KAJIAN YURIDIS *CYBER CRIME* PENANGGULANGAN DAN PENEGAKAN HUKUMNYA[1]

Oleh : Indriani Berlian Mewengkang[2]
Robert N. Warong[3]
Michael Kuntag, SH,MH.

ABSTRAK

Tujuan dilakukannya peneleitian ini yaitu untuk mengetahui bagaimana pengaturan tentang *Cyber crime* sebagai upaya penanggulangan kejahatan dibidang teknologi computer dan bagaimanakah bentuk penegakan pelaku tindak pidana *Cyber crime* dalam penggunaan computer di mana dengan metode penelitian hukum normatif disimpulkan: 1. Penanggulangan terhadap *Cyber crime* telah dilakukan dengan diundangkannya Undang-Undang No. 11 Tahun 2008 tentang Transaksi Teknologi. Dengan diundangkannya undang-undang tersebut diharapkan setiap bentuk kejahatan *Cyber crime* akan ditindak sesuai dengan aturan dalam undang-undang tersebut di samping Kitab Undang-Undang Hukum Pidana (KUHP) yang mengatur tentang berbagai modus tindak pidana. Dengan diundangkannya Undang-Undang No. 11 Tahun 2008, maka sikap tegas dan jelas bahwa *Cyber crime* adalah tindak pidana yang dilarang oleh undang-undang dan setiap pelaku akan ditindak menurut undang-undang yang berlaku. 2. Penegakan hukum terhadap pelaku dilakukan melalui proses pertanggungjawaban pidana *Cyber crime* yang dilakukan oleh pelaku dengan menggunakan komputer dan internet. Pertanggungjawaban pidana oleh pelaku dilakukan sesuai dengan prosedur Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Transaksi Elektronik. Untuk prosedur penegakan hukum dilakukan menurut Kitab Undang-Undang Hukum Acara Pidana sesuai dengan Undang-Undang No. 8 Tahun 1981 karena pelanggaran *Cyber crime* akan dituntut secara formil dalam Kitab Undang-Undang Hukum Acara Pidana sebagai bentuk penegakan hukum bagi pelaku untuk mempertanggungjawabkan perbuatan pidana *Cyber crime*.

Kata kunci: cyber crime;

PENDAHULUAN

A. Latar Belakang Masalah

Dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan 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. Hal ini 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).

B. Rumusan Masalah

1. Bagaimana pengaturan tentang *Cyber crime* sebagai upaya penanggulangan kejahatan dibidang teknologi komputer?
2. Bagaimanakah bentuk penegakan pelaku tindak pidana *Cyber crime* dalam penggunaan komputer?

C. Metode Penelitian

Metode penelitian kepustakaan *(Library Research)* yakni suatu metode yang digunakan dengan jalan mempelajari buku literature, perundang-undangan dan bahan-bahan tertulis lainnya.

PEMBAHASAN

A. Penanggulangan *Cyber crime* Sebagai Tindak Pidana

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

[1] Artikel Skripsi
[2] Mahasiswa pada Fakultas Hukum Unrsat, NIM. 17071101365
[3] Fakultas Hu

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).

Pengaturan tentang kejahatan pada umumnya termuat dalam Kitab Undang-Undang Hukum Pidana KUHP. Dalam KUHP pada prinsipnya kejahatan penggunaan komputer atau *Cyber* merupakan tindak pidana pada umumnya. Walaupun belum diatur secara khusus, pelaku kejahatan *Cyber* adalah pelaku tindak pidana. Pemikiran demikian telah sesuai dengan asas legalitas dalam hukum pidana (KUHP) 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". Pelaku *Cyber crime* telah melakukan tindak pidana pada umumnya, apalagi sesudah ditetapkannya Undang-Undang No 11 Tahun 2008.

Bertolak dari prinsip diatas maka jelas bila dikaitkan dengan *Cyber crime,* dengan berlakunya Undang-undang Nomor 11 Tahun 2008 merupakan perbuatan pidana. Dalam proses hukum untuk menetapkan pelaku *Cyber crime* sebagai pelaku tindak pidana maka unsur membuktikan dengan kekuatan alat bukti menjadi hal yang paling penting. Dalam hukum acara pidana KUHAP penetapan alat bukti yang cukup merupakan masalah yang tidak kalah pentingnya untuk diantisipasi di samping unsur kesalahan dan adanya perbuatan pidana. Pentingnya persoalan pembuktian dalam proses litigasi *Cyber crime,* merupakan unsur utama dalam menetapkan tersangka sebagai pelaku tindak pidana *Cyber crime.*

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik merupakan dasar hukum pengaturan tentang kejahatan dalam teknologi informasi disebut dengan *Cyber crime*. *Cyber crime* adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi dan komunikasi tanpa batas, serta memiliki sebuah karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan tingkat keamanan yang tinggi, dari sebuah informasi yang disampaikan dan diakses oleh pengguna internet.[4]

Dalam Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang ITE telah dijelaskan bahwa "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"[5].

