapat mengurangi jumlah angka tindak pidana ini.

5. Bagi Pengetahuan

   Penelitian ini diharapkan dapat memberi masukan khususnya bagi para akademis dan praktisi hukum. Dengan adanya penelitian ini diharapkan juga dapat memberikan kontribusi, referensi atau bahan bacaan tambahan bagi mahasiswa maupun masyarakat luas.

E. Sistematika Penulisan

Dalam sub bab ini diberikan gambaran yang jelas dan terarah mengenai penyusunan proposal skripsi. Berikut dikemukakan sistematika dan alur pembahasan yang terbagi dalam :

BAB I : PENDAHULUAN

Berisi tentang latar belakang dari permasalahan-permasalahan yang timbul dari kejahatan dunia maya (cyber crime), serta dampak dari akibat perbuatan tersebut. selain itu juga berisi

perumusan masalah, tujuan dan kegunaan serta metode analisis data yang dilakukan dalam penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini diuraikan tentang pengertian tindak pidana menurut para ahli, pengertian tindak pidana menurut Undang-Undang Nomor 19 tahun 2016 tentang informasi dan transaksi elektronik, pengertian informasi dan transaksi elektronik menurut Undang-Undang Nomor 19 tahun 2016 tentang informasi dan transaksi elektronik, pengertian komputer, pengertian dokumen elektronik, pengertian kejahatan dunia maya (cyber crime) dan hukum-hukumnya, pengertian pencemaran nama baikmenurut para ahli, pengertian pencemaran nama baik menurut KUHP, serta jenis-jenis dari kejahatan dunia maya berikut dengan pengertiannya, sistem pembuktian.

BAB III : METODE PENELITIAN

Dalam bab ini akan dijelaskan mengenai jenis metode pendekatan yang digunakan oleh peneliti dalam melakukan penelitian, penelitian ini dilakukan dengan menggunakan pendekatan normatif, tinjauan yuridis normatif, yaitu dengan mengkaji literatur-literatur yang berkaitan, pendapat para ahli-ahli hukum terkait dan analisa kasus dalam dokumen-dokumen untuk memperjelas hasil penelitian.

BAB IV : HASIL PENELITIAN DAN PEMBAHASAN

Dalam bab ini menjelaskan mengenai hasil penelitian beserta pembahasannya, dimana hasil penelitiannya merupakan pemecahan masalah tentangperumusan sistem pembuktian pencemaran nama baik melalui media sosial, hambatan penyidik dalam menemukan alat bukti, serta upaya penyidik dalam mengatasi suatu hambatan

BAB V : PENUTUP

Dalam bab ini akan berisi kesimpulan dari hasil pembahasan bab-bab sebelumnya dan berisi saran-saran yang diharapkan dapat menjadi masukan yang berguna dan bermanfaat bagi instansi yang terkait.

BAB II

TINJAUAN PUSTAKA

A. Pengertian dan Unsur-Unsur Tindak Pidana

1. Pengertian Tindak Pidana

Istilah tindak pidana merupakan terjemahan dari "*strafbaar feit*" perbuatan yang dilarang oleh suatu aturan hukum larangan dengan mana disertai ancaman(sanksi) yang berupa pidana tertentu, bagi barang siapa yang melanggar larangan tersebut. Kitab Undang-undang Hukum Pidana tidak terdapat penjelasan mengenai apa sebenarnya yang dimaksud dengan *strafbaarfeit* itu sendiri. Tindak pidana biasanya disamakan dengan delik, yang berasal dari bahasa latin yakni kata *delictum.*

Delik tercantum dalam Kamus Besar Bahasa Indonesia sebagai berikut : "Delik adalah perbuatan yang dapat dikenakan hukuman karena merupakan pelanggaran terhadap undang-undang tindak pidana". Pengertian tindak pidana adalah tindakan yang tidak hanya dirumuskan oleh KUHP, Istilah tindak pidana sebagai terjamahan dari *strafbaarfeit* menunjukkan pengertian gerak-gerik tingkah laku seseorang. Hal-hal tersebut terdapat juga seseorang untuk tidak berbuat, akan tetapi dengan tidak berbuatnya dia, dia telah melakukan tindak pidana. Mengenai kewajiban untuk berbuat tetapi tidak berbuat, yang di dalam undang-undang menentukan pada Pasal 164 KUHP, ketentuan dalam pasal ini mengharuskan seseorang untuk melaporkan kepada pihak yang berwajib

apabila akan timbul kejahatan, ternyata dia tidak melaporkan, maka ia dapat dikenai sanksi.

Seperti diketahui istilah *strafbaarfeit* telah diterjemahkan ke dalam bahasa Indonesia yang menimbulkan berbagai arti, umpamanya saja dapat dikatakan sebagai perbuatan yang dapat atau boleh dihukum, peristiwa pidana, perbuatan pidana, tindak pidana. Para sarjana Indonesia mengistilahkan *strafbarfeit* itu dalam arti yang berbeda, diantaranya Moeljatno menggunakan istilah perbuatan pidana, yaitu : "perbuatan yang dilarang oleh suatu aturan hukum, larangan mana disertai ancaman sanksi yang berupa pidana tertentu, bagi barang siapa larangan tersebut".

Sementara Menurut Pompe, *strafbaarfeit* adalah Suatu pelanggaran norma (gangguan terhadap tata tertib hukum) yang dengan sengaja ataupun dengan tidak sengaja telah dilakukan oleh seorang pelaku, dimana penjatuhan hukuman terhadap pelaku tersebut adalah perlu demi terpeliharanya tertib hukum dan terjaminnya kepentingan hukum.

Menurut E.Utrecht, *strafbaarfeit* dengan isilah peristiwa pidana yang sering juga ia sebut delik, karena peristiwa itu suatu perbuatan (*handelen* atau *doen positif*) atau suatu melalaikan (*natalen-negatif*), maupun akibatnya (keadaan yang ditimbulkan karena perbuatan atau melalaikan itu).

