PEMBUKTIAN TERHADAP KEJAHATAN DUNIA MAYA DAN UPAYA MENGATASINYA MENURUT HUKUM POSITIF DI INDONESIA[1]

Oleh: Aan Andrew Johanes Pahajow[2]

ABSTRAK

Tujuan dilakukannya penelitian ini adalah untuk mengetahui apakah kendala yuridis dalam pembuktian kejahatan dunia maya (*cyber crime*) dan bagaimanakah upaya mengatasi tindak pidana *cyber crime* menurut hukum positif Indonesia, yang dengan menggunakan metode penelitian hukum normatif disimpulkan bahwa: 1. Undang-Undang ITE tidak mengatur secara khusus hal-hal yang menyangkut *cybercrime*, Pemerintah dalam membentuk Undang-Undang ITE ini masih menggunakan pendekatan politis-pragmatis, bukan menggunakan pendekatan kebijakan publik yang melibatkan lebih banyak kalangan. UU ITE ini lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, tidak lebih. Padahal siapapun tahu bahwa dunia siber (*cyberword*) lebih luas dari sekedar transaksi elektronik. Ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam Undang-Undang ITE seperti kelalaian atau khilaf. Undang-Undang ITE ini juga tidak mengatur kapan kadaluwarsa perbuatan pidana kejahatan hacking; 2. Penanggulangan *cyber crime* dapat merujuk pada beberapa instrumen hukum internasional, antara lain instrumen Palermo dan instumen Hongaria. Dimana substansinya dimungkinkan untuk diratifikasi dan diaksesi oleh Negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan mayantara atau *cyber crime*, dan mencakup kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari *cyber crime*, baik melalui Undang-Undang maupun kerjasama internasional. Optimalisasi UU ITE dapat mempermudah kepolisian dalam melakukan investigasi kejahatan *cyber crime*, khususnya dalam mengumpulkan alat bukti berdasarkan pasal 5 dan pasal 44 UU ITE. Pendekatan budaya atau cultural 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.

Kata kunci: pembuktian, kejahatan, dunia maya

PENDAHULUAN

A. Latar Belakang

Di Indonesia produk hukum yang dipakai untuk menanggulangi *cyber crime* yaitu UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, UU ITE berfungsi sebagai pedoman, norma dan kontrol terhadap perilaku para pengguna internet. Hal ini bertujuan untuk memprevensi, mendeteksi atau mereduksi kejahatan internet, kecurangan dan perilaku pengguna internet yang tidak etis, yang dilakukan melalui penggunaan teknologi informasi. Pedoman, norma dan fungsi kontrol tercermin pada ketentuan yang terdapat dalam bab dan pasal-pasal UU ITE 11/2008. Ketentuan ini mengacu pada upaya regulator untuk mengarahkan dan mengendalikan perilaku para pengguna internet serta meningkatkan kepatuhan para pengguna terhadap UU ITE 11/2008. Peningkatan kepatuhan para pengguna internet diharapkan mampu mereduksi terjadinya kejahatan internet (*cybercrime*) dan perilaku negatif para pengguna internet.[3]

Abdurrahman mengemukakan bahwa ada dua tugas berat yang kini diemban Pemerintah dan seluruh Bangsa Indonesia yaitu melaksanakan usaha-usaha penegakan hukum dan melaksanakan pembangunan Nasional di segalah bidang. Kedua bidang tugas tersebut haruslah senantiasa selaras antara satu dengan lainnya, akan tetapi kadang – kadang dan tidak jarang terjadi kedua bidang tersebut menempati suatu posisi yang kontradiktif, yang menimbulkan berbagai macam masalah.[4]

---

[1] Artikel skripsi. Pembimbing skripsi: Dr. Rodrigo Elias, SH, MH dan Jolly K. Ponngoh, SH, MH.

[2] Mahasiswa Fakultas Hukum Universitas Sam Ratulangi, Manado; NIM: 090711209.

