IV. HASIL PENELITIAN DAN PEMBAHASAN

A. Karakteristik Responden

1. Polisi :

   Nama : BRIPTU Yayan Sopiyan

   Umur : 26 Tahun

   Jabatan : Anggota Krimsus Polda Lampung

   Pendidikan : SMA

2. Jaksa :

   a. Nama : Hartono, S.H

      Umur : 46 Tahun

      Jabatan : Jaksa Fungsionalis Kejaksaan Negeri Bandar Lampung

      Pendidikan : Sarjana Hukum (S1)

   b. Nama : Suyanto, S.H., M.H

      Umur : 48 tahun

      Jabatan : Kasi Pidsus Kejaksaan Negeri Bandar Lampung

      Pendidikan : Magister Hukum (S2)

3. Akademisi Unila :

a. Nama : Syafruddin, S.H., M.H

NIP : 19600207 198603 1 001

Umur : 49 Tahun

Jabatan : Dosen Fakultas Hukum Universitas Lampung

Pendidikan : Magister Hukum (S2)

b. Nama : Prof. Dr. I Gede AB. Wiranata, S.H.,M.H

NIP : 131804060

Umur : 47 Tahun

Jabatan : Ketua Bagian Jurusan Perdata Fakultas Hukum Unila

Pendidikan : S3

B. Tindak Pidana yang Terdapat Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Menurut Hartono, tindak kejahatan di Internet merupakan perbuatan yang mempunyai pengetahuan dibidang internet yang mana kejahatan melalui internet merupakan kejahatan menggunakan fasilitas teknologi informasi dan tidak semua orang bisa melakukannya, pelaku seharusnya dapat membayangkan akan adanya akibat yang ditimbulkan dari perbuatannya karena adanya niat dan kehendak, atau dengan kata lain bahwa pelaku dapat menduga bahwa akibat dari perbuatannya itu akan menimbulkan suatu akibat yang dilarang oleh undang-undang.

Dilihat dari perspektif hukum pidana, upaya penanggulangan *cybercrime* dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi

tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan, dan aspek juridiksi.

Suyanto berpendapat pada dasarnya *cybercrime* meliputi semua tindak pidana yang berkenaan dengan informasi itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya.

Kebijakan penanggulangan *cybercrime* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari kebijakan penanggulangan kejahatan. Dilihat dari sudur *criminal policy*, upaya penanggulangan kejahatan termasuk penanggulangan *cybercrime*, tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana tetapi harus ditempuh pula dengan pendekatan integral.

Menurut Hartono, kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana.

Patut diketahui, kebijakan kriminalisasi harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang sedang berlaku saat ini. Sistem hukum pidana yang saat ini berlaku di Indonesia terdiri dari keseluruhan sistem perundang-undangan yang ada di dalam KUHP dan UU khusus diluar KUHP. Keseluruhan peraturan perundang-undangan di bidang hukum pidana substansif itu terdiri dari aturan umum, Buku I KUHP dan aturan khusus, Buku II dan III KUHP dan dalam UU khusus di luar KUHP.

Aturan khusus ini umumnya memuat perumusan tindak pidana tertentu namun dapat pula memuat aturan khusus yang menyimpang dari aturan umum. UU ITE

adalah salah satu Undang-undang yang menyimpang dari ketentuan umum KUHP, terlihat dari materi muatan dan perumusan yang dilarang serta ketentuan pidana yang termuat didalamnya. Masalah perumusan sanksi pidana dan aturan pemidanaan dalam UU ITE tidak terlepas dari perumusan sanski berkaitan dengan jenis-jenis sanksi pidana, pelaksanaan pidana, dan ukuran atau jumlah lamanya pidana.