Menurut Moeljatno menyatakan bahwa **Tindak Pidana** berarti perbuatan yang dilarang dan diancam dengan pidana, terhadap siapa saja

yang melanggar larangan tersebut. Perbuatan tersebut harus juga dirasakan oleh masyarakat sebagai suatu hambatan tata pergaulan yang dicita-citakan oleh masyarakat.(Sudarto, 1989)

Dengan demikian dapat disimpulkan bahwa tindak pidana bersifat melawan hukum, yaitu harus benar-benar dirasakan oleh masyarakat sehingga perbuatan yang tidak patut dilakukan. Jadi meskipun perbuatan itu memenuhi rumusan undang-undang, tetapi apabila tidak bersifat melawan hukum, maka perbuatan itu bukan merupakan suatu tindak pidana. (Djajuli, 1989)

Pengertian perbuatan ternyata yang dimaksudkan bukan hanya berbentuk positif, artinya melakukan sesuatu atau berbuat sesuatu yang dilarang, dan berbentuk negatif, artinya tidak berbuat sesuatu yang diharuskan. Perbuatan yang dapat dikenakan pidana dibagi menjadi dua yakni sebagai berikut:

1. Perbuatan yang dilarang oleh Undang-undang.
2. Orang yang melanggar larangan itu.

Beberapa Unsur-unsur tindak pidana sebagai berikut:

a. Unsur Objektif Unsur yang terdapat di luar si pelaku.

Unsur-Unsur yang ada hubungannya dengan keadaan di mana tindakan-tindakan si pelaku itu harus dilakukan terdiri dari:

1 Sifat melanggar Hukum.

2 Kualitas dari si pelaku.

3 Kausalitas yaitu hubungan antara suatu tindakan sebagai penyebab dengan suatu kenyataan sebagai akibat.

b. Unsur Subjektif Unsur yang terdapat atau melekat pada diri si pelaku, atau yang di hubungkan dengan diri si pelaku dan termasuk di dalamnya segala sesuatu yang terkandung di dalam hatinya. Unsur ini terdiri dari :

1 Kesengajaan atau ketidaksengajaan (dolus atau culpa).

2 Maksud pada suatu percobaan, seperti di tentukan dalam Pasal 53 ayat 1 KUHP.

3 Macam-macam maksud seperti terdapat dalam kejahatan, pencurian, penipuan, pemerasan, dan sebagainya.

4 Merencanakan terlebih dahulu seperti tercantum dalam pasal 340 KUHP, yaitu pembunuhan yang direncanakan terlebih dahulu.

5 Perasaan takut seperti terdapat di dalam Pasal 308 KUHP.(Moeltjatno, 1987)

B. Pengertian Tindak Pidana Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik

Menurut Josua Sitompul menjelaskan mengenai delik kejahatan internet yang diatur dalam UU ITE, antara lain:

1. Tindak Pidana yang berhubungan dengan aktivitas ilegal, yaitu:
    a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal, yang terdiri dari:
        - Kesusilaan (Pasal 27 ayat (1) UU ITE)
        - Perjudian (Pasal 27 ayat (2) UUITE)
        - Penghinaan atau Pencemaran Nama Baik (Pasal 27 ayat (4) UU ITE)
        - Berita Bohong yang menyesatkan dan merugikan konsumen (*HOAX* - Pasal 28 ayat (1) UU ITE)
        - Menimbulkan Rasa Kebencian berdasarkan SARA (*Hate Speech*- Pasal 28 ayat (2) UU ITE)
        - Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE)
    b. Dengan cara apapun melakukan Akses Ilegal (Pasal 30 UU ITE)
    c. Intersepsi Ilegal terhadap Informasi atau Dokumen Elektronik dan Sistem Elektronik (Pasal 31 UU ITE)
2. Tindak Pidana yang berhubungan dengan gangguan (*interferensi*), yaitu:
    a. Gangguan terhadap Informasi atau Dokumen Elektronik (*Data Interference*- pasal 32 UU ITE)
    b. Gangguan terhadap Sistem Elektronik (*System Interference*- Pasal 33 UU ITE)
3. Tindak Pidana memfasilitasi perbuatanyang dilarang (Pasal 34 UU ITE)

4. Tindak Pidana Pemalsuan Informasi atau Dokumen Elektronik (Pasal 35 UU ITE)
5. Tindak Pidana Tambahan (*Accessoir* – Pasal 36 UU ITE) dan
6. Pemberatan-Pemberatan terhadap ancaman pidana (Pasal 52 UU ITE)

C. Pengertian Informasi Dan Transaksi Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik

Dalam ketentuan umum pasal 1 Undang-Undang Nomor 16 Tahun 2016 tentang informasi dan transaksi elektronik disebutkan, bahwa informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, elektronic data interchange (EDI), surat elektronik (elektronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Sedangkan Transaksi elektronik adalah perbuatan hukum yang dilakukan menggunakan komputer, jaringan komputer, dan atau media elektronik lainnya.

D. Pengertian Komputer

Institut komputer indonesia mendefinisikan komputer sebagai berikut:

"Suatu rangkaian peralatan-peralatan dan fasilitas yang bekerja secara elektronis, bekerja dibawah kontrol suatu operating system, melaksanakan pekerjaan berdasarkan rangkaian instruksi-instruksi yang disebut program serta mempunyai internal storage yang digunakan untuk menyimpan operating system, program dan data yang diolah."

Operating system berfungsi untuk mengatur dan mengkontrol sumber daya yang ada, baik dari hardware berupa komputer, Central Processing Unit (CPU) dan memory / storage serta software komputer yang berupa program-program komputer yang dibuat oleh programmer. Jenis-jenis operating sytem antara lain: PC-DOS System, UNIX, Microsoft Windows, dan lain-lain.

E. Pengertian Dokumen Elektronik

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 memsiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

F. Pengertian dan Jenis-Jenis Cybercrime

A. Pengertian Cybercrime

Kejahatan adalah perbuatan merugikan orang lain dan/atau sekelompok orang dan/atau instansi yang dilakukan dengan bertujuan untuk menguntungkan diri sendiri, baik secara materi maupun kejiwaannya.(P.H., Skripsi, 2010) Kejahatan dapat dilakukan dengan menggunakan fasilitas apapun sebagai alat untuk melakukan perbuatannya, termasuk didalamnya adalah perangkat Informasi dan Transaksi Elektronik, contohnya seperti komputer, credit card, televisi, dan lain sebagainya (Raharjo, 2002).

Menurut Dan Koeing tindak pidana Cyber Crime adalah menitik beratkan pada penggunaan teknologi computer dalam melakukan kejahatan baik kejahatan baru maupun kejahatan tradisional(Suseno, 2012).

Istilah hukum cyber digunakan dalam tulisan ini dilandasi pemikiran, bahwa cyber jika diidentikan dengan dunia maya akan cukup menghadapi persoalan ketika terkait dengan pembuktian dan penegakan hukumnya mengingat para penegak hukum akan menghadapi kesulitan jika harus membuktikan suatu persoalan yang diasumsikan sebagai “maya” yaitu sesuatu yang tidak terlihat atau semu.

