Vol. 03, No. 2 2021, pp. 1759 – 1774

Sultra Law Review

Vol. 03, No. 02 Oktober 2021
ISSN: *2685-208X* (Online)
Publisher: Fakultas Hukum Universitas Sulawesi Tenggara
Website: https://jurnal-unsultra.ac.id/index.php/sulrev

TINJAUAN TERHADAP TINDAK PIDANA CYBER CRIME (Suatu Studi di Reskrimum Polda Sultra)

Ibrahim, Muhammad Tahir, Basoddin

Program Studi Ilmu Hukum, Fakultas Hukum Universitas Sulawesi Tenggara

ARTICLE INFO

Keywords:
Cyber Crime,
Review,
Reskrimum Polda Sultra.

e-mail:
ibrahim88@gmail.com

Corresponding Author:
Ibrahim

Received:21/03/2021
Accepted:18/06/2021
Published:30/10/2021

ABSTRACT

The research aims (1) to find out what legal obstacles are faced by the Cyber Unit of the Southeast Sulawesi Regional Police in dealing with Cyber Crime, as well as obstacles in carrying out the investigation process related to the collection of evidence of Cyber Crime. (2) to find out the efforts that can be made by the court in carrying out the process of providing evidence to perpetrators of Cyber Crime, considering the difficulty of the criminal process related to the limited evidence in the crime. To carry out the research, the author focuses on the location at the Southeast Sulawesi Regional Police Criminal Investigation Unit and will then collect some data that the author will use to answer the problems raised in the thesis. Research results (1) The principle of legality in Indonesian criminal law provides a policy outline to realize legal protection against arbitrary actions by state authorities/organizers against the legal interests of society and human rights. Therefore, the system of proof based on the Criminal Procedure Code formally can no longer reach and be the legal basis for proof of Cyber Crimes cases, because the modus operandi of Cyber Crime crimes is not only carried out with sophisticated tools but this crime is really difficult to determine quickly and simply who is the perpetrator of the crime. Therefore, optimization of Law Number 11 of 2008 concerning Electronic Information and Transactions is needed. (2) The weakness of the legal apparatus in enforcing criminal law, especially in Cyber Crimes cases, has many limitations. This can be felt as if the crime that occurs, the law enforcement officers are not ready or even unable (technologically illiterate) to investigate the perpetrators and the evidence used in relation to this form of crime is difficult to detect. Another weakness is in the forensic computer equipment that is not yet owned by the National Police, considering the importance of its existence in preventing or handling cases related to Cyber Crime.

I. PENDAHULUAN

Teknologi informasi dan komunikasi telah mengubah perilaku mayarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan social yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi arena efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan Hukum Siber, yang diambil dari kata *Cyber Law* adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang digunakan adalah Hukum Teknologi Informasi *(Law Of Information Technology),* Hukum Dunia Maya *(Virtual World Law)* dan hukum Mayantara. Itilah-itilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbaris *virtual.* Istilah hukum siber digunakan dalam tulisan ini dilandasi pemikiran bahwa *cyber* jika diidentikan dengan *"Dunia Maya"* akan cukup menghadapi persoalan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu.

Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace, pertama* adalah pendekatan teknologi, *kedua* pendekatan sosial budaya-etika, dan *ketiga* pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalah gunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *Cyber Crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan Undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal I ayat (1) KUHP "Nullum delictum nulla poena sine praevia lege poenali" atau dalam istilah lain dapat dikenal, " tiada pidana tanpa kesalahan".

Bertolak dari dasar pembenaran sebagaimana diuraikan di atas, bila dikaitkan dengan *Cyber Crime,* maka unsur membuktikan dengan kekuatan alat bukti yang sah dalam hukum acara pidana merupakan masalah yang tidak kalah pentingnya untuk diantisipasi di samping unsur kesalahan dan adanya perbuatan pidana. Akhirnya dengan melihat pentingnya persoalan pembuktikan dalam *Cyber Crime,* skripsi ini hendak mendeskripsikan pembahasan dalam fokus masalah Hukum Pembuktian terhadap *Cyber Crime* dalam Hukum Pidana Indonesia.

Oleh karena alasan-alasan tersebut di atas, bagaimana pembuktian-pembuktian dalam *Cyber Crime* cukup sulit dilakukan mengingat, bahwa hukum di Indonesia yang mengatur masalah ini masih banyak cacat hukum yang dapat dimanfaatkan oleh para pelaku *Cyber Crime* untuk lepas dari proses pemidaan.

Kegiatan siber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang siber sudah tidak pada tempatnya lag] untuk kategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan siber adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Penggunaan hukum pidana dalam mengatur masyarakat (lewat peraturan perundang-undangan pidana) pada hakekatnya merupakan bagian dari suatu langkah kebijakan *(policy).* Selanjutnya untuk menentukan bagaimana suatu langkah (usaha) yang rasional dalam

melakukan kebijakan tidak dapat pula dipisahkan dari tujuan kebijakan pembangunan itu sendiri secara integral. Dengan demikian dalam usaha untuk menentukan suatu kebijakan apapun (termasuk kebijakan hukum pidana) selalu terkait dan tidak terlepaskan dari tujuan pembangunan nasional itu sendiri; yakni bagaimana mewujudkan kesejahteraan bagi masyarakat.