[3] Diakses dari http://fraudcyberbsi.blogspot.co.id/p/berikut-ini-penjelasan-secara-hukum.html. pada tanggal 14 Desember 2015. Pukul 14.00 WITA

[4] Abdurrahman. *Aneka Masalah Hukum Dalam Pembangunan Di Indonesia*. Alumni. Bandung. 1979. Hlm 11

Di Indonesia walaupun sudah ada aturan untuk memberantas kejahatan komputer akan tetapi masi terdapat kendala di dalam penangulangannya atau pemberantasannya. Penindakan kasus *cybercrime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet (warung internet) sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana.[5]

Berdasarkan uraian latar belakang di atas terdorong Penulis untuk mengangkat skripsi dengan judul: "KENDALA YURIDIS DALAM PEMBUKTIAN KEJAHATAN DUNIA MAYA (*CYBER CRIME*) DAN UPAYA MENGATASI TINDAK PIDANA CYBER CRIME MENURUT HUKUM POSITIF INDONESIA"

B. Perumusan Masalah

1. Apakah kendala yuridis dalam pembuktian kejahatan dunia maya (*cyber crime*)?
2. Bagaimanakah upaya mengatasi tindak pidana *cyber crime* menurut hukum positif Indonesia?

C. Metode Penulisan

Penelitian ini bersifat normatif, atau disebut juga dengan penelitian normatif. Sumber data yang digunakan dalam penelitian ini, ialah data sekunder yang mencakup bahan hukum primer, bahan hukum sekunder, dan bahan hukum tertier.

PEMBAHASAN

A. Kendala Yuridis Dalam Pembuktian Kejahatan Dunia Maya (*Cyber Crime*)

Dalam pasal 27 - 37 Undang-Un dang 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 pasa 43 ayat 5 e : "melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Inforrnasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang -Undang ini".[6]

Dan dalam pasal yang sama ayat 5 h tentang saksi ahli : "meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini ".[7]

Pasal 44 UU ITE:

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut :

a. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-Undangan; dan;
b. Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).[8]

Di Indonesia walaupun hukum dibuat antisipatif atau preventif dan seholistik mungkin agar dapat memayungi setiap kegiatan khususnya bidang telematika akan tetapi Undang-Undang ITE ini tetap memiliki kendala-kendala antara lain:

Undang-Undang ITE tidak mengatur secara khusus hal-hal yang menyangkut *cybercrime*. Di dalam Bab Ketentuan Umum tidak secara jelas digambarkan tentang penjelasan kejahatan-kejahatan dengan menggunakan komputer. Kejahatan-kejahatan komputer yang dikenal dalam dunia maya tidak tergambar secara jelas.

[5] Diakses dari https://balianzahab.wordpress.com/artikel/penyidikan-terhadap-tindak-pidana-cybercrime/. Pada tanggal 15 Desember 2015. Pukul 07.00 WITA

[6] Lihat pasal 43 ayat 5 e. UU No 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik

[7] Lihat pasal 43 ayat 5 h. UU No 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik

[8] Lihat pasal 44. UU No 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik

Pemerintah dalam membentuk Undang-Undang ITE ini masih menggunakan pendekatan politis-pragmatis atau cara pandang atau pola pikir yang ingin memperoleh atau mendapatkan sesuatu dengan cara - cara yang mudah dan praktis, bukan menggunakan pendekatan kebijakan publik yang melibatkan lebih banyak kalangan, sehingga tidak heran kalau UU ITE ini hanya sepotong-sepotong mengatur pemanfaatan teknologi yang sudah begitu luas penggunaannya di berbagai aspek kehidupan manusia. UU ITE ini lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, tidak lebih. Padahal siapapun tahu bahwa dunia siber (*cyberword*) lebih luas dari sekedar transaksi elektronik.