Perumusan perbuatan yang dilarang dalam UU ITE mencakup semua aktivitas yang merugikan sebagaimana dalam pasal 27-37, yaitu :

a. Mendistibusikan dan/atau menstranmisikan dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, memiliki muatan perjudian, penghinaan dan/atau pencemaran nama baik serta pemerasan dan/atau pengancaman (Pasal 27 Ayat (1), (2), (3) dan (4) UU ITE).
b. Menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik serta menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) (Pasal 28 Ayat (1) dan (2) UU ITE).
c. Mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakuti-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE).
d. Mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun, dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Pasal 30 Ayat (1), (2) dan (3) UU ITE).

e. Melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain, intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat public dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan (Pasal 31 Ayat (1), (2),(3), dan (4) UU ITE).

f. Dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik public, memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak (Pasal 32 Ayat (1), (2) dan (3) UU ITE).

g. Melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektonik dan/atau mengakibatkan Sistem Elektonik menjadi tidak bekerja sebagaimana mestinya (Pasal 33 UU ITE).

h. Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :

    1) Perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai Pasal 33;

    2) Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan

memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33 (Pasal 34 Ayat (1) dan (2) UU ITE).

i. Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Inforamsi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik (Pasal 35 UU ITE).
j. Melakukan perbuatan sebagaimana yang dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain (Pasal 36 UU ITE)
k. Melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektonik yang berada di wilayah yurisdiksi Indonesia (Pasal 37 UU ITE).

UU ITE mengatur dua hal pokok yang berkaitan dengan penerapan sanksi pidana, agar hukum itu dipatuhi sekaligus ditakuti oleh setiap orang. Pasal 27 sampai dengan Pasal 37 mengatur tentang perbuatan-perbuatan yang dilarang oleh hukum. Sedangkan Pasal 45 sampai dengan Pasal 52 merupakan bentuk ancaman pidana yang dilanggar.

Ada hubungan yang signifikan antara ancaman pidana dengan perilaku yang dikehendaki oleh hukum. Setiap manusia dalam memanfaatkan dunia maya, dilakukan secara tertib, tidak merugikan kepentingan orang lain, karena efek samping ini tidak hanya terbatas pada wilayah Indonesia itu sendiri, akan tetapi juga memasuki dunia maya internasional.

Hukum akan memberikan efek terhadap sikap tindak seseorang, hal ini dapat diamati dari oerilaku melalui pancaindera, yang mencerminkan dari motivasi atau hasrat seseorang untuk bertindak dalam mencapai tujuan yang diinginkan. Efek ini juga dapat dilihat dari perbandingan antara perilaku yang diatur oleh hukum, dengan yang tidak diatur, agar hukum itu mempunyai pengaruh terhadap sikap perilaku, diperlukan penciptaan kondisi-kondisi sehingga hukum dapat dikomunikasikan.

C. Barang Bukti Elektronik Sebagai Alat Bukti yang Sah

Kejahatan di bidang elektronik dapat dikatakan sebagai suatu kejahatan yang dilakukan oleh seseorang dengan menggunakan alat elektronik (pada umumnya dengan menggunakan teknologi atau prasarana yang mendukung untuk melakukan kejahatan) dilakukan oleh seorang yang mempunyai kemampuan intelektual yang tinggi.

Yayan Sopiyan berpendapat, untuk mengantisipasi si pelaku kejahatan di bidang kejahatan komputer, supaya mereka dapat terjaring dengan ketentuan mengenai kejahatan yang sesuai dengan apa yang mereka lakukan, dan tidak lagi dengan memakai hanya pasal-pasal yang ada dalam KUHP tetapi memakai pasal-pasal dalam Undang-undang lainnya agar lebih memberatkan pelaku.

Penegak hukum harus dapat membuktikan, agar pembuktian dengan alat elektronik ini dapat diterima sebagai alat bukti yang sah sebagaimana alat bukti yang dimaksud dalam Pasal 184 ayat (1) KUHAP.