Selain itu, perkembangan hukum di Indonesia terkesan lambat, karena hukum hanya akan berkembang setelah ada bentuk kejahatan baru. Jadi hukum di Indonesia tidak ada kecenderungan yang mengarah pada usaha preventif atau pencegahan, melainkan usaha penyelesaiannya setelah terjadi suatu akibat hukum. Walaupun begitu, proses perkembangan hukum tersebut masih harus mengikuti proses yang sangat panjang, dan dapat dikatakan, setelah negara menderita kerugian yang cukup besar, hukum tersebut barn disahkan. Kebijakan hukum nasional kita yang kurang bisa mengikuti perkembangan kemajuan teknologi tersebut, justru akan mendorong timbulnya kejahatairkejahatan baru dalam masyarakat yang belum dapat dijerat dengan menggunakan hukum yang lama. Padahal negara sudah terancam dengan kerugian yang sangat besar, namun tidak ada tindakan yang cukup cepat dari para pembuat hukum di Indonesia untuk mengatasi masalah tersebut.

II. TINJAUAN PUSTAKA

A. Pengertian Tindak Pidana

Tindak pidana berasal dari suatu istilah dalam hukum belanda yaitu *strafbaarfeit.* Ada pula yang mengistilahkan menjadi *delict* yang berasal dari bahasa latin *delictum.* Hukum pidana negara *anglo saxon* memakai istilah *offense atau criminal act.* Oleh karena itu KUHP Indonesia bersumber pada Wetbook van strafrecht Belanda, maka memakai istilah aslinya pun sama yaitu *Strafbaarfeit. Strafbaarfeit* telah diterjemahkan dalam bahasa indonesia sebagai:

1. Perbuatan yang dapat atau oleh dihukum.
2. Peristiwa pidana.
3. Perbuatan pidana.
4. Tindak pidana dan
5. Delik.

Menurut P. Simons yang menggunakan istilah peristiwa pidana adalah perbuatan atau tindakan yang diancam dengan pidana oleh Undang-undang, bertentangan dengan hukum dan dilakukan oleh orang yang mampu bertanggung jawab. Simon memandang semua syarat untuk menjatuhkan pidana sebagai unsur tindak pidana dan tidak memisahkan unsur yang melekat pada perbuatannya *(crime act)* tindak pidana dengan unsur yang melekat pada aliran tindak pidana *(criminal responsibility* atau *criminal liability* atau pertanggung jawaban pidana). Kemudian dia menyebut unsur unsur tindak pidana, yaitu perbuatan manusia, diancam dengan pidana, melawan hukum, dilakukan dengan kesalahan, oleh orang yang mampu bertanggung jawab.

Moeljatno memberikan pengertian tentang perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, barang siapa melanggar larangan tersebut. Larangan tersebut ditujukan kepada perbuatan, sedangkan ancaman pidananya ditujukan pada orang yang menimbulkan kejadian itu. Moeljatno memisahkan antara *criminal act* dan *criminal responsibility* yang menjadi unsur tindak pidana.

Menurut Moeljatno hanyalah unsur-unsur yang melekat pada *criminal act* (perbuatan yang dapat dipidana). Sedangkan yang termasuk unsur-unsur tindak pidana adalah perbuatan (manusia), memenuhi rumusan Undang-undang, bersifat melawan hukum.

B. Pengertian Informasi, Transaksi Elektronik Dan Dokumen Elekronik Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE)

Dalarn ketentuan umum Pasal 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan, bahwa Informasi elektronik adalah satu atau sekumpulan data elektronik, tennasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (*electronic 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. 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, gatnbar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

C. Pengertian Cyber Crime

Berbicara masalah cyber crimetidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internetdalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalau dimutaakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya (cyber crime) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Untuk lebih mendalam ada beberapa pendapat di bawah ini tentang apa yang dimaksud dengan cyber crime? Di antaranya adalah Menurut Kepolisian Ingris, Cyber crimeadalah segala macam penggunaan jaringan computer untuk tujuan criminal dan/atau criminal berteknologi tinggi dengan menyalahgunakankemudahan teknologi digital.

Sedangkan menurut Indra Safitri mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet

Dari pengertian kejahatan komputer menurut peraturan perundang-undangan di Virginia dapat dipahami bahwa sesuatu yang berhubungan dengan peralatan pemerosesan data listrik, magnetic, optic, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melalukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau tipesetter, sebuah kalkulator tangan atau peralatan serupa lainnya.

D. Jenis-jenis Cyber Crime

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:

1. Unauthorized Access to Computer System and Service

2. Illegal Contents
3. Data Forgery
4. Cyber Espionage
5. Cyber Sabotage and Extortion
6. Offense against Intellectual Property
7. Infringements of Privacy

E. Pengaturan tentang Cyber Crime

Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang yang diharapkan (iuskonstituendum) adalah perangkathukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan Internetdengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi. Saat ini, Indonesia belum memiliki Undang-Undang khusus yang mengatur mengenai cyber crime walaupun rancangan undang undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari rancangan undang-undang tindak pidana di bidang teknologi informasi sejak tahun 2004 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki.

