ANALISIS YURIDIS TENTANG PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU *CYBER CRIME*

Abdul Rahim Wahab /Faris Ali Sidqi /M. Yusran bin Darham

UNIVERSITAS ISLAM KALIMANTAN (UNISKA)
Email: abdulrhm.whb@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengetahui ketentuan hukum tentang tindak pidana cyber crime di Indonesia dan untuk mengetahui bentuk pertanggungjawaban pidana terhadap pelaku cyber crime. Jenis penelitian dalam penulisan skripsi ini dilakukan dengan jenis penelitian hukum normatif berupa penelitian kepustakaan yang menggunakan 3 bahan hukum yaitu bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Penelitian hukum ini menitikberatkan pada studi kepustakaan yang berarti akan lebih banyak menelaah dan mengkaji aturan-aturan hukum yang ada dan berlaku. Hasil penelitian menunjukan Ketentuan hukum mengatur tindak pidana cyber crime Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik merupakan bentuk dari perubahan Undangundang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun terkait dengan bentuk-bentuk dari tindak pidana cyber crime yang diatur tidak ada perubahan, sehingga segala bentuk tindak pidana cyber crime masih sama halnya dengan yang diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bentuk- bentuk tindak pidana cyber crime yang tercantum dalam psl 27 sampai dengan psl 35 UU No11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Tanggung jawab pidana Cybercrime dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik 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.

Kata kunci : *Pertanggungjawaban Pidana, Pelaku, Cyber Crime*

ABSTRACT

This study aims to determine the legal provisions regarding cyber crime in Indonesia and to determine the form of criminal liability against cyber crime

perpetrators. The type of research in writing this thesis is carried out with normative legal research in the form of library research using 3 legal materials, namely primary legal materials, secondary legal materials and tertiary legal materials. This legal research focuses on the study of literature, which means it will study more and examine the existing and applicable legal rules. The results of the study show that the legal provisions governing cyber crime, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions is a form of amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. However, regarding the forms of cyber crime that are regulated there is no change, so that all forms of cyber crime are still the same as those regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions. Law Number 11 of 2008 concerning Information and Electronic Transactions regulates forms of cyber crime as listed in Articles 27 to 35 of Law No. 11 of 2008 concerning Electronic Information and Transactions. Cybercrime criminal responsibility in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions is regulated in 9 articles, from article 27 to article 35. In these 9 articles, 20 forms or types of criminal acts are formulated ITE. Article 36 does not formulate certain forms of ITE criminal acts, but formulates the basis for criminal aggravation which is placed on the consequences of harming others in criminal acts as regulated in Article 27 to Article 34. Meanwhile, the criminal threat is determined in Article 45 to Article 52.

Keywords: *Criminal Liability, Perpetrators, Cyber Crime*

PENDAHULUAN

Globalisasi telah menjadi pendorong lahirnya era perkembangan teknologi informasi.Fenomena kecepatan perkembangan teknologi informasi ini telah merebak di seluruh belahan dunia.Tidak hanya negara maju saja, namun negara berkembang juga telah memacu perkembangan teknologi informasi pada masyarakatnya masing-masing, sehingga teknologi informasi mendapat kedudukan yang penting bagi sebuah kemajuan bangsa.Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi (*information technology)* memegang peran penting, baik di masa kini maupun di masa mendatang.[1] Perkembangan yang pesat dalam teknologi internet

[1] Agus Rahardjo, *Cybercrime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, (*Bandung: Citra Aditya Bakti, 2002), hal. 1.

menyebabkan kejahatan baru di bidang itu juga muncul, misalnya kejahatan manipulasi data, *spionase, sabotase, provokasi, money laundry, hacking,* pencurian *software* maupun perusakan *hardware* dan berbagai macam lainnya

Kejahatan *cyber crime* dibagi menjadi 2 kategori, yakni *cyber crime* dalam pengertian sempit dan dalam pengertian luas. *cyber crime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan *cyber crime* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.[2]

