BAB II

TINJAUAN UMUM TENTANG TINDAK PIDANA *CYBERCRIME*

A. Pengertian dan Pengaturan Tindak Pidana *Cybercrime*

1. Pengertian Tindak Pidana *Cybercrime*

Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan.[1] Dampak pergeseran tersebut ditemukanya perkembangan dan kemajuan ilmu pengetahuan dan teknologi, terjadilah konvergensi antara keduanya.

Kemajuan teknologi yang merupakan hasil budaya menusia di samping membawa dampak positif, dalam arti dapat diperdayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E Sahetapy telah menyatakan dalam tulisannya, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan

[1] Abdul Wahid dan Mohammad Labib, 2005, *Kejahtan Mayaantara (Cybercrime)*, Bandung, PT Refika Aditama, hlm. 23.

semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya.[2]

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan).[3] Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime.*

Cybercrime merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional (*street crime*). *Cybercrime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagimana dikemukakan oleh Ronni R. Nitibaskara bahwa: "*Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan*

[2] J. E Sahetapy dalam Abdul Wahid, 2002, *Kriminologi dan Kejahatan Kontemporer*, Lembaga Penerbitan Fakultas Hukum Unisma, Malang.

[3] Edmon Makarim, 2005, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi)*, Jakarta PT Raja Grafindo Persada, hlm. 426.

hubungan sosial yang berupa kejahatan (crime) akan menyesuaiakan bentuknya dengan karakter baru tersebut."[4]

Ringkasnya, sesuai dengan ungkapan "*kejahatan merupakan produk dari masyarakat sendiri" (crime is a product of society its self)*, "habitat" baru ini, dengan segala bentuk pola interaksi yang ada didalamya, akan menghasilkan jenis-jenis kejahatan yang berbeda dengan kejahatan-kejahatan lain yang sebelumnya telah dikenal. Kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah *cybercrime.*

Pada masa awalnya, *cybercrime* didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa sarjana menggunakan istilah *computer misuse, computer abuse, computer fraud, computer related crime, computer assistend crime, atau computer crime.* Namun para sarjana pada waktu itu, pada umumnya lebih menerima pemakaian istilah *computer crime* oleh karena dianggap lebih luas dan bias dipergunakan dalam hubungan internasionl.

Dua dokumen Konferensi Perserikatan Bangsa-bangsa (PBB) tentang *The Prevention of Crime and The Treatment of Offenders* di

[4] Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, PT Refika Aditama, hlm. 25.

Havana (Cuba) tahun 1990, dan di Wina (Austria) tahun 2000, memang ada dua istilah yang digunakan: *cybercrime,* dan *computer-related crime*. Laporan Dokumen Kongres PBB ke-10 di Wina, tanggal 19 Juli 2000 menggunakan istilah *computer-related crime*, dengan pengertian 2 bentuk berikut:

> *The term computer-related crime had been developed encompass both the entirely new formst of crime that were directed at computer, networks and their users, and the more traditional from crime that were now being commited with the use or assistance of computer equipment.*
>
> *a. Cybercrime in narrow sense (computer crime); any illegal beheviour directed by means of electronic operations that targets the security of computer system and the data processed by them.*
> *b. Cybercrime in broader sense (computer-related crime); any illegal behavior commited by means of, or in relation to, a computer system network, including such crimes as illegal possession, offering or distributing information by means of computer system an network.*[5]

Berdasarkan laporan tersebut dapat dimengerti bahwa *cybercrime* dibedakan menjadi 2 pengertian, yaitu dalam pengertian sempit dan luas. Dalam pengertian sempit, *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer sebagi sasaran atau target kejahatan, baik pada keamanan sistem maupan datanya. Sedangkan *cybercrime* dalam arti luas merupakan keseluruhan bentuk kejahatan yang ditunjukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer. Pengertian

[5] Agus Rahardjo, 2002, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung, PT Citra Aditiya Bakti, hlm 32 dalam Widodo, 2011, *Aspek Hukum Kejahatan Mayantara*, Yogyakarta, Aswindo, hlm. 7

yang digunakan dalam istilah *cybercrime* adalah dalam pengertian luas.

Pengkategorian jenis *cybercrime* menjadi dua tersebut selaras dengan *The Encyelopedia of Crime and Justice* yang menjelaskan bahwa ada dua kategori kejahatan yang *cybercrime*, yaitu:

a. *In the first, computer is a tool of a crime, such as froud, embezzlement, and thieft of property, or is used to plan manage a crime.*
b. *In the second, the computer is aobject of a crime, such as sabotage, theft or alteration of storage data, or theft of it service.*[6]

Dari definisi yang diberikan oleh departemen kehakiman Amerika, penyalahgunaan komputer dibagi atas dua bidang utama. Pertama, adalah penggunaan komputer sebagia alat untuk melakukan kejahatan, contoh kasusnya adalah pencurian. Kemudian, yang kedua adalah komputer tersebut merupakan objek atau sasaran dari tindak kejahatan tersebut, contoh kasusnya adalah sabotase komputer sehingga tidak dapat berfungsi sebagimana mestinya.