Di Indonesia banyak kasus yang berkaitan dengan kejahatan dunia maya (*Cybercrime*). Maskun menyatakan, dalam praktik di Indonesia, tindak pidana dengan menggunakan komputer sejak dahulu merupakan jenis kejahatan yang sulit untuk diklasifikasikan sebagai tindak pidana[6]. *Cyber crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu :

a. Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer
   1. *Illegal access* (akses secara tidak sah terhadap sistem komputer)
   2. *Data interference* (mengganggu data komputer)
   3. *System interference* (mengganggu sistem komputer)
   4. *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)
   5. *Data Theft* (mencuri data)
   6. *Data leakage and espionage* (membocorkan data dan memata-matai)
   7. *Misuse of devices* (menyalahgunakan peralatan komputer)
b. Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan
   1. *Credit card fraud* (penipuan kartu kredit)
   2. *Bank fraud* (penipuan terhadap bank)

[4]Agus Tri P.H. *Cyber Crime dalam Perspektif Hukum Pidana*, Skripsi, UMS, Surakarta, 2010, hlm. 10.

[5] Undang-Undang Transaksi Elektronik Nomor 11 Tahun 2008

[6] Maskun, *Kejahatan Siber Cyber Crime*, Kencana Prenada Media Group, Jakarta, 2013, hlm. 62.

3. *Service Offered fraud* (penipuan melalui penawaran suatu jasa)
4. *Identity Theft and fraud* (pencurian identitas dan penipuan)
5. *Computer-related fraud* (penipuan melalui komputer)
6. *Computer-related forgery* (pemalsuan melalui komputer)
7. *Computer-related betting* (perjudian melalui komputer)
8. *Computer-related Extortion and Threats* (pemerasan dan pengancaman melalui komputer)

c. Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem komputer
   1. *Child pornography* (pornografi anak)
   2. *Infringements Of Copyright and Related Rights* (pelanggaran terhadap hak cipta dan hak-hak terkait)
   3. *Drug Traffickers* (peredaran narkoba), dan lain-lain.

Kegiatan *Cyber* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata dalam transaksi dan aplikasi. Secara yuridis dalam hal ruang *Cyber* 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 teknologi computer 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.

Hukum pada prinsipnya harus mengantisipasi kecepatan perkembangan teknologi informasi dan internet. 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.

Pengaturan hukum di bidang teknologi harus bisa mengikuti kecepatan perkembangan kemajuan teknologi tersebut, justru akan mendorong timbulnya kejahatan-kejahatan 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. Landasan pemikiran inilah yang mendasari lahirnya.

Tindak pidana penggunaan komputer dan internet *Cybercrimes* dalam arti sempit (*computer crimes)* dilakukan dengan berbagai modus Bentuk-bentuk modus kejahatan dalam *Cyber crime* di bagi menjadi: a. Akses ilegal *(illegal access*) b. Intersepsi ilegal (*illegal interception*) c. Gangguan terhadap data (data *interference*) d. Gangguan terhadap sistem (*system interference*) e. Penyalahgunaan alat dan perangkat (*miscue of device)* Tindak pidana yang terkait dengan komputer (*computer related offences*). Tindak-tindak pidana ini merupakan ruang lingkup *Cyber*crimes dalam arti luas (*computer related crimes*). Tindak pidana yang dimaksud terdiri dari: a. Pemalsuan dengan penggunaan komputer (*computer related forgery*) b. Penipuan dengan penggunaan komputer *(computer related fraud*) c. Tindak pidana yang terkait dengan konten (*content-related offences*). Tindak pidana *Cyber crime* banyak juga terkait dengan yang terkait dengan pelanggaran hak cipta dan hak yang terkait pelanggaran tersebut merupakan pelanggaran yang sangat sering terjadi di internet, Tindak pidana percobaan (*attempt*) dan pembantuan (*aiding or abetting*).

Pembatasan Pertanggungjawaban Pidana Terkait dengan ketentuan pembantuan dalam tindak pidana *Cyber*, *Convention on Cybercrime* memberikan batasan pertanggungjawaban terhadap penyelenggara jasa yang terlibat dalam transmisi atau komunikasi elektronik. Misalnya, meskipun transmisi konten *malicious code* memerlukan keterlibatan penyelenggara jasa, mereka yang tidak memiliki tujuan untuk melakukan tindak pidana tersebut tidak dapat dimintai pertanggungjawaban secara pidana atas perbuatan yang terjadi melalui layanannya. Oleh karena itu, tidak ada kewajiban bagi penyelenggara jasa untuk memonitor konten secara terus menerus dalam rangka menghindari pertanggung jawaban pidana berdasarkan ketentuan ini.