B. Jenis-Jenis Cyber Crime

Dalam realitasnya, penyalahgunaan internet dapat dilakukan dengan berbagai macam dan cara. Berikut ini akan diuraikan beberapa jenis cyber

crime, seperti kejahatan dalam aspek *e-Commerce, Cyber Sex, Hacker, dan Merusak Situs Milik Negara.*

1. E-Commerce

   Kegiatan perdagangan yang dilakukan melalui layanan elektronik, dalam hal ini melalui sarana internet, baik sistem promosi, sistem transaksi, sistem pembayaran, dan lain-lain. Landasan yang dipakai adalah *electronic based* dan *Information Technology*, khususnya Internet dan Web.

   Dengan hadirnya *E-Commerce*, perdagangan dapat dilakukan sangat efektif, karena publik dapat mengakses suatu toko dari rumah masing-masing, tanpa harus memasuki toko atau perusahaan tersebut. *Web Site* perusahaan dapat dianggap sebagai sebuah toko, karena dalam *web site* itu tersedia ruangan-ruangan maya yang menyediakan layanan spesifikasi barang-barang yang diperdagangkan. Adapun kejahatan dalam *E-Commerce* meliputi:

   a. Pembobolan Kartu Kredit melalui Internet.

      Tersangka PETRUS PANGKUR alias BONY DIOBOK-OBOK, yang diputus oleh Pengadilan Negeri Sleman dengan hukuman penjara satu tahun penjara, dalam Perkara Nomor: 94/Pid.B/2002/PN.SLMN, tanggal 23 Agustus 2002, dalam perkara Tindak Pidana Penipuan dan atau Pemalsuan, pada tanggal 1 Maret 2001 dengan memesan barang berupa Helm, Sarung tangan melalui E-Commerce dengan account Kenny-jr@indonet.com dan

bonz.2000@licos.com dan melakukan pembayaran dengan kartu kredit milik orang lain yang diperoleh dengan carding atas kartu kredit VSA nomor 4388.5750.4013.3006, dan tersangka pada tanggal 8 Maret menerima kiriman barang yang dipesan itu melalui jasa paket UPS Yogyakarta.

b. Pemelesetan WWW.klikbca.com

Pada Bulan Juni 2001, STEVEN HARYONO sempat membuat gempar dunia TI indonesia, dengan kasus pemelesetan www.klik.bca.com . motivasinya sebenarnya adalah untuk membuat kita semua melek terhadap masalah keamanan internet khususnya Internet Banking.

Lima situs dari hasil pelesetan situs BCA tersebut telah berhasil memperoleh sekitar 130 PIN milik pengunjung yang tersesat secara tidak sadar. Peristiwa ini memicu berbagaiperdebatan sengit, baik dari segi hukum, keamanan internet. Dampak dari kejadian ini, pihak BCA merasa dirugikan dan Steven Haryono sendiri diancam terkena tindakan hukum. Namun dukungan dari komunitas teknologi informasi (TI) dan para hacker pada khususnya menjadikan kasus ini berhenti sampai pada pro kontra pendapat didalam masyarakat.

Adapun motif kejahatan yang terjadi dalam komunitas E-Commerce ini, bisa berbentuk pemalsuan kartu kredit, persaingan

usaha tidak sehat, monopolo barang perdagangan, Haki, dan lain-lain.

2. Cybersex

Cybersex adalah dunia pornografi yang dilakukan di internet, yang dapat diakses secara bebas. Ada yang membayar terlebih dahulu melalui pendaftaran dan pembayaran dengan kartu kredit, namun ada juga yang gratis. Situs ini dapat diakses bebas, meskipun mereka mengakses ini masih belum cukup umur. Dan di cafe internet ataupun di penyedia layanan internet lainnya tidak ada aturan perbatasan umur, pembatasan akses, dan aturan lain yang membatasi akses, dan aturan lain yang membatasi akses yang negatif

Dalam situs internet dapat dicari apa saja tentang *pornografi*, dan ini akan mempengaruhi orang-orang yang mengaksesnya. Apabila kemudian aplikasi dalam kehidupan bermasyarakat maka akan terjadi perbuatan asusila.

Keadaan ini tidak dapat dibiarkan secara terus menerus, karena dapat merusak moral bangsa. Atau setidak-tidaknya ada rambu-rambu khusus untuk mengatur hal ini, karena situs ini bergerak ke seluruh dunia tanpa batas.

Pada bulan Mei 2003 satuan Reskrimsus cyber crime Polda Metro Jaya menangkap mucikari cyber. Pelakunya *sepasang* suami istri, Ramdoni alias Rino dan Yanti Sari alias Bela. Prostitusi cyber ini

adalah modus baru, menawarkan berbagai wanita melalui sebuah alamat web.

Dalam web tersebut ditampilkan deretan foto wanita bentuk close up atau dalam busana minim, yang siap *melayani* pria. Pengelola situs nampaknya tidak malu-malu menampilkan nomor telepon genggamnya, sehingga para peminat bisa memesan wanita yang dikehendaki, lalu pesanan tersebut diantar ke hotel atau apartemen sesuai pesanan.

Menurut Ari Juliano Gema, sebagaimana dikutip oleh Abdul *Wahid* dan Mohammad Labib, menyatakan bahwa cyber crime dapat dikelompokkan dalam beberapa bentuk, yaitu:

1. Unauthorized acces to computer system and service, Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan computer yang dimasukinya.
2. Illegal contents, Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggarhukum atau mengganggu ketertiban umum
3. Data forgery, Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet

4. Cyber espionage, Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.
5. Cyber sabotage and extortion, Kejahatan ini dilakukan dengan membuat gangguan perusakan atau penghancuran terhadap suatu data, program computer atau sistem jaringan computer yang terhubung dengan internet.
6. Offense against intellectual property, Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Seperti peniruan tampilan pada web page suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain dan sebagainyaInfrengments of privacy, Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain akan dapat merugikan korbannya secara materiil maupun immaterial seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

G. Pengertian dan Macam-Macam Pencemaran Nama Baik

A. Pengertian Pencemaran Nama Baik

Pencemaran nama baik atau fitnah adalah salah satu cara yang paling banyak dilakukan untuk melawan media masa, sehingga *"Netizen"* sebutan untuk pengguna dunia maya atau media sosial merasa sangat terbatas dalam menuangkan ekspresinya menggunakan media sosial. Belakangan ini persoalan eksistensi delik menjadi persoalan yang sangat dipermasalahkan oleh berbagai pihak, sehingga munculnya perhatian publik terhadap kasuskasus tertentu sering terjadi. Pasal-pasal pencemaran nama baik sering digunakan untuk menjerat *"Whistle Blower"*(Perlakuan bagi Pelapor Tindak Pidana).