Pengertian *cybercrime* menurut Prof Widodo adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum

[6] Widodo, 2011, *Aspek Hukum Kejahatan Mayantara*, Yogyakarta, Aswindo, hlm. 7

secara material maupun melawan hukum secara formal.[7] Kemudian, definisi lain mengenai kejahatan komputer ini dikeluarkan oleh *Organization of European Community Development* (OECD) yaitu sebagai berikut: " *any illegal, unethicall or unauthorized behavior relating to the authomathic processing and/or the transmission of data".*[8] Dari definisi tersebut, kejahatan komputer ini termasuk segala akses illegal atau akses secara tidak sah terhadap suatu transmisi data. Sehingga telihat bahwa segala aktivitas yang tidak sah dalam suatu system komputer merupakan suatu kejahatan.

Batasan atau definisi dari kejahatan komputer juga diberikan oleh Andi Hamzah, menurut Andi Hamzah, bahwa "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal".[9] Dari pengertian yang diberikan oleh Andi Hamzah dapat disimpulkan bahwa beliau memperluas pengertian kejahatan komputer, yaitu segala aktivitas tidak sah yang memanfaatkan komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau illegal merupakan suatu kejahatan.

Cybercrime memiliki beberapa karakteristik, yaitu:[10]

---

[7] *Ibid.*,

[8] Eddy Djunedi Karnasudiraja, 1993, *Yurisprudensi Kejahatan Komputer*, Jakarta, CV Tanjung Agung, hlm. 3.

[9] Andi Hamzah, 1989, *Aspek-aspek Pidana di Bidang Komputer*, Jakarta, Sinar Grafika, hlm. 26.

[10] Abdul Wahid dan M. Labib, 2005, *Kejahatan Mayantara (Cybercrime)*, Bandung, Rafika Aditama, hlm. 76 dalam Budi Suhariyanto, 2013, *Tindak Pidana Teknologi Informasi (Cybercrime) : Urgensi Pengaturan dan Celah Hukumnya*, Jakarta, PT Raja Grafindo Persada, hlm. 13.

a. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber* (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.
c. Perbuatan tersebut mengakibatkan kerugian materill maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasian informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensionla.
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
e. Perbuatan tersebut sering dilakukan secara transnasional/melintas batas negara.

Cybercrime atau kejahatan dunia maya dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi, hal ini sejalan dengan pengertian yang diberikan oleh Donn B. Parker yang memberikan definisi mengenai penyalahgunaan komputer :"*Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain*", dan diterjemahkan oleh Andi Hamzah sebagai "penyalahgunaan komputer

didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan".[11]

Kejahatan dalam bidang teknologi informasi secara umum terdiri dari dua kelompok, yaitu :

a. Kejahatan konvensional yang menggunakan bidang teknologi informasi sebagai alat bantunya, contohnya pembelian barang dengan menggunakan nomor kartu kredit curian melalui media internet;
b. Kejahatan timbul setelah adanya internet, dengan menggunakan sistem komputer sebagai korbannya, contoh kejahatan ini ialah perusak situs internet (*cracking*), pengiriman virus atau program-program komputer yang bertujuan untuk merusak sistem kerja komputer.

Menurut Petrus Reinhard Golose, dalam kasus kejahatan dunia maya, baik korban maupun pelaku tidak berhadapan langsung dalam 1(satu) tempat kejadian perkara. Dalam beberapa kasus, baik korban maupun pelaku dapat berada pada negara yang berbeda. Hal tersebut menggambarkan bahwa kejahatan dunia maya merupakan salah satu bentuk kejahatan lintas negara (*transnational crime*), dan tak berbatas

[11] Donn B.Parker, 1976, Crime by Computer, Hlm.12, 'Andi Hamzah, 1993, *Hukum Pidana yang berkaitan dengan komputer*, Sinar Grafika Offset, hlm. 18

(*borderless*), tanpa kekerasan (*non violence*), tidak ada kontak fisik (*no phisically contact*) dan tanpa nama (*anonimity*).[12]

2. Pengaturan Tindak Pidana *Cybercrime* di Indonesia

a. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi,

Dalam undang-undang tersebut terdapat beberapa pasal yang mengatur perbuatan yang dilarang yang termasuk tindak pidana *cybercrime*. Sebelum ada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan dalam tindak pidana *cybercrime*. Namun undang-undang ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana *cybercrime* yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomudir tindak-tindak pidana yang berkaitan dengan komputer.

> **"**Pasal 22 yang berbunyi**: "**Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi :
> 1) Akses ke jaringan telekomunikasi; dan atau
> 2) Akses ke jasa telekomunikasi; dan atau
> 3) Akses ke jaringan telekomunikasi khusus."
>
> "Pasal 38 yang berbunyi : "Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi"
>
> "Pasal 40 yang berbunyi : "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun"

[12] Petrus Reinhard Golose, 12 April 2007, *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia* dalam Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI, Jakarta, hlm. 19

Bentuk-bentuk tindak pidana *cybercrime* dalam Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi adalah Akses Illegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi. Hal ini merujuk pada pengertian *cybercrime* yang diberikan oleh Konferensi PBB yang menyatakan *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada sistem keamnanya. Telekomunikasi merupakan salah satu bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal pasal tersebut dapat dikategorikan menjadi tindak pidana *cybercrime*.

b. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Tanggal 23 April 2008 telah diundangkan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini bukanlah undang-undang tindak pidana khusus, melainkan juga memuat tentang pengaturan mengenai pengelolaan informasi dan transaksi elektronik dengan tujuan pembangunan, namun undang-undang ini juga mengantisipasi pengaruh buruk dari pemanfaatan kemajuan teknologi ITE tersebut, yakni dengan diaturnya hukum pidana khususnya tentang tindak pidana yang menyerang kepentingan hukum orang pribadi,

masyarakat, atau kepentingan hukum Negara dengan memanfaatkan kemajuan teknologi ITE, atau sering disebut tindak pidana *cybercrime*.