Istilah–istilah yang tetap digunakan tersebut tetap diarahkan pada pengertian kejahatan terhadap komputer *(Crime directed at computer),* kejahatan dengan mendayagunakan komputer *(Crimes utilizing computers),* atau kejahatan yang berkaitan dengan komputer *(Crimes related to computer),* walaupun istilah-istilah tersebut belum memberikan gambaran–gambaran yang tepat. Meskipun demikian, istilah apapun yang digunakan, berbagai pihak telah berusaha membuat definisinya sendiri–sendiri berdasarkan pemahamannya.[3] Dalam hal ini terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace,* per tama adalah pendekatan teknologi, ke-dua pendekatan sosial budaya-etika, dan ke-tiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, atau diakses secara ilegal dan tanpa hak.

Melihat fakta hukum sebagaimana yang ada pada saat ini, 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

[2] Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: Rajawali Pers, hal 25.

[3] *Ibid*

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).

METODE PENELITIAN

Dalam melakukan suatu penelitian ilmiah jelas harus menggunakan metode sebagai ciri khas keilmuan. Metode mengandung makna sebagai cara mencari informasi dengan terencana dan sistimatis. Langkah-langkah yang diambil harus jelas serta ada batasan-batasan yang tegas guna menghindari terjadinya penafsiran yang terlalu luas.[4]

1. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian hukum normatif, yaitu penelitian yang berfokus pada norma dan penelitian ini memerlukan bahan hukum sebagai data utama.

2. Sifat Penelitian

Sedangkan sifat penelitian yang penulis pergunakan adalah penelitian yang bersifat deskriktif *analitis* dalam pengertian semua bahan hukum yang penulis dapatkan akan digambarkan dan diuraikan kemudian dianalisa.

3. Bahan Hukum

a. Bahan hukum primer, yaitu bahan hukum yang mem punyai kekuatan mengikat, yaitu berupa peraturan perundang-undangan sepertii:[5]
   1) Undang-Undang Dasar Negara Republik Indonesia 1945;
   2) Kitab Undang-Undang Hukum Pidana;
   3) KUHAP

b. Bahan hukum sekunder adalah yang memberikan penjelasan terhadap bahan hukum primer, meliputi buku, hasil penelitian,

[4] Soerjono Soekanto dan Sri Mamudi, 1986, P*enelitian Hukum Normatif,* (Jakarta: CV. Rajawali), hal. 27

[5]Bambang Sunggono, *Metodologi Peneliti an Hukum*, (Jakarta: PT. Raja Grafindo Persada, 2003), hal. 116

pendapat hukum, dokumen-dokumen lain yang ada relefansinya dengan masalah yang diteliti.

c. Bahan hukum tersier adalah bahan hukum penunjang yang memberikan petunjuk dan pengertian terhadap bahan hukum primer dan sekunder, meliputi kamus-kamus hukum atau kamus bahasa lain.

4. Teknik Pengumpulan Bahan Hukum.

Untuk menjawab permasalahan yang ada Peneliti melakukan pengumpulan bahan hukum melalui studi dokumen (studi kepustakaan) meliputi bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier yakni dengan cara melakukan inventarisasi dan identifikasi terhadap sejumlah peraturan perundang-undangan, dokumen hukum, catatan hukum, hasil-hasil karya ilmiah dan bahan bacaan/literatur yang berasal dari ilmu pengetahuan hukum dalam bentuk buku, artikel, jurnal dan hasil penelitian yang ada kaitannya dengan penelitian yang diangkat.