Mulyana W. Kusuma menyampaikan bahwa pembangunan hukum yang intinya adalah pembaharuan terhadap ketentuan hukum yang telah ada yang dianggap usang, dan penciptaan ketentuan hukum baru yang diperlukan untuk memenuhi tuntutan perkembangan masyarakat.[9]

Banyak ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam Undang-Undang ITE seperti hal-hal yang diatur dalam buku I KUHP tidak ada dalam Undang-Undang ITE. Seperti kelalaian atau khilaf, di mana lalai atau khilaf adalah kalimat yang sering dilakukan oleh manusia dalam melakukan kegiatannya. Apabila kelalaian itu dilakukan oleh manusia di dunia nyata dan menimbulkan kerugian bagi dirinya sendiri dan orang lain, diatur secara tersendiri dengan menggunakan pasal-pasal tertentu, bahkan kadang pula si pembuat lalai ini juga akan mendapatkan ancaman hukuman seperti banyak ditemukan kasus-kasus pelanggaran lalu lintas. Namun di dalam dunia maya (*cyberspace*) kelalaian adalah tindakan fatal yang bisa menimbulkan kerugian yang tidak sedikit, bahkan bisa menghancurkan sebuah negara sekalipun. Dalam Undang-Undang ITE tidak menyebutkan sedikitpun tentang kelalaian yang dibuat oleh pembuat situs sehingga *hacker* bisa masuk dengan leluasa. Kegiatan yang lain yang sama pentingnya dengan kelalaian adalah percobaan melakukan perbuatan jahat dan turut serta melakukan. Dalam Undang-Undang ITE ini tidak diatur apakah percobaan melakukan dan juga turut serta kejahatan hacking dapat dipidana atau tidak. Kemudian Undang-Undang ITE ini juga tidak mengatur kapan kadaluwarsa perbuatan pidana kejahatan *hacking*. Semua kegiatan kejahatan tersebut diatur pada Bab tentang perbuatan-perbuatan apa saja yang dilarang, sehingga terkesan seperti pasal keranjang sampah, pokoknya semua kegiatan yang melanggar aturan telematika di Indonesia itulah yang dilarang.

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik belum juga mencakup semua aspek dari kejahatan dunia maya. Misalnya *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. Selain itu, kita tidak bisa terus mengacu pada Undang-Undang Informasi Dan Transaksi Elektronik saja, melainkan kita harus menyusun konsep Kitab Undang-undang Hukum Pidana yang baru. Karena KUHP lama sudah tidak dapat lagi menjangkau tindak-tindak pidana baru yang tercipta oleh perkembangan jaman, untuk itu dibutuhkan konsep-konsep baru tentang KUHP dan Hukum Acara Pidana kita, untuk itu Martiman Prodjohamidjojo mengemukakan bahwa untuk lebih menyempurnakan hukum perlu mengadakan Undang – Undang tentang hukum acara pidana untuk melaksanakan peradilan bagi pengadilan dalam lingkungan peradilan umum dan Mahkamah Agung dengan

[9] Mulyana W. Kusuma. *Perspektif, Teori, Dan Kebijaksanaan Hukum*. CV. Rajawali. Jakarta. 1986. Hlm 43

mengatur hak serta kewajiban bagi mereka yang ada dalam proses pidana, sehingga dengan demikian dasar utama negara hukum dapat ditegakan.[10]

B. Upaya Mengatasi Tindak Pidana *Cyber Crime* Menurut Hukum Positif Indonesia

Aktivitas pokok dari *cybercrime* adalah penyerangan terhadap *content*, *computer system* dan *communication system* milik orang lain atau umum di dalam *cyberspace*. Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan.

a. Penanggulangan Global

The Organization for Economic Cooperation and Development (OECD) telah membuat *guidelines* bagi para pembuat kebijakan yang berhubungan dengan *computer related crime*, dimana pada tahun 1986 OECD telah memublikasikan laporannya yang berjudul *Computer Related Crime* : *Analysis of Legal Policy*. Menurut OECD, beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cybercrime* adalah :