Pengaturan Prosedural Mengingat *Convention on Cybercrime* merupakan konvensi regional untuk negara-negara anggota Council of Europe meskipun dapat diterapkan oleh negara-negara lain yang mengaksesi atau meratifikasi konvensi yang dimaksud, dalam konvensi ini diatur hukum acara pidana yang harus diterapkan oleh negara anggota dalam peraturan perundang-undangan untuk menciptakan keseragaman pengaturan.

Kemampuan penyidik untuk menemukan unsur-unsur kejahatan komputer sangat penting minimal penyidik mempunyai pengetahuan dan kemampuan di bidang komputer dan teknologi informasi lainya. Aspek lain mencakup kewenangan prosedur dalam menangani: 1. Penyidikan tindak pidana yang diatur dalam konvensi; 2. Penyidikan tindak pidana lain yang dilakukan dengan menggunakan sistem komputer; 3. Pengumpulan alat bukti elektronik.

Kerjasama Internasional Karakteristik tindak pidana *Cyber* yang lintas batas negara mengharuskan aparat penegak hukum untuk bekerjasama dengan aparat penegak hukum dari negara lainya.

Aspek lain kejahatan *Cyber crime* berskala global dan Internasional untuk itu dalam penyidikan bersifat luas memerlukan kerjasama dengan Negara lain atau Interpol. Untuk memfasilitasi kerjasama tersebut, *Convention on Cybercrime* mencantumkan pengaturan kerjasama internasional dalam bidang penyidikan maupun proses peradilan pidana lainya terkait dengan sistem komputer dan data komputer serta pengumpulan alat bukti elektronik. Secara umum, kerja sama yang dimaksud ialah dalam bidang ekstradisi dan dalam bidang bantuan timbal balik (*mutual assistance*).

Bukti yang memberi keterangan yaitu hanya sebagai saksi sehingga kemungkinan bagi korban untuk memperoleh keleluasaan dalam memperjuangkan haknya adalah kecil. Hukum pidana materil dan hukum pidana formal (KUHAP) lebih menitik beratkan perhatian pada pembuat korban (pelaku kejahatan) dari pada korban, seolah-olah terdapat suatu perbedaan atau pemisahan yang tajam antara si pembuat korban dengan si korban, walaupun keduanya memiliki peranan yang fungsional dalam terjadinya tindak pidana.

Dalam penegakan hukum pidana Nasional (baik KUHP maupun KUHAP) harus dilaksanakan sesuai dengan isi ketentuan hukum pidana nasional tersebut, yang telah diatur secara tegas tanpa memerhatikan kedudukan dan kepentingan korban, ternyata hingga sekarang hanyalah sebuah regulitas yang bersifat rutin namun tanpa makna ketika harus berhadapan dengan pentingnya perlindungan korban kejahatan, Jika hukum pidana nasional berlaku secara umum untuk seluruh wilayah Indonesia, muncul pertanyaan, berlaku untuk siapa ketentuan tersebut jika tidak memerhatikan kepentingan para korban kejahatan.

Semakin meluasnya *Cyber crime* dalam kehidupan masyarakat dalam bisnis dan transaksi perbankan dan perdagangan *online* memerlukan pengaturan untuk melindungi masyarakat agar tidak menjadi korban. Perlindungan hukum bagi masyarakat sangatlah penting karena masyarakat baik kelompok maupun perorangan, dapat menjadi korban atau bahkan sebagai pelaku kejahatan.

Perlindungan hukum korban kejahatan sebagai bagian dari perlindungan kepada masyarakat dapat diwujudkan dalam berbagai bentuk seperti melalui pemberian restitusi dan kompensasi, pelayanan medis, dan bantuan hukum. Dalam penanganan perkara pidana, kepentingan korban sudah saaatnya untuk diberikan perhatian khusus, selain sebagai saksi yang mengetahui terjadinya suatu kejahatan juga karena kedudukan korban sebagai subjek hukum yang memiliki kedudukan sederajat di depan hukum (*equality before the law*).

Perhatian kepada korban dalam penanganan perkara pidana hendaknya dilakukan atas dasar belas kasihan dan hormat atas martabat korban (*compassion and respect for their dignity*).

Kegiatan *Cyber* dengan penggunaan computer dalam kehidupan sehari hari 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 pada hakekatnya merupakan bagian dari suatu langkah kebijakan. Selanjutnya untuk menentukan bagaimana suatu 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.

B. Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cyber Crime*

Pelaku Tindak pidana *Cyber crime* akan dituntut pertanggungjawaban pidana sama dengan pelaku tindak pidana lainya sesuai KUHP dan UU ITE Nomor 11 Tahun 2008. Masalah Pertanggungjawaban Pidana *Cyber crime* Pertanggungjawaban pidana pada hakikatnya mengandung makna tuntutan pidana pembuat (subjek hukum) atas tindak pidana yang telah dilakukannya. Oleh karena itu, pertanggungjawaban pidana mengandung di dalamnya pencelaan objektif dan pencelaan subjektif. Artinya, secara objektif si pembuat telah melakukan tindak pidana (perbuatan terlarang/melawan hukum dan diancam pidana menurut hukum yang berlaku) dan secara subjektif si pembuat patut dicela atau dipersalahkan/ dipertanggungjawabkan atas tindak pidana yang dilakukannya itu sehingga ia patut dipidana.

Penegakan hukum terhadap seseorang yang telah melakukan perbuatan pidana tetapi tidak dapat dipertanggungjawabkan karena dalam Pasal 44 Kitab Undang-undang Hukum Pidana itu, maka tidaklah dipidana. Menurut Martiman Prodjohamidjojo seseorang mendapatkan pidana tergantung pada dua hal:

1. Harus ada perbuatan yang bertentangan dengan hukum, atau dengan kata lain: harus ada unsur melawan hukum. Jadi, ada unsur obyektif.
2. Terhadap pelakunya ada unsur kesalahan dalam bentuk kesengajaan atau kealpaan, sehingga perbuatan yang melanggar hukum dapat dipertanggungjawabkan kepadanya. Jadi unsur subjektif.[7]

Subyek hukum sebagai pelaku tindak pidana *Cyber crime* selalu dilihat dari kemampuan bertanggungjawab. Istilah pertanggungjawaban pidana terdiri dan dua kata yakni pertanggungjawaban dan pidana. Pertanggungjawaban berasal dan kata dasar tanggung jawab. Menurut W.J.S. Poerwadarminta "tanggung jawab diartikan sebagai: keadaan wajib menanggung segala sesuatunya kalau ada sesuatu hal boleh dituntut, dipersalahkan, diperkarakan dan sebagainya".[8]

S.R. Sianturi mengatakan bahwa: Dalam bahasa asing pertanggungjawaban pidana disebut sebagai *toerekenbaarheid, criminal responsibility, criminal liability.* Diutarakan bahwa pertanggungjawaban pidana dimaksudkan untuk menentukan apakah seseorang tersangka/terdakwa dipertanggungjawabkan atas suatu tindak pidana *(crime)* yang terjadi atau tidak.[9]

Dengan perkataan lain apakah pelaku akan dipidana atau dibebaskan. Jika pelaku dipidana, harus ternyata bahwa tindakan yang dilakukan itu bersifat melawan hukum dan terdakwa mampu bertanggung jawab. Kemampuan tersebut memperlihatkan kesalahan dari petindak yang berbentuk kesengajaan atau kealpaan. Atau dengan kata lain tindakan tersebut tercela dan pelaku menyadari tindakan yang dilakukan tersebut.

Dalam hukum pidana seseorang tidak mungkin dipertanggungjawabkan atau dijatuhi pidana, meskipun dia melakukan tindak pidana,

7 Martiman Prodjohamidjojo, *Memahami Dasar-dasar Hukum Pidana Indonesia II,* Pradnya Paramita, Jakarta, 1996. hlm. 36.

8 W.J.S. Poerwadarminta, *Kamus Umum Bahasa Indonesia,* Balai Pustaka, Jakarta, 1976, hlm. 1014.

9 S.R. Sianturi, *Op.Cit.* hlm. 250.

kalau orang itu tidak mempunyai kesalahan. Pertanyaan yang timbul ialah kapan orang mempunyai kesalahan? Kesalahan merupakan masalah pertanggungjawaban pidana.

Roeslan Saleh mengatakan bahwa "seseorang mempunyai kesalahan apabila pada waktu melakukan perbuatan pidana terlihat dari segi masyarakat dia dapat dicela oleh karenanya, sebab dianggap dapat berbuat lain jika memang tidak ingin berbuat demikian".[10] Dilihat dari segi masyarakat ini menunjukan pandangan yang normatif mengenai kesalahan. Seperti diketahui mengenai kesalahan ini dulu orang berpandangan *psychologisch.* Demikian misalnya pandangan dari pembentuk WvS. Tetapi kemudian pandangan ini ditinggalkan orang dan orang lalu berpandangan normatif.

Ada atau tidaknya kesalahan tidaklah ditentukan bagaimana dalam keadaan senjatanya batin daripada terdakwa, tetapi bergantung pada bagaimanakah penilaian hukum mengenai keadaan batinnya itu, apakah dipernilai ada ataukah tidak ada kesalahan.