Sebagai langkah preventif terhadapsegala hal yang berkaitan dengan tindak pidana di bidang komputer khususnya cyber, sedapat mungkin dikembalikan pada peraturan perundang-undangan yang ada, yaitu KUHP (Kitab Undang-undang Hukum Pidana) dan peraturan di luar KUHP. Pengintegrasian dalam peraturan yang sudah ada berarti melakukan suatu penghematan dan mencegah timbulnya over criminalization, tanpa mengubah asas-asas yang berlaku dan tidak menimbulkan akibat-akibat sampingan yang dapat mengganggu perkembangan teknologi informasi.

Ada beberapa hukum positif yang berlaku umum dan dapat dikenakan bagi para pelaku cyber crime terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

1. Kitab Undang Undang Hukum Pidana
2. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta.
3. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi
4. Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan
5. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

F. Pengertian Alat Bukti Menurut Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik pasal 5 ayat I dan 2 mendeskripsikan bahwa Dokumen elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain dalam pasal 44 Undang-undang yang sama mengatakan:"Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai herikut :

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang undangan; dan
b. alat hukti lain berupa Inforinasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka I dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3). "

G. Kejahatan Dunia Maya *(CYBER CRIME)*

Kejahatan adalah perbuatan merugikan orang lain dan/atau sekelompok orang dan/atau

instasi yang dilakukan dengan bertujuan untuk menguntungkan diri sendiri, baik secara materi maupun kejiwaannya. Kejahatan dapat dilakukan dengan menggunakan fasilitas apapun sebagai alat untuk nelakukan perbuatannya, termasuk di dalamnya adalah perangkat Tnformasi dan Transaksi Elektronik, contohnya seperti komputer, *credit card,* televisi, dan lain sebagainya.

Istilah *cyberspace* muncul pertama kali dari novel William Gibson berjudul Neuromancer pada tahun 1984. Istilah *cyberspace* pertama kali digunakan untuk menjelaskan dunia yang terhubung langsung *(online)* ke internet oleh Jhon Perry Barlow pada tahun 1990. Secara etimologis, *istilah cyberspace* sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir. Cambridge Advanced Learner's Dictionary memberikan definisi *cyberspace* sebagai *"the Internet considered as an imaginary area without limits where you can meet people and discover information about any subject". The American Heritage Dictionary of' English Language Fourth Edition* mendefinisikan cyberspace sebagai *"the electronic medium of computer networks, in which online communication takes place".* Pengertian *cyberspace* tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet. Bruce Sterling mendefinisikan *cyberspace* sebagai *the `place' where a telephone conversation appears to occur".*

Kejahatan Dunia Maya *(Cyber Crime)* merupakan suatu tindak kejahatan atau perbuatan mclawan hukum yang dilakukan dengan mcnggunakan mediasi dunia maya atau *virtual World,* salah satunya adalah melalui internet. Perbuatan melawan hukum dalam dunia maya sangat tidak mudah untuk diatasi dengan mengandalkan hukum positif konvensional. Indonesia saat ini sudah merefleksikan diri dengan negara-negara lain seperti Malaysia, Singapura, India, atau negara-negara maju seperti Amerika Serikat, dan negara-negara Uni Eropa yang secara serius mengintegrasikan regulasi Hukum Siber ke dalam instrumen hukum positif nasionalnya.

Cyber Law atau disebut juga Hukum Siber adalah hukum yang mengatur tentang kejahatan dunia maya, yang secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi yang tidak bertanggung jawab. Sebutan Hukum Siber di beberapa negara lain adalah *Law of Information Technology, Virtual World Law* dan *Hukum Mayantara.* Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi yang tidak bertanggung jawab yang berbasis virtual atau maya.

Istilah Hukum Siber 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", sesuatu yang tidak terlihat atau semu.

III. METODE PENELITIAN

Untuk melaksanakan penelitian penulis memfokuskan pada lokasi di Reskrimum Polda Sultra selanjutnya akan mengumpilkan beberapa Data-data yang akan penulis lakukan untuk menjawab permasalahan yang penulis angkat dalam skripsi tersebut. Jenis data yang digunakan adalah primer dan sekunder yang berasal dari field research dan Library research. Teknik pengumpulan data yang digunakan adalah wawancara dan dokumentasi dan menganalisis secara kualitatif.

IV. HASIL PENELITIAN DAN PEMBAHASAN

A. Kendala-Kendala Yuridis Yang Dihadapi Oleh Perangkat Hukum Di Indonesia Dalam Menangani Para Pelaku Cyber Crime Terkait Dengan Masalah Pembuktian

1. Kejahatan Dan Kemajuan Dunia Teknologi

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai *(user)* atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.

Pada tahun 1982 telah terjadi penggelapan uang di bank melalui komputer sebagaimana dapat dilihat dalam Putusan Mahkamah Agung Nomor 363 K/Pid11984 tanggal 25 Juni 1984 mengenai. "Suara Pembaharuan" edisi 10 Januari 1991 memberitakan tentang dua orang mahasiswa yang membobol uang dari sebuah bank swasta di Jakarta sebanyak Rp. 372.100.000,00 dengan menggunakan sarana komputer. Perkembangan lebih lanjut dari teknologi komputer adalah berupa *computer network* yang kemudian melahirkan suatu ruang komunikasi dan informasi global yang dikenal dengan internet. Penggunaan teknologi komputer, telekomunikasi, dan informasi tersebut mendorong berkembangnya transaksi melalui internet di dunia.