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya.
2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
3. meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime.*
4. Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi.
5. Meningkatkan kerjasama antarnegara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*.[11]

Instrumen hukum Internasional yang dapat dirujuk dalam fenomena *cyber crime* sebagai kejahatan transnasional adalah *United Nations Conventions Againts Transnational Organized Crime*, atau yang dikenal dengan Palermo Convention, tahun 2000. Dalam Palermo Convention ini ditetapkan bahwa kejahatan-kejahatan yang termasuk dalam kejahatan transnasional adalah *cybercrime* salah satunya. *Cyber Crime* merupakan bentuk perkembangan kejahatan transnasional yang cukup menghawatirkan saat ini. Konvensi ini meskipun pada awalnya dibuat oleh negara regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan mayantara.[12]

Pada tanggal 23 November 2001 negara-negara yang tergantung dalam Uni Eropa telah membuat dan menyepakati *Convention on Cyber Crime di Budapest*, Hongaria. Hasil dari konvensi tersebut kemudian dimasukan kedalam European *Treaty Series* dengan nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 negara termasuk diratifikasi oleh 3 negara anggota *Council of Europe*. Substansi konvensi mencakup area yang cukup luas, bahkan mencakup kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari *cyber crime*, baik melalui Undang-Undang maupun kerjasama internasional. Pertimbangan dari pembentukan konvensi ini antara lain sebagai berikut:

1) Bahwa masyarakat internasional menyadari perlunya kerjasama antar negara dan industri dalam memerangi kejahatan mayantara dan adanya kebutuhan untuk melindungi kepentingan yang sah di dalam suatu negara serta pengembangan teknologi informasi.

[10] Martiman Prodjohamidjojo. *Komentar Atas KUHAP Kitab Undang – Undang Hukum Acara Pidana*. PT. Pradnya Paramita. Jakarta. 2002. Hlm 2

[11] Dikutip dari karya ilmiah Dr. H. Obsatar Sinaga. Penanggulangan kejahatan Internasional *cyber crime* di Indonesia. Universitas Padjadjaran Bandung. 2010. Hlm 23

[12] Muladi. *Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*. Jakarta. The Habibie Center. 2002. Hlm 89

2) Konvensi saat ini diperlukan untuk meredam penyalahan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Dengan demikian, perlu adanya kepastian hukum dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dicapai, dipercaya dan cepat.
3) Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak asasi manusia (HAM) dan konvenan PBB 1996 tentang hak politik dan sipil yang memberikan perlindungan kebebasasn berpendapat seperti hal berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyabarkan informasi dan pendapat.[13]

Resolusi Kongres PBB VIII tahun 1990 tentang *The Prevention of Crime and Treatment of Offenders* di Havana mengajukan bebrapa kebijakan dalam upaya menaggulangi cyber crime, antara lain sebagai berikut:

1) Menghimbau negara anggota untuk menginvestasikan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah di antaranya.
2) Melakukan modernisasi hukum pidana material dan hukum acara pidana;
3) Mengembangkan tindakan-tindakan pencegahan dan pengamanan computer;
4) Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer;
5) Melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat dan para penegak hukum mengenai kejahatan ekonomi dan *cyber crime*;
6) Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika.
7) Mengadopsi kebijakan perlindungan korban *Cyber Crime* sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk korban melaporkan adanya *cyber crime*;
8) Menghimbau negara anggota menigkatkan kegiatan internasional dalam upaya penanggualngan *Cyber Crime*;
9) Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*Committe on Crime Prevention and Control*) PBB untuk:
   a) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *Cyber Crime* di tingkat nasional, regional dan internasional;
   b) Mempertimbangkan *Cyber Crime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.[14]