Dalam SEMA disebutkan, *Whistle Blower* adalah Pihak yang mengetahui dan melaporkan tindak pidana tertentu dan bukan merupakan bagian dari pelaku kejahatan yang dilaporkannya. Wakil menteri Hukum dan HAM Denny Indrayana mengatakan, menjadi *whistle blower* memiliki perlindungan sesuai ketentuan pasal 10 Undang-Undang No.13 Tahun 2006 tentang Perlindungan Saksi Korban.

Pasal itu menyebutkan, *whistle blower* atau saksi pelapor tidak dapat dituntut secara hukum baik pidana maupun perdata atas laporan, kesaksian yang akan, sedang atau yang telah diberikan. Namun kesaksiannya dapat dijadikan pertimbangan hakim dalam meringankan pidananya.

Terdapat dua jenis *"Whistle Blower"* yaitu (Niniek Suparni, 2009 : 111) :

a) Seseorang yang mengungkapkan pelanggaran atau perbuatan salah yang terjadi dalam suatu organisasi kepada publik atau orang yang memiliki otoritas.
b) Seseorang pekerja yang memiliki pengetahuan atau informasi dari dalam tentang akti
c) fitas illegal yang terjadi di dalam organisasinya dan melaporkannya kepada publik.

B. Pencemaran Nama Baik Menurut KUHP

Salah satu perbuatan pidana yang sering mengundang perdebatan di tengah masyarakat adalah pencemaran nama baik. Dalam peraturan perundang-undangan di Indonesia, pencemaran nama baik (penghinaan) diatur dan dirumuskan dalam Pasal 310 KUHP. yang terdiri dari 3 (tiga) ayat. Dalam ayat (1) dinyatakan bahwa barangsiapa sengaja menyerang kehormatan atau nama baik seseorang, dengan menuduh sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran, dengan pidana penjara paling lama sembilan bulan atau denda paling banyak tiga ratus rupiah. Selanjutnya ayat (2) menyatakan bahwa apabila perbuatan tersebut dilakukan dengan tulisan ataugambaran yang disiarkan, dipertunjukan atau ditempelkan di muka umum, maka yang bersalah, karena pencemaran tertulis, diancam pidana penjara paling lama satu tahun empat bulan atau denda paling banyak tiga ratus rupiah.

Sebaliknya, ayat (3) menegaskan bahwa tidak merupakan pencemaran atau pencemaran tertulis, jika perbuatan terang dilakukan demi kepentingan umum atau karena terpaksa untuk bela diri. Dari ketentuan Pasal 310, telah dirumuskan tindakan Pencemaran Nama Baik itu dapat berupa:

1 Menista dengan lisan (*smaad*) - Pasal 310 ayat (1),

2 Menista dengan surat (*smaadschrift*) - Pasal 310 ayat (2). Sedangkan perbuatan yang dilarang adalah perbuatan yang dilakukan "*dengan sengaja*" untuk melanggar kehormatan atau menyerang kehormatan atau nama baik orang lain. Dengan demikian, unsur-unsur Pencemaran Nama Baik atau penghinaan (menurut Pasal 310 KUHP) adalah:

   a. dengan sengaja;

   b. menyerang kehormatan atau nama baik;

   c. menuduh melakukan suatu perbuatan;

3 Menyiarkan tuduhan supaya diketahui umum. Apabila unsur-unsur penghinaan atau Pencemaran Nama Baik ini hanya diucapkan (*menista dengan lisan*), maka perbuatan itu tergolong dalam Pasa1 310 ayat (1) KUHP. Namun, apabila unsur-unsur tersebut dilakukan dengan surat atau gambar yang disiarkan, dipertunjukkan atau ditempelkan (*menista dengan surat*), maka pelaku dapat dijerat atau terkena sanksi hukum Pasal 310 ayat (2) KUHP. Hal-hal yang menjadikan seseorang tidak dapat dihukum dengan pasal Pencemaran Nama Baik atau Penghinaan adalah:

   a. Penyampaian informasi itu ditujukan untuk kepentingan umum.

b. Untuk membela diri.

c. Untuk mengungkapkan kebenaran.

Dengan demikian, orang yang menyampaikan informasi, secara lisan ataupun tertulis diberi kesempatan untuk membuktikan bahwa tujuannya itu benar. Kalau tidak bisa membuktikan kebenarannya, itu namanya penistaan atau fitnah. Berdasarkan rumusan pasal di atas dapat dikemukakan bahwa pencemaran nama baik bisa dituntut dengan Pasal 310 ayat (1) KUHP, apabila perbuatan tersebut harus dilakukan dengan cara sedemikian rupa, sehingga dalam perbuatannya terselip tuduhan, seolah-olah orang yang dicemarkan (dihina) itu telah melakukan perbuatan tertentu, dengan maksud agar tuduhan itu tersiar (diketahui oleh orang banyak). Perbuatan yang dituduhkan itu tidak perlu perbuatan yang menyangkut tindak pidana (menipu, menggelapkan, berzina dan sebagainya), melainkan cukup dengan perbuatan biasa seperti melacur di rumah. pelacuran. Meskipun perbuatan melacur tidak merupakan tindak pidana, tetapi cukup memalukan pada orang yang bersangkutan apabila hal tersebut diumumkan. Tuduhan itu harus dilakukan dengan lisan, karena apabila dilakukan dengan tulisan atau gambar, maka perbuatan tersebut digolongkan pencemaran tertulis dan dikenakan Pasal 310 ayat (2) KUHP. Kejahatan pencemaran nama baik ini juga tidak perlu dilakukan di muka umum, cukup apabila dapat dibuktikan bahwa terdakwa mempunyai maksud untuk menyiarkan tuduhan tersebut. Pencemaran nama baik (menista) sebenarnya merupakan bagian dari bentuk penghinaan yang

diatur dalam Bab XVI KUHP. Pengertian "*penghinaan*" dapat ditelusuri dari kata "*menghina*" yang berarti "*menyerang kehormatan dan nama baik seseorang*". Korban penghinaan tersebut biasanya merasa malu, sedangkan kehormatan di sini hanya menyangkutnama baik dan bukan kehormatan dalam pengertian seksualitas. Perbuatan yang menyinggung ranah seksualitas termasuk kejahatan kesusilaan dalam Pasal 281-303 KUHP Penghinaan dalam KUHP terdiri dari pencemaran atau pencemaran tertulis (Pasal 310), fitnah (Pasal 311), penghinaan ringan (Pasal 315), mengadu dengan cara memfitnah (Pasal 317) dan tuduhan dengan cara memfitnah (Pasal 1318)

a. Memfitnah -- Laster [Pasal 311 ayat (1) KUHP]

Pasal 311 ayat (1) KUHP berbunyi: "Barangsiapa melakukan kejahatan menista atau menista dengan tulisan, dalam hal ia diizinkan untuk membuktikan dan jika tuduhan itu dilakukannya sedang diketahuinya tidak benar, dihukum karena salah memfitnah dengan hukuman penjara selamalamanya empat tahun."