UU ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang ITE (*cybercrime*) dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Tindak Pidana *Cybercrime* dalam UU ITE diatur dalam 9 pasal, dari pasal 27 sampai dengan pasal 35. Dalam 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 samapai dengan Pasal 34. Sementara ancaman pidananya ditentukan didalam Pasal 45 sampai Pasal 52. Adapun rumusan pasal-pasal tersebut adalah sebagai berikut:

> **"**Pasal 27 yang berbunyi :
> 1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
> 2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
> 3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau

Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

“Pasal 28 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).”

“Pasal 29 yang berbunyi**: “**Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.”

“Pasal 30 yang berbunyi:

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

“Pasal 31yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/

atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah."

"Pasal 32 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum 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 publik.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."

"Pasal 33 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

"Pasal 34 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
    a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk

memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33

b) 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

2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum."

"Pasal 35 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."

"Pasal 36 yang berbunyi: " Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain."

"Pasal 37 yang berbunyi**: "**Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia."

Dari uraian rumusan pasal-pasal bentuk-bentuk tindak pidana *Cybercrime* menurut Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diklasifikasikan menjadi 2 bentuk yakni:

1) *Cybercrime* yang menggunakan komputer sebagai alat kejahtan, yakni Pornografi Online (*Cyber-Porno*), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui komputer, pemalsuan melalui komputer,

pemerasan dan pengancaman melalui komputer, penyebaran berita bohong melalui komputer, pelanggaran terhadap hak cipta, *cyber terrorism*

2) *Cybercrime* yang berkaitan dengan komputer, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (*illegal acces)*, menggangu sistem komputer dan data komputer, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan komputer.

c. Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Perbutan yang dilarang dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sama dengan perbuatan yang dilarang dengan Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik tidak ada penambahan maupun pengurangan tindak pidana tersebut yang diancam pemidanannya, sehingga bentuk-bentuk *cybercrime* masih sama dengan undang-undang sebelumnya. Perbedaan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah sebagai berikut :

TABEL I

PERBANDINGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG ITE DENGAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG ITE

No	UU No 11 Tahun 2008 tentang ITE	UU No 19 tahun 2016 tentang Perubahan UU No 11 Tahun 2008 tentang ITE
1.	Dalam Pasal 1 mengenai ketentuan umum terdapat 23 poin ketentuan-ketentuan umum	Dirubah dengan penambahan dalam Pasal 1 yakni Pasal 1 diantara angka 6 dan angka 7 disipkan 1 angka yakni angka 6a, ketentuan mengenai Penyelenggara Sistem Elektronik
2.	Rumusan pasal mengenai bentuk-bentuk tindak pidana	Rumusan bentuk-bentuk tindak pidana ITE masih tetap sama dengan UU sebelumnya tidak ada penambahan rumusan pasal mengenai perbuatan yang dilarang hanya terdapat perubahan dalam pasal 31
3	Tidak adanya penjelasan mengenai Pasal 5 tentang alat bukti elektronik	Dirubah dengan penambahan penjelasan dalam Pasal 5

4.	Tidak adanya kewajiban penyelenggara sistem elektronik untuk menghapus Informasi Elektronik yang tidak relevan berdasarkan penetapan pengadilan	adanya kewajiban penyelenggara sistem elektronik untuk menghapus Informasi Elektronik yang tidak relevan berdasarkan penetapan pengadilan
5.	Segala bentuk penyadapan tidak diperbolehkan	Penyadapan boleh dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan
6.	Dalam hukum acara yang digunakan ada ketentuan khusus dalam hal pengeledahan, penyitaan barang bukti yakni mutlak harus melalui izin pengadilan	Adanya perubahan dalam penggeledahan dan penyitaan barang bukti elektronk dilakukan sesuai dengan ketentuan hukum acara pidana dalam KUHAP

Sumber : Diolah secara pribadi dari hasil penelitian

3. Yurisprudensi dalam Tindak Pidana *Cybercrime* di Indonesia

Yurisprudensi adalah Suatu keputusan hakim yang terdahulu yang diikuti oleh hakim-hakim lainnya dalam perkaranya yang sama. Berikut beberapa perkara *cyber* yang pernah diputus oleh pengadilan di Indonesia :

a. Kasus di Bank Danamon. Pelakunya, orang dalam bank tersebut, dan dijatuhi hukuman karena terbukti melakukan pemalsuan, sebagaimana dimaksud Pasal 264 ayat 2 KUHPidana. Tindak

kejahatan itu dilakukan dengan cara, pelaku terlebih dulu membuka rekening di Bank Danamon Cabang Utama dengan nama dan alamat palsu. Sebagai orang dalam pelaku mempelajari bagaimana melakukan akses. Setelah paham, melalui komputer di ruang kerjanya, pelaku menggunakan USER ID dan *password* tertentu untuk memindahkan uang dari kantor pusat, dan dikreditkan pada rekening miliknya. Kerugian mencapai Rp 372.100.000.