PEMBAHASAN

A. Ketentuan Hukum Tentang Tindak Pidana *Cyber Crime* Di Indonesia

Tidak dapat dipungkiri, perkembangan ilmu pengetahuan diikuti oleh teknologi. Perkembangan teknologi dimanfaatkan untuk mendorong pertumbuhan bisnis yang begitu pesat. Informasi tersajikan dalam waktu yang begitu cepat. Hanya dengan memanfaatkan teknologi komunikasi, bisnis antar negara dapat dilakukan tanpa perlu bertemu *face to face.*[6] Inilah tanda bahwa era *cyber* dalam bisnis telah dimulai. Selain menguntungkan pelaku bisnis, perkembangan teknologi juga memudahkan untuk mendapatkan informasi, dan berdampak juga terhadap sector ekonomi, politik, budaya serta hukum suatu negara.

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan,

[6] Niniek Suparni, *Cyberspace Problematika & Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009, hlm. 1.

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. [7]

Seiring dengan perkembangan teknologi internet, kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan tercepat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia bisa diketahui selama 24 jam. Melalui dunia internet, apapun dapat dilakukan. Segi positif dunia maya ini tentu saja menambah *trend* perkembangan teknologi dunia sebagai segala bentuk kreatifitas manusia.[8]

Kemajuan teknologi sangat berdampak besar bagi masyarakat yang membawa dampak positif dan dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E Sahetapy telah menyatakan, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Maka demikian artinya semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya.[9]

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan

[7] A. Rahmah dan Amiruddin Pabbu, *Kapita Selekta Hukum Pidana*, Mitra Wacana Media, Jakarta, 2015, hlm. 1.

[8] Edmon Makarim, *Pengantar Hukum Telematika*, Rajagrafindo Perkasa, Jakarta, 2005, hlm. 31.

[9] J. E Sahetapy dalam Abdul Wahid, 2002, *Kriminologi dan Kejahatan Kontemporer*,

Lembaga Penerbitan Fakultas Hukum Unisma, Malang

tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang memiliki ciri-ciri tersendiri sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya mulai dari penyelidikan, penyidikan hingga dengan penuntutan.[10]

Sehingga berdasarkan beberapa pendapat tersebut maka dapat dikatakan bahwa adanya kemajuan teknologi dan informasi selain dapat dipergunakan manusia sebagai komoditi informasi, juga dapat membawa dampak negatif yakni penyalahgunaan teknologi yang membawa hal tersebut pada suatu tindak pidana yang disebut dengan *cyber crime*. Adapun tindak pidana cyber crime ini memiliki karakteristik tersendiri karena berhubungan dengan jaringan teknologi komputer sehingga dalam penangannya tidak dapat disamakan dengan tindak pidana konvensional.

Cybercrime merupakan kejahatan yang berbeda dengan kejaharan konvensional (*street crime*). *Cyber crime* 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. Penyimpangan social menyesuasikan bentuk dn karakter baru dalam kejahatan.[11]

B. Bentuk Pertanggungjawaban Pidana Terhadap Pelaku *Cyber Crime*

Pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat, dan berkembang dalam tatanan kehidupan baru dan mendorong terjadinya perubahan sosial, ekonomi, budaya, pertahanan dan keamanan. Pesatnya perkembangan teknologi informasi menjadikan sebuah fenomena kehidupan yang

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

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

menarik, dimana masyarakat pengguna teknologi informasi dalam berkomunikasi tidak lagi dibatasi oleh waktu dan tempat *(borderless).* Kapan pun dan dimana pun masyarakat pengguna perangkat teknologi tersebut bisa menjalin komunikasi, mendapatkan informasi, dan menyebarkan informasi kepada orang lain. Globalisasi teknologi tersebut menempatkan masyarakat Indonesia sebagai bagian dari masyarakat dunia pengguna teknologi komunikasi dan informasi.[12]

Teknologi informasi dan komunikasi saat ini sedang mengarah kepada konvergensi yang memudahkan kegiatan manusia sebagai pencipta, pengembang dan pengguna teknologi itu sendiri. Salah satunya dapat dilihat dari perkembangan media internet yang sangat pesat. Internet sebagai suatu media dan komunikasi elektronik telah banyak dimanfaatkan untuk berbagai kegiatan, antara lain untuk menjelajah *(browsing,surfing)*, mencari berita, saling mengirim pesan melalui *email,* dan perdagangan.[13]