Pasal 184 ayat (1) KUHAP berisi :

Alat bukti yang sah adalah :

a. Keterangan saksi
b. Keterangan ahli
c. Surat
d. Petunjuk
e. Keterangan terdakwa

Mengacu kepada pendapat Yayan sopian tersebut apabila dihubungkan dengan pasal 184 KUHAP yang menjelaskan secara tegas beberapa alat-alat bukti yang dapat diajukan oleh para pihak yang berperkara di muka persidangan.

Sedangkan penjelasan Pasal 184 KUHAP dijelaskan ;

"Dalam acara pemeriksaan cepat, keyakinan hakim cukup di dukung satu alat bukti yang sah". Bertolak dari Pasal 184 dan penjelasannya tersebut, berarti kecuali pemeriksaan cepat, untuk mendukung keyakinan hakim diperlukan alat bukti lebih dari satu atau sekurang-kurangnya dua alat bukti yang sah. Untuk hal ini Pasal 183 KUHAP secara tegas dirumuskan bahwa" Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya". Dengan demikian dalam KUHAP secara tegas memberikan legalitas bahwa di samping berdasarkan unsur keyakinan hakim, pembuktian dengan sekurang-kurangnya dua alat bukti yang sah adalah sangat diperlukan untuk mendukung unsur kesalahan dalam hal menentukan seseorang benar-benar terbukti melakukan tindak pidana atau tidak. Kemudian praktik yang berkembang, bahwa modus operandi kejahatan dibidang *Cyber Crime* tidak saja dilakukan dengan alat canggih tetapi kejahatan ini

benar-benar sulit menentukan secara cepat dan sederhana siapa sebagai pelaku tindak pidananya, ketika perangkat hukum dalam penegakan hukum pidana masih banyak memiliki keterbatasan. Fenomena hukum dalam upaya penanggulangan *Cyber Crimes* ini juga tampak memiliki kendala khususnya bila dikaitkan dengan sistem pembuktian menurut hukum pidana Indonesia, sebab sebagaimana dalam Pasal 184 KUHAP, bahwa alat-alat bukti mana secara legalitas tidak dapat diterapkan sebagai dasar pembuktian apabila kejahatan yang dilakukan dalam konteks *"Cyber Crimes"* secara nyata bukti-buktinya tidak mencocoki (tidak tergolong) rumusan alat bukti sebagai mana dikehendaki menurut KUHAP.

Menurut Suyanto, kemungkinan yang dapat dijadikan keterangan saksi ialah melalui hasil interaksi di dalam dunia *cyber,* seperti *chatting* dan *e-mail* antara pengguna internet, atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi.

Menurut Syafruddin, surat adalah tanda baca yang mengandung pesan dari pembuat dan dipahami oleh penerima. Surat bisa dijadikan alat bukti yang sah dengan ketentuan hasil *print out* tersebut asli dan ada kaitannya dengan alat bukti yang lain.

Keterangan ahli menjadi signifikan penggunaannya jika jaksa mengajukan alat bukti elektronik untuk membuktikan kesalahan pelaku *cybercrime.* Peran keterangan ahli disini adalah untuk memberikan suatu penjelasan di dalam persidangan bahwa dokumen elektronik yang diajukan sah dan dapat dipertanggungjawabkan secara umum. Hal ini diperlukan karena dalam praktiknya, para pelaku *cybercrime* dapat menghapus atau menyembunyikan aksi mereka agar tidak terdeteksi oleh aparat penegak hukum.

Merujuk pada terminology surat dalam kasus *cybercrime* mengalami perubahan dari bentuknya yang tertulis menjadi tidak tertulis dan bersifat *on-line.* Alat bukti surat dalam sistem komputer yang telah disertifikasi ada dua kategori , pertama bila sebuah sistem komputer yang telah disertifikasi oleh badan yang berwenang, maka hasil *print out* komputer dapat dipercaya keotentikannya. Kedua, bukti sertifikasi dari badan yang berwenang tersebut dapat dikategorikan sebagai alat bukti surat, karena dibuat oleh dan atau pejabat yang berwenang.