b. Dani Firmansyah merupakan pelaku *hacking* situs *http://tnp.kpu.go.id* milik Komisi Pemilihan Umum pada tanggal 17 April 2004. Dalam tuntutan jaksa Dani telah melanggar ketentuan dalam Pasal 22 huruf a Jo. Pasal 5 Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Pasal 22 huruf b. Jo. Pasal 5 Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, dari tuntutan jaksa tersebut Dani melakukan Tindak Pidana *cybercrime* bentuknya adalah akses ilegal atau sering disebut hacking. Dani menyatakan bahwa keinginannya untuk melakukan *hacking* ini didasarkan atas dasar perkataan dari Tim Ahli Komisi Pemilihan Umum dan anggota KPU yang menyatakan bahwa situs yang dikelolanya tersebut aman dengan sistem pengamanan tujuh lapis (*seven layers*). Oleh karena itu pelaku ingin membuktikan bahwa situs tersebut tidak aman tidak sepertiyang dikatakan mereka. Dalam putusan NOMOR :

1322/PID.B/2004/PN.JKT.PST bahwa Dani Firmansyah terbukti bersalah melakukan tindak pidana "Tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi.

B. Bentuk-bentuk Tindak Pidana *Cybercrime*

Cybercrime mempunyai bentuk beragam, karena setiap negara tidak selalu sama dalam melakukan kriminalisasi. Begitu pula, dalam setiap negara dalam menyebut apakah suatu perbuatan tergolong kejahatan *cybercrime* atau bukan kejahatan *cybercrime* juga belum tentu sama. Secara teoritik, berkaitan dengan konsepsi kejahatan. Muladi mengemukakan bahwa asas *mala in se* mengajarkan bahwa suatu perbuatan dikategorikan sebagai kejahatan karena masyarakat dengan sendirinya menganggap perbuatan tersebut jahat. Sedangkan berdasarkan asas *mala prohibita,* suatau perbuatan dianggap jahat karena melanggar peraturan perundang-undangan.[13] Asas *Mala Prohibita* menghasilkan konsep si kejahatan dalam arti yuridis (yaitu sebagaimana diatur dalam peraturan perundang-undangan tertulis).

Jonathan Rosenoer menjelaskan tentang bentuk-bentuk *cybercrime* sebagai berikut:

1. *Copright, include exclutive right, subject matter of copyright, formalities, infringement, source of risk, word wide web sites, hypertext link, graphical element, e-mail, criminal liability, fair use, first amandment, and softwere rental.*
2. *Trademark*
3. *Defamation*

[13] Muladi, 2002, *Demokratisasi , Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, Jakarta, Habibie Center, hlm. 196

4. *Privacy, include common law privacy, constitutinal law, anonymity, and technology expanding privacy right.*
5. *Duty of care*
    a. *Negligence*
    b. *Negligent misstatement*
    c. *Equipment malfunctions*
    d. *Economic loss may not be recoverable*
    e. *Contractural limitations of liability.*
6. *Criminal liability; such as; computer fraud and abuse act, wire fraund. Electronic communication privacy act, extortion and threats, expose, sexual exploitation of children, obscene and indent telephone call, copyright stalking.*
7. *Procedural issues, include jurisdiction, venue and conflict of law.*
8. *Electronic contract and digital signature, include electronic agreement enforceable, public key encryption and digital signature*.[14]

Cybercrime meliputi pelanggaran hak kekayaan intelektual, fitnah atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi (*privacy*), ancaman dan pemerasan, ekploitasi seksual anak-anak dan pencabulan, perusakan sistem komputer, pembobolan kode akses, dan pemalsuan tanda tangan digital. Semua perbuatan tersebut dapat dipertanggungjawabkan secara pidana sesuai dengan yurisdiksinya. *Cybercrime* juga dapat berbentuk pemalsuan data, penyebaran virus komputer ke jaringan komputer atau sistem komputer, penambahan atau pengurangan sistem instruksi dalam jaringan komputer, pembulatan angka, perusakan data, dan pembocoran data rahasia. Ini diuraikan oleh Sue Titus Reid, bahwa *cybercrime* meliputi "*data diddling, the Trojan horse, the salami technique, superzapping, and date leakgage*."[15]

---

[14] Jonathan Rosenoer, 1997, *Cyberlaw: The Law of the Internet,* New York, Spring-Verlag, hlm. 45.

[15] Sue Titus Reid, 1985, *Crime and Criminology*, New York, CBS College Publishing, hlm. 56

The International Hendbook on Computer Crime mengklasifikasikan bentuk-bentuk *cybercrime* sebagai berikut.