Jadi yang harus diperhatikan adalah: keadaan batin dari orang yang melakukan perbuatan itu; dan hubungan antara keadaan batin itu dengan perbuatan yang dilakukan, menurut rumusannya Simons sedemikian rupa, sehingga orang itu dapat dicela karena perbuatan tadi. Dua hal yang harus diperhatikan itulah terjalin erat satu dengan lainnya merupakan hal yang dinamakan kesalahan, masalah kemampuan bertanggungjawab; hal yang kedua, yaitu mengenai hubungan antara batin itu dengan perbuatan yang dilakukan, merupakan masalah kesengajaan, kealpaan serta alasan pemaaf; sehingga mampu bertanggungjawab, mempunyai kesengajaan atau kealpaan serta tidak adanya alasan pemaaf merupakan unsur-unsur dari kesalahan.

Pertanggungjawaban hukum terkait dengan bukti elektronik kejahatan *cyber crime* yang dilakukan oleh pelaku. Pasal 1 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menyatakan dalam Undang-Undang ini yang dimaksud dengan :

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange (EDI),* surat elektronik *(electronic mail),* telegram, perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.
3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

Informasi ialah: (1) hasil olahan yang dilakukan baik secara manual atau komputer atau (2) data yang sudah diproses yang diperlukan pimpinan sebagai "bahan untuk mengambil keputusan.[11] Komputer ialah: (1) mesin penghitung dan pengolah data yang bekerja atas instruksi dan data yang di kode dalam bentuk biner (2) alat elektronik berkemampuan tinggi untuk melakukan perhitungan dan operasi yang logis serta menyimpan dan melaksanakan sederetan instruksi tanpa campur tangan manusia.[12]

Pasal 1 ayat (14) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menyebutkan Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan. Dikenalnya Internet yang kemudian diikuti disusul dengan munculnya *World Wide Web* (WWW) yaitu sistem informasi tersebar berbasis teks tingkat tinggi *(hypertext)* dengan kemampuan menampilkan beragam bentuk/gaya teks berikut gambar grafis, atau membuat, menyunting dan melihat dokumen *hypertext,* maka secara tidak langsung masing-masing pengguna Internet saling berinteraksi satu sama lain menciptakan suatu hubungan sosial. Hubungan ini pada akhirnya menciptakan

10 Roeslan Saleh, *Perbuatan Pidana dan Pertanggungjawaban Pidana, Dua Pengertian Dasar Dalam Hukum Pidana,* Aksara Baru, Jakarta, 1983, hlm. 75.

11 Saydam Gouzali, *Kamus Istilah Telekomunikasi,* Djambatan, 1992, hlm. 152.

12 *Ibid*, hlm. 183

suatu bentuk kehidupan masyarakat di dunia maya, atau di kenal dengan *Cyber community.*

Kemajuan teknologi informasi tersebut antara lain ditandai dengan maraknya penggunaan media elektronik mulai dari penggunaan *handphone* hingga komputer yang semakin canggih. Penggunaan media elektronik yang menyangkut teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa dan atau menyebarkan informasi merupakan hal yang sudah lazim dilakukan seseorang di zaman modern ini.

Kemajuan teknologi menyebabkan kemudahan seseorang untuk dapat mengakses apa saja yang dibutuhkan baik mengenai informasi, transaksi, dan banyak hal lagi lainnya. Pemanfaatan teknologi informasi telah banyak mengubah perilaku manusia. Perkembangan penggunaan alat komunikasi secara elektronik memiliki keuntungan antara lain efisiensi, kecepatan dan kemudahan dalam melakukan kegiatan, namun muncul kekhawatiran ketika alat komunikasi secara elektronik akan disalahgunakan untuk keuntungan pribadi dan merugikan orang lain. Untuk mengatasi penyalahgunaan penggunaan media elektronik, pendekatan hukum sangat diperlukan guna memperoleh kepastian hukum. Pendekatan hukum juga diperlukan untuk menangani kasus-kasus yang berkaitan dengan bukti elektronik, antara lain pencemaran nama baik, pembunuhan yang terekam CCTV, penipuan dalam transaksi bisnis.

Untuk menyelesaikan kasus dengan media elektronik aparat penegak hukum masih sering menghadapi permasalahan dalam pembuktian. Permasalahan dalam pembuktian ini terjadi karena pembuktian menggunakan bukti elektronik pada persidangan perkara pidana umum masih menjadi hal yang diperdebatkan mengenai keabsahannya.

Sebagaimana dapat kita ketahui bahwa mengenai informasi elektronik merupakan hal baru dalam hukum pidana di Indonesia. Dalam hukum acara pidana di Indonesia yaitu Undang-undang Nomor 8 Tahun 1981 tidak mengenal informasi elektronik sebagai alat bukti yang sah. Dalam gunakan informasi dan elektronik, pada tahun 2008 telah diterbitkan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Keberadaan Undang-undang ini memberikan pengakuan terhadap alat bukti elektronik.