Jika kita bandingkan antara kejahatan memfitnah (*laster*) dan kejahatan menista (*smaad*) atau penghinaan/Pencemaran Nama Baik, maka perbedaan itu terletak dari ancaman hukumannya. Namun demikian, pada intinya, kejahatan memfitnah ini juga merupakan kejahatan Pencemaran Nama Baik. Hanya saja, memfitnah ini mempunyai unsur-unsur yang lain. Unsur-unsur memfitnah, yaitu:

1. Seseorang melakukan kejahatan menista (*smaad*) atau menista dengan tulisan.
2. Apabila orang yang melakukan kejahatan itu "diberikan kesempatan untuk membuktikan kebenaran dari tuduhannya itu", dan bila
3. Setelah diberikan kesempatan tersebut, ia tidak dapat membuktikankebenarannya daripada tuduhannya itu, dan
4. Melakukan tuduhan itu dengan sengaja walaupun diketahuinya tidak benar. Salah satu unsur daripada delik fitnah (*lasterdelict*) ini adalah bahwa kepada orang yang melakukan kejahatan menista atau menista dengan tulisan itu diberi kesempatan untuk membuktikan kebenarannya daripada tuduhan yang dilancarkannya.

C. Macam-Macam Pencemaran Nama Baik

1. Penghinaan Ringan Penghinaan biasa atau penghinaan ringan ini diatur dalam Pasal 315 KUHP.

   Jika penghinaan (*Pencemaran Nama Baik*) itu dilakukan dengan jalan menuduh seseorang telah "*melakukan suatu perbuatan*", maka hal itu tergolong Pasal 310 dan 311 KUHP. Namun, apabila dengan jalan atau cara lain, seperti misalnya mengumpat atau memaki-maki dengan kata-kata keji yang menurut pendapat umum dapat digolongkan sebagai kata-kata penghinaan, maka hal ini tergolong memenuhi unsur Pasal 315 KUHP yang disebut penghinaan ringan atau biasa. Pasal 315

KUHP berbunyi: "Tiap-tiap penghinaan dengan sengaja yang tidak bersifat mencemar atau mencemar dengan surat yang dilakukan terhadap seseorang, baik di muka umum dengan lisan atau dengan surat, baik di muka orang itu sendiri dengan lisan atau dengan perbuatan, atau dengan surat yang dikirimkan atau diterimakan kepadanya, karena bersalah melakukan penghinaan ringan, dipidana dengan pidana penjara selama-lamanya empat bulan dua minggu atau dengan sebanyak-banyaknya empat ribu lima ratus rupiah." Dari ketentuan Pasal 315 KUHP ini, maka unsur-unsur penghinaan ringan ini adalah:

a. setiap penghinaan yang dilakukan dengan sengaja;
b. penghinaan itu tidak boleh bersifat menista atau menista dengan surat (*smaad atau smaadschrift*);
c. Dilihat dari cara perbuatan itu dilakukan, yaitu dengan syarat salah satu atau semua jenis perbuatan ini dilakukan:
    1. di tempat umum dengan lisan atau dengan tulisan;
    2. di depan atau di hadapan orang yang dihina dengan lisan atau dengan perbuatan-perbuatan;
    3. secara tertulis yang dikirimkan atau yang disampaikan kepada yang terhina.

2. Memfitnah dengan Pengaduan (*lasterlijke aanklacht*)

Yang dimaksud memfitnah dengan pengaduan sebagaimana diatur dalam Pasal 317 KUHP adalah: "menyampaikan suatu

pengaduan tertentu kepada yang berwajib dan pengaduan ini mengandung suatu penghinaan:" Pasal 317 KUHP berbunyi:

Ayat (1): Barangsiapa dengan sengaja memasukkan atau menyuruh menuliskan suratpengaduan atau surat pemberitahuan yang palsu tentang seseorang kepada pembesar negeri, sehingga kehormatan atau nama baik orang itu terserang, dipidana karena bersalah memfitnah dengan pengaduan dengan pidana penjara selama-lamanya empat tahun.

Ayat (2): Pencabutan hak tersebut dalam Pasal 35 No. 1-3 dapat dijatuhkan.

3. Penghinaan terhadap Orang yang Meninggal

Sebagaimana yang telah dijelaskan di muka, bahwa penghinaan atau Pencemaran Nama Baik itu harus memenuhi syarat dilakukan terhadap manusia hidup. Akan tetapi, terhadap hal ini ada pengecualiannya, yaitu beberapa jenis perbuatan yang dilarang dan diancam dengan hukuman penghinaan yang ditujukan kepada "*orang yang telah meninggal dunia*" dan "*badan resmi*". Mengenai penghinaan atau Pencemaran Nama Baik terhadap "orang yang telah meninggal dunia" diatur dalam Pasal 320 KUHP, yang berbunyi:

Ayat (1): Barangsiapa yang melakukan perbuatan terhadap orang yang sudah mati dan perbuatan itu bersifat menista atau menista dengan surat jika sekiranya ia masih hidup, dihukum dengan hukuman penjara selama-lamanya empat bulan dua minggu atau denda sebanyak-banyaknya tiga ratus rupiah.

Ayat (2): Kejahatan itu hanya dituntut atas pengaduan salah seorang keluarga sedarah atau keluarga semenda dalam keturunan yang lurus atar yang menyimpang sampai derajat kedua dari orang yang rnati itu atau atas pengaduan suami (isterinya).

Ayat (3): Bilamana menurut adat keturunan ibu (matriamhale instellingen) kekuasaan bapak dijalankan oleh orang lain daripada bapak, maka kejahatan itudapat dituntut atas pengaduan orang itu.