Upaya internasional dalam penanggulangan *cyber crime*, juga telah dibahas secara khusus dalam suatu lokakarya yaitu *workshop on crime related to computer networks* yang diorganisasi oleh UNAFEI selama Kongres PBB X tahun 2000 berlangsung. Adapun kesimpulan dari lokakarya ini adalah sebagai berikut :

1. *Computer Related Crime* (CRC) harus dikriminalisasikan.
2. Diperlukan hukum acara yang tepat untuk penyidikan dan penuntutan terhadap penjahat mayantara (*cyber criminals*).
3. Harus ada kerja antara pemerintah dan industri terhadap tujuan umum pencegahan dan penaggulangan kejahatan komputer agar internet menjadi aman.
4. Diperlukan kerjasama internasional untuk menelusuri atau mencari para penjahat internet.

[13] *Ibid*. Hlm 24

[14] Garda T. Paripurna. *Sekilas Tentang Kejahatan Transnasional, Riset Hukum Kejahatan Transnasional*. Bandar maju. Bandung. 2008. Hlm 77

5. PBB harus mengambil langkah atau tindak lanjut yang berhubungan dengan bantuan dan kerja sama teknis dalam penaggulangan *computer related crime* (CRC).[15]

Tegu Prasetyo juga mengungkapkan bahwa, salah satu tujuan sistem peradilan pidana yang ada secara universal, sehingga cakupan tugas sistem peradilan pidana itu memang dapat dikatakan luas, yaitu:

1. Mencegah masyarakat menjadi korban kejahatan;
2. Meyelesaikan kejahatan yang terjadi sehingga masyarakat menjadi puas bahwa keadilan telah ditegakan dan pelaku kejahatan telah dipidana; dan
3. Berusaha agar mereka yang pernah melakukan kejahatan itu tidak mengulangi perbuatannya lagi.[16]

b. Penanggulangan *Cyber Crime* Di Indonesia

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

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dilihat dalam perspektif penanggulangan penyalahgunaan internet di atas, maka semestinya tak perlu ada pro dan kontra. Ini karena pada dasarnya kehadiran UU itu untuk melindungi masyarakat dari kerugian dan kehancuran akhlak yang akan berimplikasi pada kelangsungan hidup berbangsa dan bernegara.

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.[17] 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 Perundang-Undangan; 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).[18]

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.[19]

Perangkat yang menggunakan format data digital untuk menyimpan informasi memang sangat banyak. 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 perangkat-perangkat 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*

[15] *Ibid*. Hlm 28

[16] Teguh Prasetyo. *Kriminalisasi Hukum Pidana*. Nusa Media. Bandung. 2013. Hlm 115

[17] Lihat pasal 44. UU No 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik

[18] Lihat pasal 43 ayat 5 e. UU No 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik

[19] Yuyun Yulianah. *Pembuktian Tindak Pidana Cyber Crime*. Sinar Grafika. Bandung. 2002. Halaman 7

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 dapat menyimpan 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.[20]

2. Penegakan Hukum *Cyber Crime* Dengan Menggunakan Sarana 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:

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.[21]

PENUTUP

A. Kesimpulan

1. Undang-Undang ITE tidak mengatur secara khusus hal-hal yang menyangkut *cybercrime*, Pemerintah dalam membentuk Undang-Undang ITE ini masih menggunakan pendekatan politis-pragmatis, bukan menggunakan pendekatan kebijakan publik yang melibatkan lebih banyak kalangan. UU ITE ini lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, tidak lebih. Padahal siapapun tahu bahwa dunia siber (*cyberword*) lebih luas dari sekedar transaksi elektronik. Ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam Undang-Undang ITE seperti kelalaian atau khilaf. Undang-Undang ITE ini juga tidak mengatur kapan kadaluwarsa perbuatan pidana kejahatan hacking
2. Penanggulangan *cyber crime* dapat merujuk pada beberapa instrumen hukum internasional, antara lain instrumen Palermo dan instumen Hongaria. Dimana substansinya dimungkinkan untuk diratifikasi dan diaksesi oleh Negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan mayantara atau *cyber crime*, dan mencakup kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari *cyber crime*, baik melalui Undang-Undang maupun kerjasama internasional. Optimalisasi UU ITE dapat mempermudah kepolisian dalam melakukan investigasi kejahatan *cyber crime*, khususnya dalam mengumpulkan alat bukti berdasarkan pasal 5 dan pasal 44 UU ITE. Pendekatan budaya atau cultural perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber*