1. *Computer-related Economic Crimes*
   a. *Fraund by Computer Manipulation*
   b. *Computer Espionage and Software Piracy*
   c. *Computer Sabotage*
   d. *Theft of Services*
   e. *Unauthorized Access to DP Systems and Hacking*
   f. *The Computer as a Tool for traditional Business Offences*
2. *Computer-related Infrigements of Privacy*
   a. *Use of Incorrect Data*
   b. *Illegal Collection and Storage of Correct Data*
   c. *Illegal Disclosure and Misuse of data*
   d. *Infrigments of Formalities of Privancy Laws*
3. *Further Abuses*
   a. *Offences Against State and Political Interests*
   b. *The Extension to Offences Against Personal Intergity.*[16]

Berdasarkan uraian *Handbook on Computer Crime, cybercrime* dikategorikan menjadi tiga. Kategori pertama, *cybercrime* adalah kejahatan ekonomi yang terkait dengan komputer, meliputi penipuan dengan manipulasi komputer, pembajakan perangkat lunak komputer, spionase komputer, sabotase, pencurian jasa, akses tidak sah ke dalam sistem atau jaringan komputer, komputer sebagai alat untuk menyerang bisnis tradisional. Kategori ke dua, adalah pelanggaran terhadap keleluasaan pribadi, yaitu penggunaan data yang tidak benar, pengumpulan data secara tidak sah, penyalahgunaan data, pelanggaran rahasia perusahaan. Sedangkan kategori ke tiga, misalnya melakukan penyerangan terhadap dan kepentingan politik, dan penyerangan terhadap kebebasan pribadi orang per orang.

[16] *Ibid.,*

Selain penggolongan *cybercrime* sebagaimana terjabar di atas, Donn Parker mengklasifikasikan bentuk-bentuk *cybercrime* ke dalam empat klarifikasi berikut.

1. Komputer sebagai Objek

   Dalam kategori ini, bentuk-bentuk *cybercrime* termasuk kasus-kasus perusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusakan terhadap sarana-sarana komputer seperti *Air Condutouring* (AC) dan peralatan yang menunjang pengoprasian komputer.

2. Komputer sebagai Subjek

   Komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya pencurian, penipuan, dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh (*intangible*), misalnya pulsa elektronis dan guratan-guratan magnetis.

3. Komputer sebagai Alat

   Komputer digunakan sebagai alat melakukan kejahatan sehingga sifat peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh adalah seseorang pelaku kejahtan yang mengambil warkat-warkat setoran darai suatu bank dan menulis nomor rekening pelaku dengan tinta magnetis pada warkat-warkat tersebut kemudian melaetakkan kembali ke tempat semula. Nasabah yang akan

memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomor rekening pelaku kejahatan memroseswarkat-warkat nasabah, komputer secara otomatis akan mengredit sejumlah uang pada rekening pelaku kejahtan. Salah iyu, pelaku kejahtan menarik uang dengan cek dari rekeningnya sebelum peram nasabah yang menyetor mengajukan complain ke bank.

4. Komputer sebagai simbol

   Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman, dalam kategori ini termasuk penipuan "Biro Jodoh" yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu si koraban mencari jodoh, akan tetapi ternyata birojodoh tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.[17]

Kejahatan yang berhubungan dengan komputer (*cybercrime*) sudah diatur oleh istrumen internasional. Satu-satunya instrument internasional yang mengatur kejahtan yang berhubungan dengan komputer adalah *Convention on Cybercrime*. Dalam Bab II konvensi tersebut diatur tentang hukum pidana substantive, yaitu sebagiaman terjabar dalam Pasal (*article*) 2 sampai dengan Pasal 11. Sedangkan Pasal 12-13 mengatur mengenai ketentuan pemidanaan. Ketentuan tersebut adalah seabagai berikut.

1. *Title 1, offences against the confidentiality, integrity and availability of computer data and system.*

[17] Widodo, *Op. Cit.,* Hlm. 199.

a. *Illegal access (article 2);*
b. *Illegal interception (article 3);*
c. *Data interference,*
d. *Damaging, deleting, deterioration, alteration or suppression of computer data without right (article 4);*
e. *System interference (article 5);*
f. *Misuse of devices (access code) (article 6).*

2. *Title 2, Computer Related Offences:*
   a. *Computer related forgery (article 7);*
   b. *Computer related fraud (article 8).*
      1) *Title 3, Content Related Offences:*
      2) *Title 4, Offences Related to Infringement of Copyright and Related Right (article 10).*
      3) *Title 5, Ancillary laiability and sanction (article 11); (article 12, (article 13).*

Berdasarkan ringkasan ketentuan dalam *Convention on Cybercrime* dapat dipahami bahawa dalam bagian 1, Pelanggaran terhadap kerahasiaan, ketersediaan dan integeritas sistem dan data komputer, terdiri atas perbutan berikut.

1. Akses tidak sah, yaitu sengaja memasuki atau mengakses komputer tanpa hak (Pasal 2);
2. Intersepsi tidak sah, yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman transmisi dan pemancaraan (emisi) data komputer yang tidak bersifat public ke, dari atau di dalam sisitem komputer dengan menggunakan alat bnatu teknis (Pasal 3);
3. Gangguan atau perusakan data, yaitu sengaja dan tanpa hak melakukan perusakan.
4. Penghapusan, perubahan atau penghapusan data komputer (Pasal 4);

5. Gangguan atau perusakan sistem, yaitu sengaja melakukan gangguan atau rintangan secara serius tanpa hak terhadap berfungsinya sistem komputer (Pasal 5);
6. Penyalahgunaan peralatan, yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, *password* komputer, kode masuk (*access code*) (Pasal 6).