4. Penghinaan terhadap Badan Resmi (Badan Umum)

Mengenai penghinaan atau Pencemaran Nama Baikterhadap badan resmi atau badan umum ini diatur dalam Pasal 207 - 208 KUHP. Pasal 207 berbunyi: "Barangsiapa yang dengan sengaja di muka umum dengan lisan atau dengan tulisan menghina suatu kekuasaan yang diadakan di daerah Republik Indonesia atau suatu badan pemerintahan yang diadakan di sini, dihukum dengan hukuman penjara selama-lamanya satu tahun enam bulan atau denda sebanyak-banyaknya empat ribu lima ratus rupiah." Unsur-unsur delik dari perbuatan Pasal 207 KUHP ini adalah:

a. Perbuatan yang dilakukan dengan sengaja;
b. Yang berupa penghinaan (*belediging*);
c. Dilakukan di muka umum;
d. Ditujukan terhadap suatu kekuasaan yang diadakan di daerah Republik Indonesia atau suatu badan pemerintahan yang terdapat di situ. Seperti yang telah dituliskan sebelumnya, bahwa kejahatan

penghinaan atau Pencemaran Nama Baik hanya ditujukan kepada seorang manusia yang masih hidup. Akan tetapi, terdapat pengecualiannya yaitu penghinaan atau Pencemaran Nama Baik itu yang ditujukan terhadap suatu badan resmi atau suatu badan kekuasaan pemerintahan. Maksud pasal ini adalah untuk menjamin alat-alat negara atau badan-badan pemerintahan agar dihormati oleh rakyatnya.

5. Penghinaan Lain dalam Pasal KUHP Sebagaimana yang telah dipaparkan sebelumnya, bahwa pasal-pasal dalam Bab XVI Pasal 310 - 321 KUHP telah mengatur tentang penghinaan atau Pencemaran Nama Baik. Namun demikian, di pasal-pasal lainnya juga diatur mengenai penghinaan atau Pencemaran Nama Baik sebagai pasalpasal khusus, yaitu:
   a. Penghinaan terhadap Presiden dan Wakil Presiden (Pasal 134 dan Pasal 137 KUHP), pasal-pasal ini telah dibatalkan atau dinyatakan tidak berlaku lagi oleh Mahkamah Konstitusi;
   b. Penghinaan terhadap kepala negara asing (Pasal 142 -144 KUHP);
   c. Penghinaan terhadap segolongan penduduk/kelompok/ organisasi (Pasal 156 dan Pasal 157 KUHP);
   d. Penghinaan terhadap pegawai agama (Pasal 177 KUHP);
   e. Penghinaan terhadap kekuasaan yang ada di Indonesia (Pasal 207 dan Pasal 208 KUHP).

H. Sistem Pembuktian Cyber Crime

Secara garis besar, Cyber Crime terdiri dari dua jenis, yaitu :

1. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas; dan
2. Kejahatan yang menjadikan sistem dan fasilitas TI sebagai sasaran

Berdasarkan UU.No 16 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), hukum Indonesia telah mengakui alat bukti elektronik atau digital sebagai alat bukti yang sah di pengadilan. Dalam acara kasus pidana KUHAP, maka UU ITE ini memperluas dari ketentuan pasal 184 KUHAP mengenai alat bukti yang sah.

Pasal 5 : (1) *Informasi Elektronik dan/atau Dokumen Elektronik dan/atau cetaknya merupakan alat bukti hukum yang sah*

(2) *Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara berlaku di Indonesia*.

(3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

a. Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan

b. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta

Pasal 6 : " Dalam hal terdapat ketentuan lain selain yang diatur dalam pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, *Informasi Elektronik dan/atau Dokumen Elektronik* dianggap sah sepanjang informasi yang tercantum didalamnya dpat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Menurut keterangan kepala unit V Information dan Cyber Crime Badan Reserse Kriminal Mabes Polri, Kombespol Dr. Petrus Golose menerangkan bahwa Kepolisian Republik Indonesia (Polri), khususnya unit Cyber Crime, telah memiliki Standar Operasional Prosedur (SOP) dalam menangani kasus terkait Cyber Crime. Standar yang digunakan telah mengacu kepada standar Internasional yang telah banyak digunakan diseluruh dunia, termasuk oleh Federal Bureau of Investigation (FBI) di Amerika Serikat.

Karena terdapat banyak perbedaan anatara cyber crime dengan kejahatan konvensional, maka penyidik polri dalamproses penyidikan di Laboratorium Forensik Komputer juga melibatkan ahli digital forensik baik dari polri sendiri maupun pakar digital forensik diluar polri. Rubi Alamsyah, seorang pakar digital forensik Indonesia, memaparkan mekanisme kerja seorang Digital Forensik antara lain:

A. Proses *Acquiring* dan *Imaging*

Setelah penyidik menerima barang bukti digital, maka harus dilakukan proses *Acquiring* dan *Imaging* yaitu mengkopi (mengkloning/menduplikat) secara tepat dan persis 1:1. Dari hasil kopi tersebutlah maka seorang ahli digital forenik dapat melakukan analisis karena analisis tidak boleh dilakukan dari barang bukti digital yang asli karena dikhawatirkan akan mengubah barang bukti.

B. Melakukan Analisis

Setelah melakukan proses *Acquiring* dan *Imaging*, maka dapat dilanjutkan untuk menganalisis isi data terutama yang sudah dihapus, disembunyikan, di-enkripsi, dan jejak log file yang ditinggalkan. Hasil dari analisis barang bukti digital tersebut yang akan dilimpahkan penyidik kepada Kejaksaan untuk selanjutnya dibawa ke Pengadilan

Dalam menentukan locus delicti atau tempat kejadian perkara suatu tindakan cyber crime, penulis tidak mengetahui secara pasti metode yang diterapkan oleh penyidik khususnya di Indonesia. Namun untuk Darrel Menthe dalam bukunya Jurisdiction in Cyberspace : A Theory of International Space, menerangkan teori yang berlaku di Amerika Serikat yaitu:

1. *Theory of The Uplader and the Downloader*

   Teori ini menekankan bahwa dalam dunia cyber terdapat 2 (dua) hal utama yaitu *uploader* (pihak yang memberikan informasi ke

dalam *cyber space*) dan *downloader* (pihak yang mengakses informasi).

2. *Theory of Law of the Server*

   Dalam pendekatan ini penyidik memperlakukan *server*dimana halaman *web* secara fisik berlokasi tempat mereka dicatat atau disimpan sebagai data elektronik.

3. *Theory of International Space*

   Menurut teori ini, *cyber space* dianggap sebagai suatu lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama.

   Namun dalam menentukan *tempus delicti* atau waktu kejadian perkara suatu tindakan *cyber crime*, maka penyidik dapat mengacu pada *log file*, yaitu sebuah file yang berisi daftar tindakan dan kejadian (aktivitas) yang telah terjadi di dalam suatu sistem komputer.