2. Hubungan Antara Kejahatan, Cyber Crime Dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Cyher Crime adalah merupakan suatu perbuatan melanggar hukum yang secara khusus di diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Karena KUHP tidak cukup kuat untuk menj erat pelaku *cyber crime,* mengingat masalah pengaturan alat bukti yang tercantum dalam KUHP dan KUHAP belum memasukan alat bukti digital yang merupakan alat bukti dalam cyber crime di dalamnya.

Dalam pasal 27 - 37 Undang-undang ITE adalah merupakan perbuatan yang berkaitan dengan Informasi Dan Transaksi Elektronik yang dilarang oleh undang-undang tersebut. Berkaitan dengan hal tersebut pembuktiannya diatur dalam Bab X tentang Penyidikan, khususnya pasa143 ayat 5e : *"melakukan pemeriksaan terhadap alai dan/atau sarana yang berkaitan dengan kegiatan Teknologi Inforrnasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang undang ini "*

3. Dunia Sebelum Berlakunya Hukum Kejahatan *Cyber Crime*

Jauh sebelum adanya komputer dan kejahatan komputer, ada banyak bentuk pelanggaran dan kejahatan. Teknologi komputer dapat digunakan sebagai fasilitas para pelaku kejahatan komputer seperti pencurian dan penggelapan. Kejahatan komputer saat ini dicirikan dengan manipulasi otorisasi user program komputer, sebagai contoh, mencuri uang dari bank dan dari para pengusaha lainnya. Kejahatan komputer fase awal diantaranya adalab penyerangan sistem telephone dan network atau pentransferan uang menggunakan perangkat elektronik. Karena komputer pada awalnya terpusat dan tidak interkoneksi, peluang terjadinya kejahatan komputer lebih terbatas berupa penyalahgunaan sistem otorisasi user.

Sebelum adanya hukum kejahatan komputer, para pelaku dan hakim apabila berurusan

dengan kejahatan komputer akan menggunakan konsep hukum criminal tindakan pencurian, perusakan properti, penyalahgunaan dan kejahatan kriminal. Pada waktu itu, komputer masih berukuran besar, *standalone* mesin, dan akses ke computer tersebut secara umum terbatas oleh terminal fisik yang berhubungan dengan computer *mainframe.* Kebanyakan kejahatan komputer dilakukan oleh orang dalam atau dekat dengan orang dalam. Pengguna komputer yang memiliki legitimasi dengan hak akses ke komputer tersebut, seperti pengembang perangkat lunak, vendor dan pengguna lainnya yang memiliki otorisasi adalah para pelaku utama kejahatan-kejahatan komputer ini, yang meliputi kejahatan pencurian data oleh karyawan, informasi dan "properti" lainnya yang ada di komputer. Bentuk penyalahgunaan komputer lainnya meliputi perusakan perangkat lunak, perangkat keras atau data dalam komputer tersebut, umumnya kejahatan komputer juga terjadi karena adanya balas dendam terhadap pemecatan karyawan atau akibat dari perselisihan terhadap persetujuan lisensi perangkat lunak.

Penyalahgunaan komputer pada awalnya masih kecil, kejadian atau peristiwa yang terpencil. Tipe kejahatan yang melibatkan karyawan seperti cyberspace. Ketika seorang karyawan melihat file atau informasi rahasia lainnya, atau mencuri barang dari seorang karyawan, aktivitas-aktivitas demikian juga berlaku dalam *cyberspace.*

Harus ada pembedaan mengenai apa yang dimaksud tidak etis dan apa yang dimaksud ilegal; respon hukum terhadap suatu masalah harus proporsional terhadap aktivitas yang dilakukan. Hanya jika kebiasaan tersebut diputuskan benar-benar merupakan kriminalitas dan perbuatan kriminal yang dilarang serta penuntutan yang harus dilakukan. Hukum kriminal, oleh karenanya, harus dilakukan dan diimplementasikan dengan pengendalian.

Sejarah telah menunjukkan bahwa kejahatan komputer dilakukan oleh masyarakat luas seperti: para Siswa, amatiran, teroris dan anggota kelompok kejahatan yang terorganisir. Yang membedakannya adalah kejahatan yang dilakukannya. Individu yang melakukan akses sistem komputer tanpa maksud berbuat kejahatan lebih jauh harus dibedakan dari karyawan lembaga keuangan yang mengambil atau mentransfer uang dari akun pelanggan.

Level keahlian tertentu untuk kejahatan komputer merupakan sebuah topik yang kontroversial. Beberapa mengklaim bahwa level keahlian bukan sebuah indikator kejahatan komputer, sedangkan yang lain mengklaim bahwa kejahatan komputer yang jelas potensial, merupakan subjek yang sangat termotivasi untuk menerima tantangan perubahan teknologi, karakteristik yang juga diinginkan seorang karyawan dalam wilayah pemrosesan data.