Kemudian dalam bagian 2, diatur tentang pelanggaran yang berhubungan dengan komputer, yaitu dalam bentuk berikut.

1. Pemalsuan yang berhubungan dengan komputer (Pasal 7), yaitu pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data otentik menjadi tidak otentik dengan maksud untuk digunakan sebagai data otentik);
2. Penipuan yang berhubungan dengan komputer (Pasal 8), yaitu penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang atau kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer, atau dengan mengganggu berfungsinya komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

Selanjutnya dalam bagian 3 tentang Pelanggaran yang berhubungan dengan isi, yaitu berkaitan dengan delik-delik yang berhubungan dengan pornografi anak (Pasal 9), yaitu meliputi perbuatan:

1. Memproduksi dengan tujuan mendistribusikan melalui sistem komputer;
2. Menawarkan melalui sistem komputer;
3. Mendistribusikan atau mengirim melaui sistem komputer;
4. Memperoleh melalui sistem komputer;
5. Memiliki dalam sistem komputer atau di dalam media penyimpanan data.

Akhirnya dalam bagian 4 tentang Pelanggaran yang berhubungan dengan Hak Cipta (Pasal 10), yaitu delik-delik yang terkait dengan pelanggaran hak cipta. Sedangkan pada bagian 5, diatur tentang pertanggungjawabkan pidana dan sanksi; Percobaan dan Pembantuan (Pasal 11); Pertanggungjawaban Korporasi (Pasal 12); Sanksi dan tindakan (Pasal 13).

Berdasarkan ketentuan-ketentuan dalam konvensi tersebut dapat disimpulkan bahwa delik-delik *cybercrime* suadah diatur secara umum dalam konvensi. Meskipun demikian, setiap Negara diberi peluang untuk mengembangkan dan mengharmonisasikan dengan kebutuhan Negara yang bersangkutan tanpa mengesampingkan kepentingan masyarakat internasional. Karena itu, bahasa yang digunakan bersifat netral, dan bentuk-bentuk kejahatan yang diatur dalam konvensi adalah ketentuan setandar minimum.

Modus Operandi dan berkembangnya tindak pidana *cybercrime* sehingga bentuk-bentuk tindak pidana *cybercrime* semakin banyak. Hal ini

dipengaruhi oleh beberapa faktor. Faktor-Faktor Terjadinya Tindak Pidana *Cybercrime*

1. Kesadaran Hukum Masyarakat

   Proses penegakan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. *Cybercrime* adalah sebuah perbuatan yang tercela dan melanggar kepatutan di dalam masyarakat serta melanggar hukum. Sampai saat ini, kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cybercrime* kurang. Hal ini disebabkan anatara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahtan *cybercrime*. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvesional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya.

   Sehingga hal tersebut membuat kejahatan tersebut meningkata dan meluas akibatnya.

2. Faktor Keamanan

   Rasa aman tentunya akan dirasakan oleh pelaku kejahatan *Cybercrime* pada saat sedang menjalankan aksinya. Hal ini tidak lain karena internet lazim dipergunakan di tempat-tempat yang relatif tertutup, seperti di rumah, kamar, tempat kerja, perpustakaan dan warung internet. Aktivitas yang dilakukan oleh pelaku di tempat-tempat tersebut sulit untuk diketahui oleh pihak luar. Akibatnya pada saat

pelaku sedang melakukan tindak pidana sangat jarang orang luar mengetahuinya. Hal ini, sangat berbeda dengan kejahatan-kejahtan yang sifatnya konvensional, yang mana pelaku akan mudah diketahui secara fisik ketika sedang melakukan aksinya. Sehingga rasa aman yang diperoleh dalam melakukan tindak pidana tersebut membuat tindak pidana *cybercrime* terjadi terus menerus dan meningkat.

3. Faktor Penegak Hukum

   Faktor penegak hukum sering menjadi penyebab maraknya kejahatan siber (*cybercrime*). Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku. Sehingga tak jarang jika pelaku dapat lolos dari jeratan hukum dan tindak pidana tersebut semakin banyak.

4. Faktor Sosial Ekonomi

   Faktor ini juga mempengaruhi maraknya tindak pidana *cybercrime* karena Isu global yang kemudian dihubungkan dengan kejahatan tersebut sebenarnya merupakan masalah keamanan jaringan *(security network).* Keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang sangat membutuhkan perangkat keamanan jaringan. *Cybercrime* berada dalam skenario besar dalam kegiatan ekonomi dunia, sosial

ekonomi yang meningkat membuat celah-celah pelaku dalam menjalankan aksinya.

5. Faktor Globalisasi

   Adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini menjadi begitu dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan jaringan yang lain sehingga memudahkan pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat dari pada yang lain. Akses internet yang tidak terbatas. Dengan akses internet yang tidak terbatas pengguna internet dengan bebas mengakses situs-situs yang ada di internet sehingga hal ini menimbulkan adanya pelaku *cyber crime* dengan cara *download*, *upload* dan lain sebagainya secara illegal atau tidak sah.