Jenis alat bukti surat lainnya dapat berupa bukti elektronik yang dapat dicetak atau *print out* dan surat yang terpampang dalam layar monitor sebuah jaringan komputer. Selama kedua bukti ini dikeluarkan/dibuat oleh yang berwenang dan sebuah sistem jaringan komputer tersebut dapat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP.

Mewujudkan suatu petunjuk dari bukti-bukti yang ditemukan dalam *cybercrime* akan sulit jika hanya mendasarkan pada keterangan saksi, surat, keterangan terdakwa saja meskipun hal tersebut masih mungkin untuk diterapkan. Bisa saja apabila hakim dapat petunjuk yang diajukan di persidangan adalah bukti elektronik yang disertai keterangan ahli, maka petunjuk ini akan bersifat lebih kuat dan memberatkan terdakwa dibandingkan dengan petunjuk-petinjuk lain.

Dalam kasus *cybercrime,* keterangan terdakwa yang dibutuhkan terutama mengenai cara-cara pelaku melakukan perbuatannya, akibat yang ditimbulkan, informasi jaringan serta motivasinya. Keterangan terdakwa mengenai keemapt hal tersebut sifatnya adalah memberatkan terdakwa.

Dalam sistem hukum pembuktian di Indonesia, terdapat beberapa doktrin pengelompokan alat bukti yang membagi alat-alat bukti ke dalam beberapa kategori, yaitu:

1. *Oral Evindence*
    a. Perdata (keterangan saksi, pengakuan, dan sumpah)
    b. Pidana (keterangan saksi, keterangan ahli, dan keterangan terdakwa)
2. *Documentary Evidence*\
    a. Perdata (surat dan persangkaan)
    b. Pidana (surat dan petunjuk)
3. *Material Evidence*
    a. Perdata (tidak dikenali)
    b. Pidana (barang yang digunakan untuk melakukan tindak pidana, barang yang merupakan hasil dari suatu tindak pidana, barang yang diperoleh dari suatu tindak pidana, dan informasi dalam arti khusus)
4. *Electronic Evidence*
    a. Konsep pengelompokkan alat bukti menjadi alat bukti tertulis dan elektronim. Tidak dikenal di Indonesia.
    b. Konsep tersebut terutama berkembang di negara-negara *common law*.
    c. Pengaturannya tidak melahirkan alat bukti baru, tetapi memperluas cakupan alat bukti yang masuk kategori *documentary evidence*.

Lebih lanjut Suyanto menyatakan jika ada kejahatan atau persangkaan orang melakukan kejahatan di bidang elektronika maka dapat dipakai bukti petunjuk dan keterangan ahli sebagaimana dimaksud Pasal 184 ayat (1). Namun, apabila ingin

menghadirkan bukti dengan menggunakan alat elektronik, harus terlebih dahulu menyatakan bahwa hasil yang didapat benar-benar asli sesuai dengan yang sebenarnya atau si terdakwa lakukan.

Setiap apa yang dihasilkan dalam bidang elektronik, hendaknya mendapat pengesahan atau pengakuan dari pejabat yang berwenang, supaya apa yang dihasilkan benar sesuai dengan bentuk yang asli, sekalipun bentuk yang asli tersebut tidak dapat dihadirkan. Dengan menddunakan alat bukti petunjuk dan keterangan ahli sebagaimana tercantum dalam Pasal 184 ayat (1) KUHAP perlu diperjelas bahwa keterangan ahli yang dimaksud adalah orang yang benar-benar mengetahui dan mengerti tentang alat-alat bukti elektronik yang akan dihadirkan di persidangan untuk menguatkan bahwa si terdakwa benar-benar telah melakukan kejahatan di bidang elektronik.