Banyak survey pemerintah dan sektor swasta menunjukkan bahwa kejahatan komputer cenderung bertambah. Sulit untuk menghitung dampak ekonomis kejahatan ini, bagaimanapun, karena banyak yang tidak pernah dideteksi atau dilaporkan. Kejahatan komputer dapat dibagi menjadi dua kategori, yakni kejahatan terhadap komputer dan kejahatan menggunakan komputer.

4. Kendala-Kendala Dalam Menangani Para Pelaku Cyber Crime

Walaupun Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah disahkan oleh pemerintah, namun belum cukup mencakup semua aspek dari kejahatan dunia maya. *Drug Trafficker,* transaksi Narkoba melalui jaringan internet masih diatur dengan menggunakan Undang-Undang No. 5 Tahun 1997 tentang Psikotropika dan Undang-Undang Nornor 22 Tahun 1997 tentang Narkotika, sedangkan dalam undang-undang tersebut tidak diatur mengenai transaksi obat-obatan terlarang tersebut jika di lakukan menggunakan jaringan internet.

Selain itu, *Credit Card Fraud (Carding)* dan *Bank Fraud,* juga masih menggunakan peraturan hukum yang konvensional mengenai penipuan, yaitu Pasal 378 KUHP. Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Inforniasi Transaksi Elektronik belum diatur tentang masalah penipuan ini, mengingat sebenarnya kejahatan ini merupakan kejahatan yang dilakukan dengan menggunakan Media Informasi dan fasilitas Transaksi Elektronik yang disediakan pada jaringan internet.

B. Upaya-Upaya Yuridis Yang Dapat Dilakukan Terkait Dengan Masalah Pembuktian Oleh Perangkat Hukum Di Indonesia

Dalam upaya-upaya yang dapat dilakukan terkait dengan masalah pembuktian oleh pengadilan dan penyidikan oleh POLRI dalam *cyber crime* dapat digunakan berbagai macam cara, antara lain dengan mengoptimalkan UndangUndang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, mengembangkan pengetahuan dan kemampuan penyidik dalam Dunia Cyber, menambahkan dan meningkatkan fasilitas komputer forensik dalam POLRI.

Kejahatan internet atau yang lebih populer dengan istilah *cyher crime* ini dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dan korban kejahatan. Dengan sifat seperti itu, semua negara termasuk Indonesia yang melakukan aktivitas internet akan terkena imbas dari perkembangan kejahatan dunia maya.
Para *hacker* selalu mencari celah untuk menggunakan keahliannya melakukan kejahatan. Memudarnya batas-batas geografi dalam abad 21 yang dikenal sebagai abad informasi ini telah mengubah cara pandang terhadap penyelesaian dan praktik kejahatan dari model lama (konvensional) ke model baru (elektronik). Kekuatan jaringan dan komputer pribadi berbasis pentium menjadikan setiap komputer sebagai alat yang potensial bagi para pelaku kejahatan.

Globalisasi aktivitas kriminal yang memungkinkan para penjahat melintas batas elektronik merupakan masalah nyata dengan potensi memengaruhi negara, hukum, dan warga negaranya. Fakta ini tak bisa dimungkiri karena internet dapat dijadikan sarana yang efektif untuk mencapai tujuan-tujuan negatif yang diinginkan tanpa batasan geografis dan teritorial.

1. Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Dalam pasal 5 ayat 1 dan 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik mendeskripsikan bahwa Dokumen elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain dalam pasal 44 Undang-undang yang sama mengatakan: "Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. Alat bukti sebagaimana dimaksud dalam ketentuan Perundangundangan; dan
b. Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal I angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3). "

Selain deskripsi undang-undang ITE tersebut, dikenal pula alat bukti digital. Tindakan kejahatan tradisional umumnya meninggalkan bukti kejahatan berupa bukti-bukti fisikal, karena proses dan hasil kejahatan ini biasanya juga berhubungan dengan benda berwujud nyata. Dalam dunia komputer dan internet, tindakan kejahatan juga akan melalui proses yang sama. Proses kejahatan yang dilakukan tersangka terhadap korbannya juga akan mengandalkan bantuan aspek pendukung dan juga akan saling melakukan pertukaran atribut.

Namun dalam kasus ini aspek pendukung, media, dan atribut khas para pelakunya adalah semua yang berhubungan dengan sistem komputerisasi dan komunikasi digital. Atribut-atribut khas serta identitas dalam sebuah proses kejahatan dalam dunia komputer dan internet inilah

yang disebut dengan bukti-bukti digital.