C. Penegakan Hukum terhadap Tindak Pidana *Cybercrime*

Penegakan hukum merupakan suatu proses untuk mewujudkan keinginan-keinginan hukum menjadi kenyataan. Keinginan hukum inilah yang nantinya menjadi pikiran badan pembuat undang-undang yang dirumuskan dalam peraturan-peraturan hukum. Perumusan pikiran pembuat hukum dituangkan dalam peraturan hukum yang nantinya menentukan bagaimana penegakan hukum itu dijalankan. Pada kenyataannya proses penegakan hukum memuncak pada pelaksanaannya

oleh para pejabat penegak hukum.[18] Aparat penegak hukum di Indonesia adalah hakim, jaksa, polisi. Hakim adalah salah satu aparat penegak hukum yang melaksanakan suatu sistem peradilan yang mempunyai tugas untuk menerima dan memutus perkara dengan seadil-adilnya. Hakim adalah pejabat yang melakukan kekuasaan kehakiman yang diatur dalam Undang-undang Nomor 48 Tahun 2009 tentang kekuasaan kehakiman. Dalam rangka penegakan hukum di Indonesia tugas hakim adalah menegakkan hukum dan keadilan melalui perkara-perkara yang dihadapkan kepadanya. Jaksa adalah aparat penegak hukum yang merupakan pejabat fungsional yang diberikan wewenang oleh undang-undang dan pelasanaan putusan pengadilan. Selanjutnya adalah Polisi, polisi sebagai penegak hukum dituntut melaksanakan profesinya secara baik dengan dilandasi etika profesi. Etika profesi tersebut berpokok pangkal pada ketentuan yang menentukan peranan polisi sebagai penegak hukum. Polisi dituntut untuk melaksanakan profesinya dengan adil dan bijaksana, serta mendatangkan keamanan dan ketenteraman.

Penegakan hukum selalu akan melibatkan manusia di dalamnya dan dengan demikian hal tersebut tingkah laku manusia terlibat di dalamnya. Hukum tidak bias tegak dengan sendirinya sehingga melibatkan aparat penegak hukum, dan aparat dalam mewujudkan tegaknya hukum harus dengan undang-undang, sarana , dan kultur, sehingga hukum dapat ditegakkan dengan seadil-adilnya sesuai dengan cita hukum itu sendiri.

[18] Satjipto Rahardjo, 2009, *Penegakan Hukum Suatu Tinjauan Sosiologis,* Yogyakarta, Genta Publishing, Cetakan 1, hlm. 24.

Hal ini menunjukan bahwa tanntangan yang dihadapi oleh aparat penegak hukum bukan tidak mungkin sangatlah banyak Penegak hukum tidak hanya dituntut untuk professional dan tepat dalam menerapkan normannya akan tetapi juga dituntut dapat membuktikan kebenaran atas dakwaan kejahatan yang terkadang dipengaruhi oleh rangsangan dari prilaku masyrakat untuk sama-sama menjadi pelanggar hukum.

Pendapat Soerjono Soekanto mengatakan bahwa pokok penegakan hukum terletak pada faktor-faktor yang mempengaruhinya. Faktor-faktor tersebut, adalah sebagai berikut:[19]

1. Faktor hukumnya sendiri, yaitu peraturan perundang-undangan yang berlaku di Indonesia.
2. Faktor penegk hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum.
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.
5. Faktor kebudayaan, yakni sebagai hasil karya, cipta dan rasa yang didasarkan pada karsa manusia didalam pergaulan hidup.

Dari kelima faktor tersebut saling berkaitan dengan eratnya karena antara yang satu dengan yang lainnya saling mempengaruhi. Kelima faktor tersebut dapat dikatakan esensi dari penegakan hukum, dan dapat dijadikan tolok ukur daripada keefektifitasan penegak hukum di Indonesia.

[19] Soerjono Soekanto, 2014, *Faktor-faktor yang mempengaruhi Penegak Hukum*, Jakarta: Rajawali Pers, Cetakan 13, hlm. 8.

Kejahatan teknologi informasi atau *cybercrime* memiliki karakter yang berbeda dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Terkait dengan hukum pembuktian biasanya akan memunculkan sebuah posisi dilema, di salah satu sisi diharapkan agar hukum dapat mengikuti perkembangan zaman dan teknologi, di sisi yang lain perlu juga pengakuan hukum terhadap berbagai jenis-jenis perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan. Pembuktian memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Apabila hasil pembuktian dengan alat bukti yang ditentukan dengan undang-undang tidak cukup membuktikan kesalahan dari orang tersebut maka akan dilepaskan dari hukuman, sebaliknya apabila kesalahan dapat dibuktikan maka dinyatakan bersalah dan dijatuhi hukuman. Oleh karena itu harus berhati-hati, cermat dan matang dalam menilai dan mempertimbangkan masalah pembuktian.

Muncul kesulitan dalam penerapan hukum dan penegakan hukum terhadap tindak pidana *cybercrime* yakni dalam penyelesaian tindak pidana tersebut , kondisi yang *paperless* (tidak menggunakan kertas) ini menimbulkan masalah dalam pembuktian mengenai informasi yang diproses, disimpan, atau dikirim secara elektronik. mendasar penggunaan

bukti elektronik dalam proses pembuktian perkara pidana, khususnya yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik di dalam perundang-undangan kita. Selain itu sulitnya mengungkap tindak pidana tersebut baik pelaku, dan kejahtan yang sering sekali sulit untuk dibuktikan sehingga hal tersebut menjadi tantangan tersendiri dalam penegakan hukum tindak pidana *cybercrime*.