BAB III

METODE PENELITIAN

Penelitian hukum merupakan suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi. Hal tersebut sesuai dengan karakter perspektif ilmu hukum.(Marzuki, 2005)

Pada dasarnya penelitian merupakan suatu upaya pencarian, bukan sekedar mengamati secara teliti terhadap suatu obyek yang mudah terpegang ditangan. Penelitian dalam bahasa inggrisnya yaitu*"research",* yang berasal dari kata *"re"* (kembali) dan*"search"*adalah penelitian.(Sunggono, 2003)

Jadi *Research* adalah suatu upaya untuk mencari kembali/meneliti kembali mengenai suatu obyek.

Dalam penulisan metodelogi penelitian ini, pembaca diharapkan setidaknya mendapatkan suatu ilustrasi yang dapat menggugah kerangka berfikir pembaca secara logis dengan mengetahui pengetahuan dasar mengenai teori, metode serta pendekatan yang berkembang dalam ilmu hukum secara doktrial (ajaran-ajaran ilmu pengetahuan), kemudian juga mengetahui dasar-dasar pembuatan usulan penelitian atau proposal, dasar-dasar teknik pengumpulan data, teknik analisis data dan penyusunan laporan akhir dan sebagai tambahan pengetahuan mengenai pedoman penulisan hukum baik media masa maupun berita hukum.

Agar dalam penelitian ini dapat diperoleh hasil yang dapat dipertanggungjawabkan kebenarannya, maka perlu didukung suatu metodelogi yang baik. Dengan demikian dapat dikatakan bahwa metodelogi merupakan suatu unsure mutlak di dalam suatu penelitian. Oleh Karena itu di dalam penelitian ini penulis menggunakan beberapa metode sebagai berikut:

A. Jenis Penelitian

Penelitian ini adalah penelitian yuridis normatif dan yuridis sosiologis. Yuridis normatif artinya meneliti sistematika hukum, asal hukum, dan bahan pustaka yang merupakan data sekunder dan disebut juga penelitian kepustakaan. (Soekanto, 2005.) serta peraturan yang mengatur tentang pembuktian cybercrime. Dan yuridis sosiologis artinya penelitian yang dilakukan dengan cara melakukan telaah terhadap kasus-kasus yang berkaitan dengan isu yang sedang ditangani. (Marzuki, 2005) seperti kasus cyber crime dalam hal pembuktiannya.

B. Bahan Penelitian

Adapun bahan hukum yang dipergunakan dalam penelitian ini adalah berasal dari bahan hukum primer, dan bahan hukum sekunder.Jika dibutuhkan juga akan mempergunakan bahan non hukum.

1. Bahan Hukum Primer

Bahan Primer adalah bahan hukum yang bersifat autoritatif artinya mempunyai otoritas. Bahan-bahan hukum primer terdiri dari perundang-undangan, dan contoh kasus. Bahan Hukum Primer yang meliputi :

a) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

b) Undang- Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana

c) Undang-Undang Nomor 11 Tahun 2008 jo Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik.

d) Undang-Undang Nomor 39 Tahun 1999 tentang Telekomunikasi.

2. Bahan Sekunder

Bahan Hukum Sekunder yang meliputi :

Literatur-literatur yang berkaitan dengan memberikan penjelasan mengenai bahan hukum primer, seperti buku-buku, hasil-hasil penelitian, hasil karya dari kalangan hukum, majalah, koran, internet, dan lain-lain yang berkaitan dengan masalah yang akan diteliti oleh penulis dalam penelitian ini.

3. Bahan Non Hukum

Bahan Non Hukum yaitu bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, meliputi:

a. Kamus Hukum

b. Kamus Bahasa Indonesia

C. Spesifikasi Penelitian

Untuk meneliti pokok permasalahan serta memahami kebenaran obyektif dan dapat dipertanggungjawabkan, maka dipakai spesifikasi penelitian bersifat perspektif dan terapan perspektif artinya mencari kebenaran dan kaidah-kaidah yang mengatur tentang sistem pembuktian

cyber crime. Sedangkan terapan artinya apakah aturan hakim yang ada dijadikan pendapat dalam pembuktian terhadap cyber crime.

D. Tahap Penelitian

Tahap penelitian yang digunakan dalam penelitian inidilakukan dengan beberapa tahap. Diantaranya :

1. Tahap Pendahuluan

   Tahap ini, peneliti melaksanakan pengajuan usulan mengenai penelitian yang akan dilaksanakan dengan menyusun suatu proposal yang mengidentifikasi fakta hukum dan mengeliminir hal-hal yang tidak relevan untuk menetapkan isu hukum yang hendak dipecahkan.

2. Tahap Pelaksanaan

   Pada tahap ini, peneliti melakukan pengumpulan bahan-bahan hukum dan sekiranya memiliki relevansi yang peneliti akan coba dapatkan dari interview/wawancara terhadap responden yang terdiri dari Reskrimsus Kapolda Metro Jaya. Serta dari bahan hukum yang didapatkan dari perpustakaan Universitas Muhammadiyah Magelang, perpustakaan Fakultas Hukum Universitas Muhammadiyah Magelang, Perpustakaan Kota Magelang maupun toko-toko buku yang memiliki bahan-bahan hukum yang dicari.

3. Tahap Akhir

Pada tahap ini, peneliti melakukan telaah atas isu hukum dan memberikan preskripsi berdasarkan argumentasi yang telah dibangun dalam kesimpulan.

E. Metode Pendekatan

Metode pendekatan yang digunakan dalam penulisan ini adalah sebagai berikut:

1. Pendekatan Perundang-Undangan (*Statute Approach*)

   Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan yang bersangkut-paut dengan permasalahan (isu hukum) yang sedang dihadapi. Pendekatan perundang-undangan ini misalnya dilakukan dengan mempelajari konsistensi/kesesuaian antara Undang-Undang Dasar dengan Undang-Undang, atau antara Undang-Undang yang satu dengan Undang-Undang yang lain, dst.(Marzuki, 2005) kegunaan dalam pendekatan ini adalah untuk menjawab isu hukum antara ketentuan undang-undang dengan filosofi yang melahirkan undang-undang itu. (Ibid,)

2. Pendekatan Kasus (*Case Approach*)

   Pendekatan kasus dilakukan dengan cara menelaah kasus-kasus terkait dengan isu yang sedang dihadapi, dan telah menjadi putusan yang mempunyai kekuatan hukum tetap.kasus ini dapat berupa kasus yang terjadi di Indonesia maupun dinegara lain. Di dalam pendekatan kasus

(*Case Approach*), beberapa kasus ditelaah untuk referensi bagi suatu isu hukum. (Marzuki, 2005)