Perangkat yang menggunakan format data digital untuk menyimpan informasi memang sangat banyak. Meskipun dalam artikel ini cakupannya hanya seputar perangkat komputer dan jaringan saja, namun perangkatperangkat lain juga memiliki potensi untuk menyimpan buktibukti digital. Seperti misalnya perangkat ponsel, smart card, bahkan microwave juga bisa berperan sebagai sumber bukti bukti digital. Berdasarkan pertimbangan inilah maka dibuat tiga kategori besar untuk sumber bukti digital, yaitu:

a. Open Computer Systems

Perangkat-perangkat yang masuk dalam kategori jenis ini adalah apa yang kebanyakan orang pikir sebagai perangkat komputer. Sistem yang memiliki media penyimpanan, keyboard, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, desktop, server, dan perangkatperangkat sejenis lain. Perangkat yang memiliki sistem media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi. Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut di akses, dan informasi lainnya semua merupakan informasi penting.

b. Communication Systems

Sistem telepon tradisional, komunikasi wireless, Internet, jaringan komunikasi data, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini. Sebagai contoh, jaringan Internet membawa pesan-pesan dari seluruh dunia melalui e-mail. Kapan waktu pengiriman e-mail ini, siapa yang mengirimnya, melalui mana si pengirim mengirim, apa isi dari e-mail tersebut merupakan bukti digital yang amat sangat penting dalam investigasi.

c. *Embedded Computer Systems*

Perangkat telepon bergerak (ponsel), personal digital assistant (PDA), smart card, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini. Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini. Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul-modul diagnosa yang dipasang dapatmenyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang amat berguna.

2. Penegakan Hukum Cyber Crime Dengan Menggunakan Sarana Non Penal

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan oleh Barda nawawi Arief sebagai berikut :

a. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;
b. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana control social yang tidak mungkin mengatasi masalah kejahatan scbagai masalah kemanusiaan dan kemayarakatan yang sangat kompleks (sebagai masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya);
c. Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan "kurierenam symptom", oleh karena itu hukum pidana hanya merupakan "pengobatan simptomatik" dan bukan "pengobatan kausatif';

d. Sanksi hukum pidana merupakan "remedium" yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif;
e. Sistem pemidanaan bersifat fragmentair dan individual/personal, tidak bersifat struktural fungsional;

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu, pencegahan kejahatan tidak selalu harus menggunakan hukum pidana. Agar penegakan hukum cyber crime ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Dalam konteks cyber crime ini erat hubungannya dengan teknologi, khususnya teknologi computer dan telekomunikasi sehingga pencegahan cyber crime dapat digunakan melalui saluran teknologi atau disebut juga techno-prevention. Langkah ini sesuai dengan apa yang telah diungkapkan oleh International Information Industri Congress (IIIC) sebagai berikut : *The UIC recognizes that government action and international treaties to harmonize laws and coordinate legal procedures are keying the fight cyber crime, but warns that these should not be relied upon as the only instrument. Cyber crime is enabled by technology and requires as healthy reliance on technology for its solution.*

Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau cultural ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan atau mengajarkan etika penggunaan computer melalui media pendidikan. Pentingnya pendekatan budaya ini, khususnya upaya mengembangkan kode etik dan perilaku (code of behavior and ethics) terungkap juga dalam pernyataan IIIC sebagai berikut :

III C members are also committed to participate in the development of code behaviour and ethics around computer and Internet use, and in campaigns for the need for ethical and responsible online behaviour Given the international reach of Internet crime, computer and Internet users around the world must be made aware of the need for high standards of conduct in cyber space.

C. Pengaturan Cyber Crime dalam Hukum Positif Indonesia

Pengaturan mengenai *Cyber Crime* yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer berdasarkan kebijakan hukum pidana adalah :

1. Illegal Access (akses secara tidak sah terhadap sistem komputer)

Yaitu dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak balk lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain. *Hacking* merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi. Perbuatan melakukan akses secara tidak sah terhadap sistem komputer belum ada diatur secara jelas di dalam sistem perundang-undangan di Indonesia. Untuk sementara waktu, Pasal 22 Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi dapat diterapkan. Pasal 22 UndangUndang Nomor 36 Tahun 1999 Tentang Telekomunikasi menyatakan: "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 50 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan Pasal 22 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah). Namun setelah Undangundang Informasi dan Transaksi Elektronik diundangkan, pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi sudah tidak perlu digunakan lagi. Karena pasal 30 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sudah mampu menjerat pelaku.

Dalam pasal 30 Undang-undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi elektronik disebutkan, bahwa "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem Elektronik Milik orang lain (ayat 1) dengan cara apa pun, (ayat 2) dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (ayat 3) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

Ketentuan pidana pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik diatur dalam pasal 46 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. untuk ayat 1, ketentuan pidananya yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah). Sedangkan ayat 2 pasal 46 memberikan ketentuan pidana penjara paling lama 7 (tujuh) tahun dan/atau pidana denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah). Untuk ayat 3, ketentuan pidananya adalah pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

b. Data Interference (mengganggu data komputer)

Yaitu dengan sengaja melakukan perbuatan merusak, menghapus, memerosotkan *(deterioration),* mengubah atau menyembunyikan *(suppression)* data komputer tanpa hak. Perbuatan menyebarkan virus komputer merupakan salah satu dari jenis kejahatan ini yang sering terjadi.

Pasal 38 Undang-Undang Telekomunikasi belum dapat menjangkau perbuatan *data interference* maupun *system interference* yang dikenal di dalam *cyber crime.* Jika perbuatan *data interference* dan *system interference* tersebut mengakibatkan kerusakan pada komputer, maka Pasal 406 ayat I KUHP dapat diterapkan terhadap perbuatan tersebut.