Setiap penegak hukum diberi kewenangan berdasarkan Peraturan Perundang-undangan yang berlaku untuk menjelaskan tugasnya. Dalam penanganan tindak pidana *cybercrime,* hukum acara yang digunakan yaitu hukum acara berdasarkan KUHAP. Hal tersebut memang tidak disebutkan secara jelas dalam atas Undang-undan Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi karena undang-undang tersebut tidak menetukan lain maka KUHAP berlaku bagi tindak pidana yang termuat dalam Undang-undan Nomor 11 tahun 2008. Dalam Pasal 42 UU Undang-undan Nomor 11 tahun 2008 disebutkan : "Penyidikan terhadap tindak pidana sebagimana dimaksud dalam undang-undang ini dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan Ketentuan dalam Undang-undang ini." Hal tersebut juga ditegaskan dalam UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa dalam perubahan tersebut sama sekali tidak merubah Pasal 43

Berdasarkan pasal tersebut sehingga dapat ditafsirkan bahwa Hukum Acara Pidana yang diatur dalam KUHAP merupakan *lex*

genaralis, sedangkan ketentuan acara dalam UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, ini merupakan *lex specialis*. Dengan demikian sepanjang tidak terdapat ketentuan lain maka ketentuan hukum acara yang digunakan seperti yang terdapat dalam KUHAP. Ketentran yang diatur lain dalam UU ITE ini yaitu menyangkut proses penyidikan dan penambahan satu alat bukti lain dalam penanganan tindak pidana yang diatur dalam UU ITE.

Pelaksanaan penyelidikan tindak pidana *cybercrime* agak sedikit berbeda dengan penyelidikan tindak pidana lainya, pejabat dalam hal ini adalah pejabat polisi Negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan (Pasal 1 angka 4 KUHAP) dihadapkan pada masalah dari mana dan dimana penyelidikan harus dimulai. Akibat perbuatan tindak pidana *cybercrime* seperti *cyber porno, cyber terrorism, hacking , dll* baik yang diketahui pertama kali oleh penyelidik yang sedang melukan *cyber-patroling* maupun berdasarkan laporan dari korban tindak pidana *cybercrime*, diketahui melalui layar monitor suatu komputer yang terhubung dengan jaringan melalui koneksi internet, ataupun terjun langsung ke warnet-warnet.

Proses awal penyelidikan harus melibatkan komputer, alat elektronik seperti handphone maupun android, tablet, dan jaringannya yang terkoneksi dengan suatu jaringan dan terkoneksi melalui internet. Bukti-bukti dalam suatu tindak pidan *cybercrime* biasanya sealu dapat

tersimpan di dalam istem alat alat elektronik tersebut ataupun sistem komputer. Dengan Demikian inti dari suatu proses penyelidikan adalah bagaimana menemukan dan selanjutnya menyita alat alat atau barang elektronik maupun komputer milik tersangka. Dari komputer tersebutlah penyelidikan dapat menentukan apakah ada bukti-bukti tindak pidana.

Karakteristik tindak pidana *cybercrime* berbeda dengan tindak pidana yang lain , karakteristik bentuk tindak pidana *cybercrime* antara yang satu dengan yang lain pun berbeda hal ini dikarenakan modus operandi yang digunakan berbeda. Sehingga dengan demikian dalam penegakan hukum dan dalam proses beracaranya dari tahap penyelidikan dan penyidikan memerlukan ketentuan khusus. Ketentuan khusus yang berkaitan dengan acara pidana yang terdapat dalam Undang-undang Nomor 11 Tahun 2008, yang telah dirubah oleh Undang-undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik adalah sebagai berikut;

1. Diakuinya alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cybercrime.*
2. Adanya wewenang khusus yang diberiakan kepada Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan transaksi elektronik sebagai penyidik

3. Adanya kewenangan penyidik, penuntut umum, dan hakim untuk meminta keterangan kepada penyedia jasa dan penyelenggara sistem elektronik mengenai data-data yang berhubungan dengan tindak pidana, dengan tetap terikat terhadap privasi, kerahasian, dan kelancaran layanan publik, integritas data dan keutuhan data.
4. Adanya wewenang terhadap penyidik untuk melakukan penggeledahan, penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat, hal ini menghindari agar sistem elektronik tersebut tidak bias hapus oleh pelaku dan menghindari agar pelacakan pelaku berjalan cepat, sehingga jejak pelaku mudah untuk ditemukan.

Upaya penegakan hukum terhadap tindak pidana *cybercrime* selain dengan aturan-aturan tersebut seharusnya juga diimbangi dengan skill dan kemampuan penegak hukumnya dalam pemberantasan tindak pidana *cybercrime.* Hal ini dikarenakan modus-modus tindak pidana *cybercrime* semakin hari semakin berkembang dikhawatirkan kejahatan tersebut akan merajalela dan pelaku-pelaku sulit untuk dilacak dan ditangkap, sehingga dapat merugikan masyarakat dan Negara dan bahkan dunia luas.