3. Pendekatan melalui interview/wawancara

   pendekatan ini dilakukan dengan melakukan proses tanya jawab secara lisan dimana dua orang atau lebih berhadapan secara fisik, interview ini merupakan suatu teknik pengumpulan data dengan tanya jawab yang bersifat sepihak yang dilakukan secara sistematis berdasarkan *research.*

F. Metode Analisis Data

Gambaran umum mengenai data yang sudah terkumpul dari objek penelitian akan dianalisis menggunakan metode kualitatif. Setelah semua data terkumpul baik data primer maupun data sekunder atau data lapangan, data tersebut akan dianalisa secara kualitatif yaitu dengan cara menjabarkan data-data yang diperoleh kemudian mencari korelasinya dengan literature yang digunakan sebagai landasan dalam penulisan. (Soekanto, Pengantar Penelitian Hukum , 1986)

Setelah semua data terkumpul baik data primer maupun data sekunder, data tersebut dianalisa secara kualitatif dengan pendekatan deduktif, yaitu prosedur yang berpangkal pada suatu peristiwa umum yang kebenarannya telah diketahui atau diyakini dan berakhir pada suatu kesimpulan atau pengetahuan baru yang bersifat lebih khusus.Metode ini diawali dari pembentukan teori, hipotesis, definisi operasional, instrument dan operasionalisasi. Dengan kata lain, untuk memahami suatu gejala terlebih

dahulu harus memiliki konsep dan teori tentang gejala tersebut dan selanjutnya dilakukan penelitian lapangan. Dan data yang diperoleh responden secara tertulis maupun lisan secara nyata diteliti dan dipelajari secara utuh setelah data terkumpul.

BAB V

PENUTUP

A. KESIMPULAN

Perlu diketahui bahwa alat bukti yang sah (pasal 184 ayat (1) KUHAP) adalah: Keterangan Saksi, Keterangan Ahli, Surat, Petunjuk; dan Keterangan Terdakwa. Menurut R. Soesilo, supaya dapat dihukum maka pencemaran nama baik itu harus dilakukan dengan cara menuduh seseorang telah melakukan perbuatan yang tertentu dengan maksud tuduhan itu akan tersiar (diketahui oleh orang banyak). Berbeda halnya dengan pencemaran nama baik dengan tulisan, dimana media yang digunakan dalam melakukan pencemaran nama baik tersebut dapat berupa tulisan (surat) atau gambar (Print Screen). print screen kata-kata atau kalimat dalam media sosial dapat digunakan sebagai alat bukti yang sah dalam persidangan sepanjang bukti tersebut secara teknis dapat dipertanggungjawabkan otentitasnya, tidak lepas dari pencarian barang bukti tersebut pihak penyidik juga mempunyai kendala-kendala yang berupa kendala internal maupun eksternal untuk menemukan barang bukti dalam tindak pidana Pencemaran Nama Baik.

B. SARAN

1. Meningkatkan kualitas SDM yang bertugas dibidang penyidikan terhadap Tindak Pidana Informasi dan Transaksi Elektronik
2. Mengajukan penambahan sarana prasarana pendukung untuk membantu penyidikan dalam memeriksa Tindak Pidana yang menggunakan media social khususnya Tindak Pidana Pencemaran Nama Baik.

DAFTAR PUSTAKA

a. BUKU :

Agus Tri P.H. Cyber Crime dalam Perspektif Hukum Pidana,Skripsi, 2010,Surakarta:UMS.

Agus Raharjo, Cybercrime, PT Citra Aditya Bakti, Bandung, 2002.

Amirudin dan Zaenal Asiki, *Pengantar Metode Penelitian Hukum*, Edisi pertama, Catatan Kedua,PT Raja GrafindoPersada,Jakarta,2004.

H. Sutarwan, Cyber Crime Modus Operandi dan Penanggulangannya, Laksbang PRESSindo, Jogjakarta,2007.

Masruchin Ruba'i – Made S. Astuti Djajuli, Hukum Pidana I, Malang, 1989

Moeltjatno, Asas-asas Hukum Pidana, Bina Aksara, Jakarta,1987.

Peter Marzuki, PenelitianHukum,Universitas Indonesia,Jakarta, 2005.

Sudarto, Hukum Pidana 1, Universitas Diponegoro, Semarang

Sigid Suseno, Yurisdiksi Tindak Pidana Siber, Bandung:Refika Aditama, 2012.

Soerjono Soekanto, Pengantar Penelitian Hukum, Universitas Indonesia, Jakarta, 2005.

Zainudin Ali, *Metode Penelitian Hukum*, Sinar Grafika, Jakarta, 2011.

b. PERUNDANG-UNDANGAN:

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Undang- Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana

Undang-Undang Nomor 39 Tahun 1999 Tentang Telekomunikasi

Undang-Undang Nomor 19 Tahun 2016PerubahanAtasUndang-Undang Nomor 11 Tahun 2008tentang Informasi dan Transaksi Elektronik.

c. JURNAL:

Ana Maria, AlviSyahrin, Syafruddin Hasibuan, Kejahatan Siber Sebagai Dampak Negatif Dari Perkembangan Teknologi Dan Internet Di Indonesia Berdasarkan Undang-Undang No. 19 Tahun 2016 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Persfektif Hukum Pidana,vol 1 No 1, 2017

Fathur Rohman, Analisis Meningkatnya Kejahatan Cyberbullying Dan Hatespeech Menggunakan Berbagai Media Sosial Dan Metode Pencegahannya, 2016

Reydi Vridell Awawangi, Pencemaran Nama Baik Dalam KUHP Dan Menurut UU No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,2014

Rudi Hermawan,Kesiapan Aparatur Pemerintah Dalam Menghadapi Cyber Crime Di Indonesia, Vol 6 No 1, 2013

Suyanto Sidik,Dampak Undang-Undang Informasi dan Transaksi Elektronik (UU.ITE) Terhadap Perubahan Hukum Dan Sosial Dalam Masyarakat,Jurnal Ilmiah Widya, 2013

Syaifullah Noor, Mohd. Din, Informasi Dan Transaksi Elektronik Dikaitkan Dengan Kebebasan Berekspresi,2015

d. WEBSITE:

(http://www.reskrimsus.metro.polri.go.id.di unduh Rabu 26 september 2018 Pukul 21.00 WIB)

(http://www.Hukumonline.com di unduh Jumat 07 Desember 2018 Pukul 18:58 WIB)

(http://www.batan.go.id/sjk/uu-ite di unduh sabtu 08 Desember 2018 Pukul 14:00 WIB)

(http://www.SIPP.PNSLMN.go.id diunduh 08 Desember 2018 Pukul 15:00 WIB)