Pasal 32 ayat I Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik berbunyi :*"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menamhah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menvembunvikan suatu informasi elektronik dan/atau dokumen elektroraikmilik orang lain atau milik puhlik. "*

Isi dari pasal tersebut di atas dapat digunakan untuk menjerat pelaku kejahatan tersebut, karena unsur-unsur pidananya telah terpenuhi. Ketentuan Pidananya diatur dalam pasal 28 ayat 1 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yaitu pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

c. System Interference (mengganggu sistem komputer)

Yaitu dengan sengaja dan tanpa hak melakukan gangguan terhadap fungsi sistem komputer dengan cara memasukkan, memancarkan, merusak, menghapus, memerosotkan, mengubah, atau menyembunyikan data komputer. Perbuatan menyebarkan program virus komputer dan *E-mail bombings* (surat elektronik berantai) merupakan bagian dari jenis kejahatan ini yang sangat sering terjadi.

Pasal 38 Undang-Undang Telekomunikasi belum dapat menjangkau perbuatan *data interference* maupun *system interference* yang dikenal di dalam *cyber crime.* Jika perbuatan *data interference* dan *system interference* tersebut mengakibatkan kerusakan pada komputer, maka Pasal 406 ayat (1) KUHP dapat diterapkan terhadap perbuatan tersebut. Namun tidak demikian apabila yang rusak hanya sistem atau data dari komputer tersebut. Untuk kerusakan pada sistem, dasar hukumnya diatur dalam pasal 33 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang mengakihatkan sistam elektronik menjadi tidak bekerja sebagaimana mestinva. "*

Kemudian untuk ketentuan pidananya diatur dalam pasal 49 Undang-undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi elektronik, yaitu pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak 10.000.000,000,00 (sepuluh miliar rupiah).

d. Illegal Interception In The Computers, Systems And Computer Networks Operation

(intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer) Yaitu dengan sengaja melakukan intersepsi tanpa hak, dengan menggunakan peralatan teknik, terhadap data komputer, sistem komputer, dan atau jaringan operasional komputer yang bukan diperuntukkan bagi kalangan umum, dari atau melalui sistem komputer, tennasuk didalamnya gelombang elektromagnetik yang dipancarkan dari suatu sistem komputer yang membawa sejumlah data. Perbuatan dilakukan dengan maksud tidak baik, atau berkaitan dengan suatu sistem komputer yang dihubungkan dengan sistem komputer lainnya. Pasal 31 ayat 1 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah mengatur permasalahan sebagai berikut :*"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. "*

Sedangkan untuk ketentuak pidananya ada pada pasal 47 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, sebagai berikut : *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 31 ayat (1) dan ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800. 000.000,00 (delapan ratus juta rupiah). "*

e. Data Theft (mencuri data)

Yaitu kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. *Identity theft* merupakan salah satu dari jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan *(fraud).* Kejahatan ini juga sering diikuti dengan kejahatan *data leakage.*

Perbuatan melakukan pencurian data sampai saat ini tidak ada diatur secara khusus, bahkan di Amerika Serikat sekalipun. Pada kenyataannya, perbuatan *Illegal access* yang mendahului perbuatan *data theft* yang dilarang, atau jika *data theftss* diikuti dengan kejahatan lainnya, barulah ia menjadi suatu kejahatan bentuk lainnya, misalnya *data leakage and espionage* dan

identity theft and fraud.

Pencurian data merupakan suatu perbuatan yang telah mengganggu hak pribadi seseorang, terutama jika si pemiik data tidak menghendaki ada orang lain yang mengambil atau bahkan sekedar membaca datanya tersebut. Pasal 32 ayat 2 Undangundang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dapat digunakan untuk menjerat pelaku. *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkcrn atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak ",* dapat dipidana dengan ketentuan pidana sebagaimana diatur dalam pasal 48 ayat 2, yaitu pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp. 3.000.000.000,00 (tiga miliar rupiah).

f. Data Leakage And Espionage (membocorkan data dan memata-matai)

Yaitu kegiatan memata-matai dan atau membocorkan data rahasia baik berupa rahasia negara, rahasia perusahaan, atau data lainnya yang tidak diperuntukkan bagi utnum, kepada orang lain, suatu badan atau perusahaan lain, atau negara asing." Karena Undang-undang Informasi Dan Transaksi elektronik belum rnencakup perbuatan tersebut, maka sementara perbuatan membocorkan dan memata-matai data atau informasi yang berisi tentang rahasia negara diatur di dalam Pasal 112, 113, 114, 115 dan 116 KUHP. Pasal 323 KUHP mengatur tentang pembukaan rahasia perusahaan yang dilakukan oleh orang dalam *(insider).* Sedangkan perbuatan membocorkan data rahasia perusahaan dann memata-matai yang dilakukan oleh orang luar perusahaan dapat dikenakan Pasal 50 jo. Pasal 22, Pasal 51 jo. Pasal 29 ayat (1), dan Pasal 57 jo. Pasal 42 ayat (1) UndangUndang Nomor 36 tahun 1999 Tentang Telekomunikasi.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