Kemajuan dibidang ilmu pengetahuan dan teknologi telekomunikasi dan informatika juga turut mendukung perluasan ruang gerak transaksi barang dan/atau jasa hingga melintas batas-batas wilayah suatu Negara. Teknologi informasi dan media elektronik dinilai sebagai symbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial budaya, ekonomi dan keuangan. Dari sistemsistem kecil lokal dan nasional, proses globalisasi dalam tahun-tahun terakhir bergerak cepat, bahkan terlalu cepat menuju suatu sistem global.[14]Manfaat dari perkembangan teknologi dapat dirasakan dalam berbagai bidang, seperti: Didalam bidang kesehatan,

[12] Lihat konsiderans Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[13] Ahmad M Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, (Bandung : Refika Aditama, 2004), hlm. 1

[14] Didik J Rachbini*, Mitos dan Implikasi Globalisasi: Catatan Untuk Bidang Ekonomi dan Keuangan, Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, Globalisasi adalah Mitos,* Yayasan Obor, Jakarta, 2001,Hlm.2.

kecanggihan teknologi informasi juga bisa ditemukan dalam bentuk pencitraan visual. Seperti sinar-X yang bisa digunakan untuk mendiagnosa penyakit atau gangguan yang terdapat di dalam tubuh manusia.

Pemanfaatan laboratorium sebagai pusat analisa dan pengembangan pengobatan terbaru juga sangat membutuhkan teknologi informasi ini. Manfaat teknologi informasi juga berdampak besar pada dunia perbankan. Sebelumnya manusia menggunakan celengan saat ingin menyimpan uang, lama kelamaan banyak bermunculan perusahaan-perusahaan perbankan baik milik pemerintah maupun swasta yang menawarkan keamanan dan keuntungan dalam menabung atau menyimpan uang. Awalnya dilakukan dengan cara penyetoran dan pengambilan uang hanya bisa dilakukan langsung di kantor pada jam kerja. Namun sekarang bisa rasakan sendiri banyak perubahan yang memudahkan dalam aktivitas perputaran uang ini. Tidak perlu lagi mengantri saat ingin mengambil atau melakukan penyetoran uang, tinggal hanya menggunakan Anjungan Tunai Mandiri (ATM) sudah dapat melakukan hal tersebut.

Akan tetapi dibalik manfaat dari perkembangan teknologi informasi dan komunikasi, timbul kejahatan yang dinamakan *Cyber Crime*. Kejahatan ini juga tidak mengenal batas wilayah *(borderless)*, ruang, tempat serta waktu kejadian karena korban dan pelaku sering berada di Negara yang berbeda. Barda Nawawi Arief mengemukakan *Cyber Crime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian masyarakat luas di dunia internasional, juga merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh kehidupan modern saat ini.[15]

Maraknya *Cyber Crime* yang terjadi yang membuat masyarakat dirugikan secara materi maka masyarakat harus dilindungi agar mendapatkan rasa kenyamanan.

---

[15] Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Raja Grafindo Persada, 2006), hlm 26

Lahirnya Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, selanjutnya disebut dengan Undang-Undang ITE, memang tidak dapat dilepaskan dari semangat zaman yang bersifat globalisasi tentang tuntutan perlunya perlindungan hukum bagi pengguna teknologi informasi, yang dipandang sebagai kelompok yang paling rentan terhadap tindak pidana salah satunya adalah perbuatan yang menyebabkan terganggunya sistem elektronik.