Pembuktian pada Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sendiri bersifat *Lex Specialis* dari KUHAP karena mengatur keberlakuan pembuktian tindak pidana di dunia maya. Berkaitan dengan tujuan dari hukum acara pidana adalah mencari kebenaran materiil maka proses pembuktian merupakan suatu tahap yang sangat menentukan bagi hakim untuk memperoleh keyakinan untuk menjatuhkan putusan. Mengacu pada kelima alat bukti yang ditentukan dalam Pasal 184 KUHAP sebagaimana diuraikan sebelumnya, maka munculah suatu pertanyaan masuk kelompok manakah alat bukti elektronik itu.

Mengingat surat elektronik dan dokumen elektronik pada intinya merupakan data yang dituangkan dalam bentuk elektronik yang belum diatur dalam KUHAP, maka untuk menentukan apakah surat elektronik dan dokumen elektronik masuk ke dalam kategori alat bukti berupa surat merupakan suatu hal yang tidak mudah.

Sistem pembuktian yang dianut dalam hukum acara pidana Indonesia adalah sistem pembuktian berdasarkan Undang-undang secara negatif atau *Negatief Wettelijke,* yaitu hakim dapat menjatuhkan hukuman pidana berdasarkan dua alat bukti yang sah menurut Undang-undang dan berdasarkan kedua alat bukti tersebut hakim memperoleh keyakinan bersalah atau tidaknya terdakwa. Hakim tidak boleh menggunakan alat bukti selain yang diatur dalam Undang-undang.

Dewasa ini informasi elektronik telah dapat dijadikan sebagai alat bukti pada kasus-kasus yang bersifat khusus, sebagaimana Undang-undang telah mengaturnya sebagai alat bukti yang sah seperti dalam kasus tindak pidana Korupsi (Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi yang telah diperbarui pada Undang-undang Nomor 20 Tahun 2001 Tentang Perubahan Undang-undang Nomor 31 Tahun 1999) yang dalam Pasal 26 A menyatakan bahwa, alat bukti yang sah dalam bentuk petunjuk sebagaimana diatur dalam Pasal 188 ayat (2) KUHAP, khusus untuk tindak pidana korupsi juga dapat diperoleh dari :

1. alat bukti lain berupa informasi lain yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa.
2. dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca atau didengar yang dapat dikeluarkan dengan tanpa bantuan suatu sarana baik yang tertuang dalam kertas, benda fisik apapun selain kertas.

Di dalam Undang-undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang yang mengatur tentang alat bukti yang berupa informasi elektronik sebagai berikut, dokumen adalah data rekaman yang dapat dilihat, dibaca, didengar dan dikeluarkan dan atau dengan bantuan sarana baik yang tertuang diatas kertas, benda fisik selain kertas atau yang terekam secara elektronik termasuk tetapi tidak terbatas pada:

1. tulisan, suara, atau gambar
2. peta, rancangan, foto,
3. huruf, tanda, angka, simbol, atau dapat dipahami oleh orang yang mampu memahaminya.

Dalam Peraturan Pemerintah Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme yang kemudian telah ditetapkan menjadi Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Pemerintah Pengganti Undang-Undang yang pada Pasal 27 menyebutkan bahwa alat bukti pemeriksaan terorisme meliputi:

1. alat bukti sebagaimana yang disebutkan dalam Pasal 184 KUHAP
2. alat bukti lain berupa informasi lain yang diucapkan, dikirimkan, diterima atau disimpan secara elektronik dengan alat bukti atau yang serupa dengan itu
3. data, rekaman atau informasi yang dapat dilihat, dibaca atau didengar baik yang tertuang diatas kertas, benda fisik selain kertas, yang terekam secara elektronik tetapi tidak terbatas pada 1. Tulisan, suara, atau gambar; 2. Peta, rancangan, foto atau sejenisnya 3. Huruf, tanda, angka, simbol yang memiliki makna atau dapat dipahami oleh orang yang mampu memahaminya.

Selanjutnya data elektronik sebagai alat bukti dapat juga ditemukan dalam Undang-undang Nomor 10 Tahun 1995 Tentang Kepabeanan yang telah diubah dengan Undang-undang Nomor 17 Tahun 2006 Tentang Perubahan Atas Undang-undang Kepabean.