1. Asas legalitas dalam hukum pidana Indonesia memberikan garis kebijakan agar mewujudkan perlindungan hukurn terhadap tindakan sewenang-wenang penguasa/penyelenggara negara terhadap kepentingan hukum bagi masyarakat dan hak asasi manusia. Maka sistem pembuktian berdasarkan KUHAP secara formil tidak lagi dapat menjangkau dan sebagai landasan hukum pembuktian terhadap perkara *Cyber Crimes,* sebab 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. Oleh karena itu dibutuhkan optimalisasi Undang-undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
2. Kelemahan perangkat hukum dalam penegakan hukum pidana khususnya perkara *Cyher Crimes* banyak memiliki keterbatasan. Hatl demikian dapat dirasakan seperti apabila kejahatan yang terjadi aparat penegak hukumnya belum siap bahkan tidak mampu (gagap teknologi) untuk mengusut pelakunya dan alat-alat bukti yang dipergunakan dalam hubungannya dengan bentuk kejahatan ini sulit terdeksi. Kelemahan lain ada pada perangkat komputer forensik yang belum dimiliki oleh POLRI, mengingat penting keberadaannya dalam mencegah, maupun menangani kasus-kasus yang berkaitan dengan *Cyher Crime.*

B. Saran

Berdasarkan ternuan yang ada selama penelitian maka disarankan kepada para pengguna internet agar mematuhi norma - norma serta harus beretika baik ketika sedang menjelajahi dunia maya. Selain itu saran juga ditujukan kepada pihak yang berwenang dalam hal ini pemerintah Indonesia melalui Departemen Informasi dan Teknologi agar memenuhi kedua prasyarat dan meningkatkan kinerja dibawah ini yakni :

1. Pembentukan Konsep Kitab Undang-Undang Hukum Pidana Yang Baru Perlu adanya konsep KUHP yang baru dalam negara kita, karena perkembangan jaman akan menciptakan kejahatan-kejahatan yang baru pula, sedangkan KUHP lama negara kita sudah tidak layak lagi. Karena sudah tidak mencakup kejahatan-kejahatan baru yang muncul seiring dengan perkembangan jaman.
2. IDCERT (Indonesia Computer Emergency Response Team) Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah kcamanan in] di luar negeri mulai dikenali dengan munculnya *"sendmail worm"* (sekitar tahun 1988) yang menghentikan system email Internet kala itu. Kemudian dibentuk sebuah *Computer Emergency Response Team* (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi point of contact bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia. Selain itu sertifikasi perangkat keamanan sistem komputer dimana perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia. Di Korea hal ini ditangani oleh *Korea Information Security Agency.*

DAFTAR PUSTAKA

Abu Bakar Munir, *Cyber Law Policies and Challenges, 1999.*

Adami Chazawi, *Hukum Pembuktian Tindak Pidana Korupsi,* Bandung : PT Alumni, 2006.

Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Bssandung: PT Citra Aditya Bakti, 2002.

Ahmad M Ramli, *Prinsip prisnsip Cyber Law Dan kendala Hukum Positif Dafam Menanggulangi Cyber Crime,* Fakultas Hukum Universitas Padjajaran, Jakarta, Desember 2004.

Ahmad Suwandi dan B. Ryanto Setyo, *"Menabur entuh, Menuai Software Tangguh ", PC* Media 08/2004.

Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer,* Sinar Grafika, Jakarta, *1990.*

Bambang Sunggono, *Metodologi penelitian hukum,* Rajawali Press. Jakarta,2005.

Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana,* Bandung: PT Citra Aditya Bakti, 1998.

Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana,* Mandar Maju. Bandung. 2003

Laporan Akhir Penelitian, Kementrian Komunikasi Dan Informasi, Jakarta, November 2003.

Moch. Safar Hayim, *Mengenali Undang-undang Media Dan Siber,* Refika Aditama.2002.

Moeljatno, *Asas-asas Hukum Pidana.* Bina Aksara, Jakarta.

Peter Mahmud Marzuki, *Penelitian Hukum,* Jakarta : Prenada Media, 2005. Saifudin Aswar, *Metode Penelitian,* Pustaka Pelajar, Jakarta, 2003. *Sto, "Seni Internet Hacking Uncencored* ",Jasakom, 2004.

_____,*"Kajian Hukum Tentang Kejahatan Di Dunia Maya (Cyber Crime) ".*

_____, *"Naskah A kademik Rancangan Undang-undang Tentang Kejahatan Dunia Maya (Cyber Crime) ",* Seminar Hak Cipta dan Informai, Jakarta, Juni 2003

Lampiran

Garis-garis Besar Haluan Negara GBHN 1999-2004 TAP MPR NO. IV/ MPR/1999", 1999, Sinar Grafika, Jakarta.

Kejaksaan Republik Indonesia, 1998, "Himpunan Peraturan tentang Tugas Dan Wewenang Kejaksaaan", Buku II, diterbitkan oleh Kejaksaan Agung R.I., Jakarta.

Moeljatno, 1994, "Kitab Undang-undang Hukum Pidana", cetakan kesembilanbelas, Bumi Aksara, Jakarta.

Soenarto Soerodibroto, 2000, "KUHP dan KUHAP", Edisi keempat, cetakan kelima, PT RajaGrafindo Persada,Jakarta.

Undang-Undang Nomor 36 tahun 1999 Tentang Telekomunikasi, 2000, cetakan pertama, Sinar Grafika, Jakarta.

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE), Kementrian Komunikasi dan Informasi Republik Indonesia, 25 Maret 2008.