Kejahatan terhadap komputer dan program komputer merupakan kejahatan yang sulit dibuktikan, karena dalam Pasal 184 KUHAP telah diberikan pembatasan berbagai alat bukti yang sah yang dapat digunakan sebagi dasar pertimbangan hakim dalam memberikan putusan. Maka pembuktian kejahatan *cyber* terhadap komputer dan program komputer harus mengikuti ketentuan tersebut. Kini menjadi tugas Penuntut Umum untuk mengajukan alat-alat bukti tersebut di depan persidangan untuk memberikan keyakinan kepada hakim mengenai kesalahan terdakwa.

Dilihat dari hubungannya dengan perkembangan teknologi saat ini, alat bukti menurut KUHAP yang dapat digunakan dalam mengadili *cybercrime* adalah keterengan ahli, surat dan petunjuk. Ketiga alat bukti ini adalah alat-alat bukti

yang paling esensiiil memberi pembuktian yang maksimal sehubungan dengan kejahatan *cyber* yang semakin pesat perkembangannya. Tidak berarti keterangan saksi dan keterangan terdakwa bukan merupakan alat bukti yang penting, hanya saja kurang dapat memberikan pembuktian yang maksimal jika dibandingkan dengan ketiga alat bukti yang lain.

Mengenai alat-alat bukti dalam transaksi elektronik, Michael Chissik dan Alistair Kelman menyatakan ada tiga tipe pembuktian yang dibuat oleh komputer, yaitu :

1. *Real Evidence*

   Meliputi kalkulasi-kalkulasi atau analisa-analisa yang dibuat oleh komputer itu sendiri melalui pengaplikasian *software* dan penerima informasi dari *device* lain.

2. *Hearsay Evidence*

   Termasuk dalam *hearsay evidence* adalah dokumen-dokumen data yang diproduksi pleh komputer yang merupakan salinan dari informasi yang diberikan oleh manusia kepada komputer.

3. *Derived Evidence*

   Adalah informasi yang mengkombinasikan antara bukti nyata dengan informasi yang diberikan oleh manusia ke komputer dengan tujuan unutk membentuk sebuah data yang tergabung.

Hartono menjelaskan dalam menghadapi kendala mengenai alat bukti perlu diupayakan jalan keluar dengan mengoptimalkan sarana hukum yang tersedia. Optimalisasi sarana hukum tersebut antara lain :

a. Dalam hal alat-alat bukti yang ada belum memenuhi aturan yang ada, maka alat bukti elektronik seperti rekaman secara hasil facsimile atau fotokopi dapat dijadikan petunjuk.
b. Apabila alat bukti tersebut ditunjang dengan keterangan ahli di bidangnya, misalnya ahli pita suara atau ahli lainnya yang menyatakan keaslian rekaman tersebut maka dapat dijadikan bukti yang sah.

Dalam sistem pembuktian terdapat macam-macam sistem atau teori pembuktian. Sistem atau teori pembuktian adalah:

1. Sistem atau teori pembuktian berdasarkan undang-undang secara positif.

   Pembuktian yang didasarkan melulu kepada alat-alat pembuktian yang disebut Undang-undang disebut sistem atau teori pembuktian berdasarkan undang-undang secara positif. Artinya jika tidak terbukti suatu perbuatan sesuai alat-alat bukti yang disebut undang-undang, maka keyakinan hakim diabaikan.
2. Sistem atau teori pembuktian berdasar undang-undang secara negative

   Teori ini menyandarkan bahwa hakim dalam mengambil keputusan tentang salah satu atau tidaknya seorang terdakwa terikat oleh alat bukti yang ditentukan oleh undang-undang dan keyakinan hakim sendiri.
3. Sistem atau teori pembuktian berdasar keyakinan hakim melulu.

   Berdasarkan teori ini, di dalam menjatuhkan putusannya Hakim tidak terikat dengan alat bukti yang ada. Darimana hakim menyimpulkan putusannya tidaklah menjadi masalah, karena ia dapat menyimpulkan dari alat bukti yang ada dalam persidangan atau mengabaikan alat bukti yang ada dalam persidangan.