Berdasarkan beberapa literatur serta praktiknya, *cybercrim*e memiliki beberapakarakteristik, yaitu: 1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah *cyber (cyberspace),* sehingga
tidak dapat dipastikan yuridiksi Negara mana yang berlaku terhadapnya. 2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet. 3. Perbuatan tersebut mengakibatkan kerugian materil maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, dan kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. 5. Perbuatan tersebut sering dilakukan secara transional/melintasi batas Negara.[16]

Disahkannya Undang-Undang ITE, merupakan suatu pemikiran yang komprehensif dari Negara dengan *political will* untuk memperhatikan dan memberikan perlindungan hukum bagi pengguna teknologi informasi. Tentunya perlindungan hukum ini, tidak hanya kepada pengguna teknologi informasi yang digunakan secara positif, tetapi bagaimana undang-undang ini dapat mencegah dan mengungkap segala bentuk kejahatan yang menggunakan sarana teknologi informasi dan komunikasi salah satunya seperti perbuatan yang mengakibatkan terganggunya sistem elektronik dengan cara mengirimkan virus melalui link yang sudah di buat dan mengakibatkan kerusakan pada

[16] Budi Suhariyanto*, Tindak Pidana Teknologi Informasi (cybercrime)*, (Jakarta: Raja Grafindo Persada, 2013), hlm 14

elektronik yang digunakan untuk membuka link tersebut sehingga membuat elektronik tersebut tidak dapat dioperasikan sebagaimana mestinya.

PENUTUP

A. Kesimpulan

1. Ketentuan hukum terkait tindak pidana *cyber crime*, telah diatur dalam Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur beberapa pasal yang memuat tentang perbuatan yang dilarang termasuk tindak pidana *cyber crime*. Undang-Undang Nomor 36 Thn 1999 tentang Telekomunikasi diberlakukan untuk mengakomodir pemidanaan dari tindak pidana cyber crime, sebelum lahirnya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun Undangundang Nomor 36 Tahun 1999 tentang Telekomunikasi 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 mengakomodir tindak-tindak pidana yang berkaitan dengan komputer. Bentuk-bentuk tindak pidana *cyber crime* yang disebutkan dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi adalah akses illegal. 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. Ketentuan hukum yang lain mengatur tindak pidana cyber crime Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan

Transaksi Elektronik merupakan bentuk dari perubahan Undangundang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun terkait dengan bentuk-bentuk dari tindak pidana cyber crime yang diatur tidak ada perubahan, sehingga segala bentuk tindak pidana cyber crime masih sama halnya dengan yang diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bentuk- bentuk tindak pidana *cyber crime* yang tercantum dalam psl 27 sampai dengan psl 35 UU No11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diantaranya 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.

2. Tanggung jawab pidana *Cybercrime* dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik 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. Berdasarkan Pasal 27 Undang-Undang ITE Tahun 2008 : "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. Ancaman pidana Pasal 45 ayat (1) KUHP. Pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah)". Pasal 28 Undang-Undang ITE Tahun 2008 : Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi Elektronik". Pasal 29 Undang-Undang ITE Tahun 2008 : "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 *(Cyber Stalking)*. Ancaman pidana Pasal 45 ayat (3), setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah)". Pasal 30 ayat (3) Undang-Undang ITE Tahun 2008 : "Setiap orang

dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan *(cracking, hacking, illegal access)*. Ancaman pidana Pasal 46 ayat (3), setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah)".

B. Saran

1. Ketentuan hukum tindak pidana cyber crime pada dasarnya sudah diatur dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik akan tetapi dalam aturan ini tidak spesifik dan khusus mengatur tentang tindak pidana cyber crime dan harapan kedepan bagi para pemangku kebijakan agar lebih khusus membentuk peraturan perundang-udangan terkait tindak pidana cyber crime
2. tanggung jaawab pidana terhadap pelaku cyber crime terdapat dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik akan tetapi kedepan adanya perubahan terkait dengan sanksi pidana terhadap pelaku tindak pidana cyber crime terkait dengan ancaman pidana yang harus di perkuat agar dapat membuat efek jera terhadap pelaku tindak pidana cyber crime.