[20] *Ibid*. Hlm 8-11

[21] *Ibid*. Hlm 7

crime dan menyebarluaskan atau mengajarkan etika penggunaan computer melalui media pendidikan.

B. Saran

1. Untuk kendala-kendala yuridis yang ada maka untuk mengatasinya perlu dilakukan revisi atas Undang-Undang tersebut seperti melakukan redefinisi mengenai pengertian atau peristilahan dalam peraturan Perundang-Undangan ITE sehingga terdapat batasan dan kejelasan makna serta tidak menimbulkan celah hukum (*loopholes*). Selain itu Berkaitan dengan kebijakan hukum pidana yang tidak hanya memikirkan kebutuhan hukum saat ini tetapi juga yang akan datang, maka untuk memberikan alternatif pemidanaan bagi pelaku *cybercrime*, rumusan dalam RUU KUHP mengenai pidana kerja sosial bisa memberikan alternatif penjeraan bagi pelaku pidana.
2. Dengan adanya instrumen hukum internasional hendaknya Pemerintah lebih pekah terhadap kejahatan *cyber crime*, memperbanyak kerja sama dengan negara-negara lain dalam memberantas kejahatan dunia maya dan Institusi penegak hukum perlu adanya pendidikan khusus untuk mendalami kejahatan *cyber crime,* sebab bukan lagi hal rahasia dimana aparat hukum jauh dari perkembangan hukum atau minimnya pengetahuan terkait dengan perkembangan kejahatan akibat perkembangan teknologi. Sehingga terlihat dalam penanganan *cyber crime* belum efektif. Sehingga, dengan adanya pendidikan khusus dapat memberikan penekanan bagi aparat penegak hukum agar memiliki ketrampilan dasar dalam menggunakan komputer dan internet sehingga mampu mengatasi kejahatan di dalam dunia maya.

DAFTAR PUSTAKA

Amirudin, dan H. Zainal Asikin. ***Pengantar Metode Penelitian Hukum*.** PT. Raja Grafindo Persada , Jakarta. 2004

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

Abdurrahman. ***Aneka Masalah Hukum Dalam Pembangunan Di Indonesia***. Alumni. Bandung. 1979

Abdul Wahid dan Mohammad Labib. ***Kejahatan Mayantara (Cyber Crime)***. PT. Refika Aditama. Jakarta. 2005

Baharudin Lopa. ***Pertumbuhan Demokrasi Penegakan Hukum Dan Perlindungan Hak Asasi Manusia***. PT Yarsif Watampone. Jakarta. 1999

Barda Nawawi, Arief. ***Bunga Rampai Kebijakan Pidana***. PT. Citra Aditya Bakti. Bandung. 1996

Bambang Sunggono. ***Metode Penelitian Hukum*.** PT. Raja Grafindo Persada. Jakarta. 2011

Barda Nawawi Arief. ***Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indoensia***. PT. Raja Grafindo Persada. Semarang. 2006

Barda Nawawi Arief. ***Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan***. Kencana Predana Media Group. Jakarta. 2007

Komar Andasasmita. ***Masalah Hukum Perdata Nasional Indonesia***. Alumni. Bandung. 1983

Mulyana W. Kusuma. ***Perspektif, Teori, Dan Kebijaksanaan Hukum***. CV. Rajawali. Jakarta. 1986