4. Sistem atau teori pembuktian berdasarkan keyakinan hakin atas alas an yang logis.

   Menurut teori ini, hakim dapat memutuskan seseorang bersalah berdasar keyakinannnya, keyakinan mana didasarkan kepada dasar-dasar pembuktian disertai dengan suatu alasan-alasan yang logis. Sistem atau teori pembuktian ini disebut juga pembuktian bebas karena hakim bebas untuk menyebutkan alasan-alasan keyakinannya.

Hartono menjelaskan hukum pidana menganggap bahwa pembuktian merupakan bagian yang sangat esensial untuk menentukan nasib seseorang terdakwa. Bersalah atau tidaknya seorang terdakwa sebagaimana yang didakwakan dalam surat dakwaan ditentukan pada proses pembuktiannya.

Dengan kata lain Hartono menjelaskan pembuktian merupakan suatu upaya untuk membuktikan kebenaran dari isi dakwaan yang disampaikan oleh para jaksa penuntut umu, yang kegunaannya untuk memperoleh kebenaran sejati terhadap:

1. Perbuatan-perbuatan manakah yang dianggap terbukti menurut pemeriksaan persidangan.
2. Apakah telah terbukti bahwa terdakwa berslah atas perbuatan-perbuatan yang didakwakan kepadanya.
3. Tindak pidana apakah yang dilakukan sehubungan dengan perbuatan-perbuatan yang didakwakan kepadanya.
4. Hukuman apakah yang harus dijatuhkan kepada terdakwa bukan pekerjaan mudah.

Prof. Gede berpendapat Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah memperlebar pengertian alat bukti, yaitu apapun yang keluar dari sebuah perangkat alat elektronik dapat dijadikan sebagai alat bukti.

D. Ketentuan Hukum Pidana Terhadap Pelaku Kejahatan *Cybercrime*

Kitab Undang-Undang Hukum Pidana Indonesia telah memberikan pengaturan yang jelas mengenai batas-batas berlakunya aturan perundang-undangan hukum pidana. Hal ini diatur dalam Bab I buku Kesatu KitabUndang-Undang Hukum Pidana yang terdiri dari Sembilan pasal mulai dari Pasal 1 sampai dengan Pasal 9. Berkenaan dengan pengaturan tersebut, Moeljatno mengemukakan bahwa dari sudut Negara ada dua kemungkinan pendirian, yaitu :

Pertama, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang terjadi di dalam wilayah Negara, baik dilakukan oleh warga negaranya sendiri maupun oleh orang asing (asas territorial).

Kedua, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang dilakukan oleh warga Negara, dimana saja, juga di luar wilayah Negara (asas personal), yang juga dinamakan prinsip nasional yang aktif.

Dari pernyataan tersebut diatas terlihat jelas bahwa pada hakikatnya untuk beberapa kasus yang melibatkan aspek asing di dalamnya (pelaku, tempat terjadinya, dan sebagainya). Kitab Undang-Undang Hukum Pidana sudah dapat diberlakukan sekalipun sifatnya masih terbatas, artinya belum dapat diterapkan untuk semua jenis kejahatan transnasional. Ada dua hal yang menyebabkan

pengaturan dalam Kitab Undang-Undang Hukum Pidana daya jangkaunya bersifat terbatas, yaitu :

1. Keterbatasan pengaturan mengenai jenis-jenis tindak pidana, hal ini sangat wajar terjadi mengingat "suasana" yang mempengaruhi pada saat penyusunan Kitab Undang-Undang Hukum Pidana kita sangat jauh berbeda degan kondisi sekarang yang sarat dengan kemajuan teknologi informasi.
2. Keterbatasan dalam pengaturan mengenai pelaku tindak pidana, dalam era teknologi informasi seperti sekarang ini penentuan siapa yang dapat dikualifikasikan sebagai pelaku tindak pidana telah lebih kompleks sifatnya.