DAFTAR PUSTAKA

Agus Rahardjo, *Cybercrime : Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi.* PT Citra

Aditya Bakti, Bandung, 2002

Andi Hamzah, *Bunga Rampai Hukum Pidana dan Acara Pidana*, Ghalia Indonesia, Jakarta, 1986

Ardiyana Riswanda, *Amandemen UUD 1945 Terbaru & Terlengkap,* Buku Pintar, Yogyakarta, 2014

Abdul Wahid, 2002, *Kriminologi dan Kejahatan Kontemporer*, LembagaPenerbitanFakultasHukumUnisma, Malang;

_____ dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cybercrime)*, RefikaAditama, Bandung;

Achmad Sodiki dalam Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cybercrime)*, Cetakan Kesatu, RefikaAditama, Bandung; Ade MamanSuherman, 2005, *Aspek Hukum Dalam Ekonomi Global*,

Ahmad M.Ramli, 2010, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung; Ghalia Indonesia, Bogor;

Barda Nawawi Arief, 1996, *Bunga Rampai Kebijakan Hukum Pidana*, Citra AdityaBakti, Bandung*;*

_____,2003, *Kapita Selekta Hukum Pidana*, Citra AdityaBakti, Bandung;

_____*,*2007,*Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* Kencana Prenada Media Group, Jakarta;

Bambang Sugono, *Metode Penelitian Hukum*, Grafindo Persada. Jakarata, 1997

CST Kansil, Christine S.T Kansil, Engelien R, Palandeng dan Godlieb N. Mamahit, *Kamus Istilah Hukum*, Jala Permata Aksara, Jakarta, 2009

Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi*, Refika Aditama, Bandung, 2010

David R. Johnson and David Post, *Law and Borders : The Rise of Law in Cyberspace,* 481 Stanford Law Review 1996

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi, Refika Aditama, Bandung, 2009* Djoko Prakoso. *Asas-Asas Hukum Pidana di Indonesia*. Edisi Pertama,

Liberty, Yogyakarta, 1987.

Gialdah Tapiansari Batubara, *Peranan Ilmu Ketuhanan Dalam Penegakan Hukum Pidana Di Indonesia*, Journal Law Reform Volume 8 No. 2, Program Studi Magister Ilmu Hukum Fakultas Hukum Universitas Diponegoro, Semarang, 2013

Gialdah Tapiansari Batubara, *Nilai Ketuhanan Sebagai Garda Pertama Unpas Dalam Menjalankan Perannya Menjaga Kebinekaan,* Media Unpas Al-Mizan, Bandung, 2017

Jan Remmelink, *Hukum Pidana: Komentar Atas Pasal-Pasal Terpenting dari Kitab Undang-Undang Hukum Pidana Belanda dan Pidananya dalam Kitab Undang-Undang Hukum Pidana Indonesia*, Gramedia Pustaka Utama, Jakarta

Maskun, *Kejahatan Siber (Cyber Crime) : Suatu Pengantar,* Kharisma Putra Utama, Jakarta, 2013

Mochtar Kusumaatmadja, *Masyarakat dan Pembinaan Hukum Nasional*, Bina Cipta, Bandung, 1986

Otje Salman dan Anthon F. Susanto, *Teori Hukum: Mengingat, Mengumpulkan, dan Membuka Kembali,* PT Refika Aditama, Bandung, 2013

Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, 1998

S.R.Sianturi, 1996, *Asas-asas Hukum Pidana Di Indonesia dan Penerapannya*, Alumni Ahaem-Petehaem, Jakarta;

Stephenson, Peter, *Investigating Computer Related Crime: A Hanbook For Corporate Investigators*, (London New York Washington D.C: CRC Press, 2000)

Soerjono Soekanto, 1986, *Pengantar Penelitian Hukum*, UI Press, Jakarta; W.Gulo, 2002, *Metode Penelitian*, GramediaWidiasarana Indonesia, Jakarta;

Widodo, 2009, *Sistem Pemidanaan dalam Cybercrime*, Laksbang Mediatama, Yogyakarta;

Warassih, Esmi, *Pranata Hukum Sebuah Telaah Sosilogis,* Universitas Diponegoro, Semarang, 2010