Martiman Prodjohamidjojo. ***Komentar Atas KUHAP Kitab Undang – Undang Hukum Acara Pidana***. PT. Pradnya Paramita. Jakarta. 2002

Soerjono Soekanto dan Sri Mamudji, ***Penelitian Hukum Normatif Suatu Tinjauan Singkat*,** PT.Raja Grafindo Persada. Jakarta. 2004

Soerjono Soekanto. ***Pokok–pokok Sosiologi Hukum***. PT. Raja Grafindo Persada. Jakarta. 2009

Sudikno Mertokusumo. ***Mengenal Hukum***. Liberty Yogyakarta. Bandung. 2000

Soerjono Soekanto. ***Pengantar Penelitian Hukum***. UI Press. Jakarta. 1982

Teguh Prasetyo. ***Kriminalisasi Hukum Pidana***. Nusa Media. Bandung. 2013

Umar Tirtaraharjda dan La Sula. ***Pengantar Pendidikan***. Rineka Cipta. Jakarta.

W. Friedmann. ***Teori dan Filsafat Hukum***. Raja Grafindo Persada. Jakarta. 1993

Wirjono Prodjodikoro. ***Asas – Asas Hukum Pidana Di Indonesia***. PT Eresco. Bandung. 1989

Yunasril Ali. ***Dasar-Dasar ILmu Hukum***. Sinar Grafika. Jakarta. 20092000

Sumber-Sumber Lainnya:

Barda Nawawi Arief, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indoensia. Handout Materi Perkuliahan Program Magister Ilmu Hukum Undip Semarang. Konsentrasi Sistem Peradilan Pidana.

Tulisan Heri Kiswanto. Cyber crime dan Transaksi Elekronik dalam UU No. 11 Tahun 2008 tentang ITE. Hlm 15. Diakses dari http://www.scribd.com/doc/24106593/Smtr-Sejarah-Hukum. pada tanggal 15 Desember 2015.

Diakses dari https://abayali31.wordpress.com/2012/03/18/manfaat-dan-dampak-komputer-bagi-kehidupan/. Pada tanggal 14 Desember 2015.

Diakses dari http://toraerdo.blogspot.co.id/2012/06/faktor-yang-mempengaruhi-terjadinya.html. pada tanggal 14 Desember 2015.

Diakses dari http://etikaprofesitikbsi.blogspot.co.id/2013/05/penyebab-terjadinya-cybercrime.html. pada tanggal 14 Desember 2015.

Diakses dari http://fraudcyberbsi.blogspot.co.id/p/berikut-ini-penjelasan-secara-hukum.html. pada tanggal 14 Desember 2015.

Diakses dari https://balianzahab.wordpress.com/artikel/penyidikan-terhadap-tindak-pidana-cybercrime/. Pada tanggal 15 Desember 2015.

Arief Adiharsa, *Cyber Crime* : Carding, Di kutip dari http://www.yahoo.com, Diakses pada tanggal 28 November 2015.

Diakses dari http://etikaprofesitikbsi.blogspot.co.id/2013/05/karakteristik-cybercrime.html. pada tanggal 15 Desember 2015.

Diakses dari https://ranggablack89.wordpress.com/2012/04/01/cyber-crime-definisi-jenis-jenis-dan-cara-penanggulangannya/. Pada tanggal 15 Desember 2015.

Yeni Widowaty. *Aspek Hukum Tindak Pidana Cyber Crime dalam Penggunaan Teknologi Informasi*. Dikutip dari http://www.yahoo.com Diakses pada tanggal 16 November 2015.

Danan Mursito dkk, Pendekatan Hukum untuk Keamanan Dunia Cyber serta Urgensi Cyber Law bagi Indonesia, 2005. Makalah Program Studi Teknologi Informasi Program Magister Fakultas Ilmu Komputer Universitas Indonesia, hlmn 5. Dikutip dari http://www.yahoo.com. Diakses pada tanggal 30 April 2015