Berdasarkan hasil penelitian Widodo, sampai saat ini pengadilan Indonesia hanya menjatuhkan pidana penjara dan pidana denda terhadap pelaku *cybercrime*. Dasar hukum yang digunakan adalah Kitab Undang-Undang Hukum Pidana (KUHP), dan Undang-Undang (UU) di luar KUHP, misalnya UU Telekomunikasi, UU Pemberantasan Tindak Pidana Korupsi, UU Perbankan (Widodo, 2006:344). Secara teoretik, penjatuhan jenis pidana penjara dan pidana denda tersebut tersebut dapat mengundang perdebatan, karena selama ini pidana penjara dianggap sebagai pidana yang kurang efektif untuk mencapai tujuan pemidanaan, meskipun mempunyai efek pencegahan umum (*deterence effect*) cukup andal. Bahkan Sudarto (1981:90) menegaskan bahwa sejak dahulu sampai saat ini efektivitas pidana penjara diragukan. Roger Hood (1967:73) mengemukakan bahwa *"Most studies show that lengthy institutional sentences are no more successful than shorter alternatives"*. Selain keraguan tersebut, pelaku *cybercrime* mempunyai karakteristik dan motivasi yang unik sehingga belum tentu sesuai

dengan karakteristik pidana penjara (Widodo, 2006:253) sehingga aneh jika hanya dijatuhi pidana penjara dan dibina di Lembaga Pemasyarakatan.

Saat ini, Indonesia belum memiliki undang - undang khusus *cyber law* yang mengatur mengenai *cybercrime* Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain :

a. Kitab Undang Undang Hukum Pidana (KUHP)

   Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal - pasal yang dapat dikenakan dalam KUHP pada *cybercrime* antara lain :

   1. Pasal 362 KUHP yang dikenakan untuk kasus carding dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan software card generator di Internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.
   2. Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan

dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

3. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.
4. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut.
5. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.
6. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal.
7. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus-kasus video porno para mahasiswa.

8. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus carding, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
9. Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya

b. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta

Menurut Pasal 1 angka (8) Undang - Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 30). Harga program komputer/ software yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual software bajakan dengan harga yang sangat murah.

Misalnya, program anti virus seharga $ 50 dapat dibeli dengan harga Rp20.000,00. Penjualan dengan harga sangat murah dibandingkan dengan software asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping.

Maraknya pembajakan software di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/ atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah) ".

c. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) Undang - Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang- Undang ini, terutama bagi para hacker yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

1. Akses ke jaringan telekomunikasi
2. Akses ke jasa telekomunikasi
3. Akses ke jaringan telekomunikasi khusus

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)"

d. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan

Dengan dikeluarkannya Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya Compact Disk - Read Only Memory (CD - ROM), dan Write - Once -Read - Many (WORM), yang diatur dalam Pasal 12 Undang-Undang tersebut sebagai alat bukti yang sah.

e. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-Undang ini merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang

dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan. Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah engirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan. Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data– data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau digital *evidence* sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

f. Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Selain Undang-Undang Nomor 25 Tahun 2003, Undang-Undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan

secara elektronik dengan alat optik atau yang serupa dengan itu. *Digital evidence* atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah e-mail dan *chat room* selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list*.

g. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi & Transaksi Elektronik

Undang-undang ini, yang telah disahkan dan diundangkan pada tanggal 21 April 2008, walaupun sampai dengan hari ini belum ada sebuah PP yang mengatur mengenai teknis pelaksanaannya, namun diharapkan dapat menjadi sebuah undang-undang *cyber* atau *cyberlaw* guna menjerat pelaku-pelaku *cybercrime* yang tidak bertanggungjawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi guna mencapai sebuah kepastian hukum.