Pihak lain yang mendukung tanggung jawab kriminal korporasi berfokus pada sulitnya mengidentifikasi individu tertentu yang akan disalahkan.[13] Perilaku kriminal agregat, bukanlah individual, yang tidak etis, atau tidak bertanggung jawab harus dicegah. Lebih lanjut kebijakan korporasi, daripada keputusan individu, mungkin akan menghasilkan pelanggaran. Hanya dengan membuat korporasi bertanggung jawab maka perilaku kriminal dalam korporasi dapat dikendalikan.

Adapun kesalahan dapat berupa kesengajaan atau kealpaan. Dengan diterimanya korporasi sebagai subjek hukum pidana, maka timbal permasalahan yang menyangkut pertanggungjawaban pidana korporasi dalam hukum pidana, yaitu apakah badan hukum (korporasi) dapat mempunyai kesalahan, baik berupa kesengajaan atau kealpaan. Karena sangat sukar untuk menentukan ada atau tidak adanya kesalahan pada korporasi, ternyata dalam perkembangannya khususnya yang menyangkut pertanggungjawaban pidana korporasi dikenal adanya "pandangan baru" atau katakanlah pandangan yang berlainan, bahwa khususnya untuk pertanggungjawaban dari badan hukum (korporasi), asas kesalahan tidak berlaku mutlak, sehingga pertanggungjawaban pidana yang mengacu pada doktrin *strict liability* dan *vicarious liability* yang pada prinsipnya merupakan penyimpangan dari asas kesalahan, hendaknya dapat menjadi bahan pertimbangan dalam penerapan tanggung jawab korporasi dalam hukum pidana.

Cyber crime berada di lingkungan elektronik dan dunia maya yang sulit diidentifikasikan secara pasti, sedangkan asas legalitas konvensional bertolak dari perbuatan riel dan kepastian hukum. *Cyber crime* berkaitan erat dengan perkembangan teknologi canggih yang sangat cepat berubah sedangkan asas legalitas konvensional bertolak dari sumber hukum formal (UU) yang statis. *Cyber crime* melampui batas-batas negara, sedangkan perundang-undangan suatu negara pada

[13] *Ibid*., hlm. 283

dasarnya/umummnya hanya berlaku di wilayah teritorialnya sendiri.

Menghadapi kondisi demikian, seyogyanya ada keberanian dan inovasi dari aparat penegak hukum untuk mengefektifkan peraturan yang ada dengan melakukan interprestasi atau konstruksi hukum yang bersumber pada teori/ ilmu hukum, pendapat para ahli, yurisprudensi, atau bersumber dari ide-ide dasar yang secara konseptual dapat dipertanggungjawabkan Seperti telah dikemukakan di atas, pertanggungjawaban pidana juga mengandung makna pencelaan subjektif. Artinya, secara subjektif si pembuat patut dicela atau dipersalahkan/dipertanggung jawabkan atas tindak pidana yang dilakukannya itu sehingga ia patut dipidana.[14] Secara singkat sering dinyatakan kesalahan (dikenal dengan asas culpabilitas). Asas culpabilitas ini pun tentunya juga harus diperhatikan dalam masalah pertanggungjawaban *Cyber crime*, walaupun mungkin menghadapi tantangan tersendiri dalam kasus-kasus *Cyber crime* karena tidak mudah membuktikan adanya unsur kesalahan (dolus/culpa) dalam masalah *Cyber crime*.

Keterkaitan Kitab Undang-Undang Hukum Pidana Dengan Hukum *Cyber* Tabel 1 Keterkaitan Kitab Undang-Undang Hukum Pidana Dengan Hukum *Cyber* No Subjek/Materi Muatan/Pasal Keterkaitan Dengan Hukum Siber Tentang Pencurian. Pasal 362 Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam dengan pidana penjara paling lama lima tahun atau denda paling banyak enam tahun. Ketentuan tentang pencurian harus diperluas mencakup pula pencurian melalui sarana elektronik dengan mengedepankan delik formil. Hal ini perlu diharmonisasikan dengan RUU ITE.

Tentang pemerasan dan pengancaman Pasal 369 (1). Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancaman pencemaran nama baik dengan lisan maupun tulisan, dengan ancaman akan membuka rahasia, memaksa seorang supaya memberikan barang sesuatu yang seluruhnya atau sebagian kepunyaan orang itu atau orang lain atau supaya memberi hutang atau menghapuskan piutang, diancam Hal ini juga harus.

[14] Barda Nawawi Arif, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia*. PT Raja Grafindo Persada. Jakarta. 2005, hlm. 33

PENUTUP

A. Kesimpulan

1. Penanggulangan terhadap *Cyber crime* telah dilakukan dengan diundangkannya Undang-Undang No. 11 Tahun 2008 tentang Transaksi Teknologi. Dengan diundangkannya undang-undang tersebut diharapkan setiap bentuk kejahatan *Cyber crime* akan ditindak sesuai dengan aturan dalam undang-undang tersebut di samping Kitab Undang-Undang Hukum Pidana (KUHP) yang mengatur tentang berbagai modus tindak pidana. Dengan diundangkannya Undang-Undang No. 11 Tahun 2008, maka sikap tegas dan jelas bahwa *Cyber crime* adalah tindak pidana yang dilarang oleh undang-undang dan setiap pelaku akan ditindak menurut undang-undang yang berlaku.
2. Penegakan hukum terhadap pelaku dilakukan melalui proses pertanggungjawaban pidana *Cyber crime* yang dilakukan oleh pelaku dengan menggunakan komputer dan internet. Pertanggungjawaban pidana oleh pelaku dilakukan sesuai dengan prosedur Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Transaksi Elektronik. Untuk prosedur penegakan hukum dilakukan menurut Kitab Undang-Undang Hukum Acara Pidana sesuai dengan Undang-Undang No. 8 Tahun 1981 karena pelanggaran *Cyber crime* akan dituntut secara formil dalam Kitab Undang-Undang Hukum Acara Pidana sebagai bentuk penegakan hukum bagi pelaku untuk mempertanggungjawabkan perbuatan pidana *Cyber crime*.

B. Saran

1. Penanggulangan terhadap *Cyber crime* telah diatur dalam Undang-Undang No. 11 Tahun 2008. Berbagai Modus *Cyber crime* sebagai kejahatan komputer harus terungkap dalam proses penyidikan Untuk itu diperlukan penyidik yang

professional uang menguasai teknologi computer dan internet agar hasil penyidikan Diperlukan aturan khusus yang memberikan kewenangan kepada penyidik untuk mengungkap kejahatan elektronik begitu juga dalam mengumpulkan alat bukti elektronik

2. Penegakan hukum harus dilakukan lewat prosedur pertanggungjawaban pidana dalam Kitab Undang-Undang Hukum Acara Pidana harus lebih tegas supaya pelaku tidak berdalih bahwa kejahatan tersebut tidak dilakukan dengan sengaja. Tindak pidana *Cyber crime* sama dengan tindak pidana lain harus dipertegas dalam sistem penegakan hukum.

DAFTAR PUSTAKA

BUKU

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara*, Refika Aditama, Bandung, 2010.

Anwar H.A.K. Moch., *"Hukum Pidana Bagian Khusus"* Jilid 2, Alumni, Bandung, 1981.

Berkowitz, L. *Agresi 1 Sebab dan Akibatnya.*Alih Bahasa: Hartatni Woro Susiatni. Pustaka Binaman Pressindo. Jakarta, 1995.

Brigham, J. C. *Social Psychology.Second Edition.* Happer Collins Publisher, Inc. New York, 1991.

Buss, Arnold H. *Psychology : Behavior in Perspective. Second Edition. New* York : John Wiley & Sons. 1978.

Bassar M. Sudrajat, *Tindak-tindak Pidana Tertentu Di Dalam Kitab Undang-Undang Hukum Pidana,* Remaja Karya, Bandung, 1988.

Bemmelen J.M. van, *Hukum Pidana 3 Bagian Khusus Delik-Delik Khusus,* Bina Cipta Bandung, 1986.

Hamzah Audi, *Asas-Asas Hukum Pidana,* Rineka Cipta, Jakarta, 1994.

Kartanegara Satochid, *Hukum Pidana I,* Balai Lektur Mahasiswa, Jakarta, Tanpa Tahun.

Lamintang P.A.F. dan C. Djisman Samosir, *Hukum Pidana Indonesia,* Sinar Baru, Bandung, 1985.

Gosita, Arif. *Masalah Korban Kejahatan.* Akademika Persindo, Jakarta ,1993.

Hamzah, Andi. *Hukum Acara Pidana Indonesia.* Sinar Grafika, Jakarta , 2008.

Koeswara, E. *Agresi Manusia.* PT Eresco, Bandung , 1988.

Poerwadarminta, W. J. S. *Kamus Besar Bahasa Indonesia, Departemen Pendidikan dan Kebudayaan.* Balai Pustaka, Jakarta, 1997.

Prodjodikoro, Wiryono. *Hukum Acara Pidana di Indonesia.* Sumur, Bandung, 1962.

Prodjodikoro, Wirjono. *Asas-Asas Hukum Pidana Di Indonesia.* Refika Aditama, Bandung, 2008.

Raven, B. dan Rubin, J. Z. *Social Psychology.* Toronto: John Wiley & Sons, 1983.

Sutan RemyS yahdeini, *Kejahatan Dan Tindak Pidana Komputer*, PT Pustaka Utama Grafiti, Jakarta, 2009.

Semin, G. & Fiedler, K. *Applied Social Psychology.* SAGE Publications Ltd, London, 1996.