UPAYA PENANGGULANGAN KEJAHATAN KOMPUTER DALAM SISTEM ELEKTRONIK MENURUT PASAL 30 UNDANG-UNDANG NOMOR 11 TAHUN 2008[1]

Oleh : Brisilia Tumalun[2]
Dosen Pembimbing:
Prof. Dr. Telly Sumbu, SH, MH;
Dr. Wempie Jh. Kumendong,SH,MH.

ABSTRAK

Penelitian ini dilakukan dengan tujuan untuk mengetahui bagaimana upaya penanggulangan kejahatan komputer dalam sistem elektronik menurut pasal 30 UU No. 11 Tahun 2008 dan apa yang menjadi faktor penghambat dalam penanggulangan kejahatan komputer dalam sistem elektronik. Dengan menggunakan metode penelitian yuridis normatif, disimpulkan: 1. Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Digunakannya hukum pidana di Indonesia sebagai sarana untuk menanggulangi kejahatan tampaknya tidak menjadi persoalan. Hal ini terlihat dari prakteknya dalam perundangan-undangan selama ini yang menunjukan bahwa penggunaan hukum pidana merupakan bagian dari kebijakan hukum yang dianut di Inonesia. 2. Walaupun pada Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sudah mencantumkan perbuatan yang dilarang dalam dunia maya yang terdapat pada Pasal 27 sampai Pasal 37. Kenyataan pelanggaran pada dunia maya juga tidak berhenti malah semakin meningkat berdasarkan laporan dari berbagai macam pengamat dan laporan statistik kejahatan dunia maya di Indonesia.

Kata kunci: Upaya penanggulangan, kejahatan, komputer, sistem elektronik.

PENDAHULUAN

A. Latar Belakang

Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Perlu digaris bawahi, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Perkembangan komputer dan internet tidak dapat dipungkiri telah menjadi sarana atau ladang baru bagi dunia kejahatan. Sebab komputer dan internet sebagai ciptaan manusia memiliki karakteristik mudah dieksploitasi oleh siapa saja yang memiliki keahlian dibidang tersebut. Oleh karena itu, membahas permasalahan ini tidak akan bisa lepas dari pembahasan masalah keamanan dari teknologi tersebut.[3]

Dewasa ini tidak ada satu sisi kehidupan yang tidak menggunakan pengolahan komputer, baik yang hanya bersifat sederhana sampai dengan yang kompleks. Saat ini komputer tidak hanya berfungsi sebagai alat pengolahan data saja, namun telah menjadi senjata utama dalam melakukan kejahatan.[4]

Cyber crime itu sendiri adalah kejahatan yang dilakukan oleh seseorang maupun kelompok dengan menggunakan sarana komputer dan alat telekomunikasi lainnya. Seseorang yang menguasai dan mampu mengoperasikan komputer seperti operator, programmer, analis, manager, kasir juga dapat melakukan *cyber crime.* Cara yang bisa dilakukan dengan cara merusak data, mencuri data, dan menggunakannya secara ilegal. Faktor yang dominan mendorong berkembangnya *cyber crime* itu sendiri adalah pesatnya perkembangan teknologi komunikasi seperti telepon, *handphone,* dan alat telekomunikasi lainnya yang dipadukan dengan perkembangan teknologi komputer.[5]

Kejahatan dapat dilakukan dimana saja, baik dalam ruang nyata maupun ruang maya (*Cyberspace*). Hal ini terjadi karena era globalisasi membuka beberapa peluang terjadinya kejahatan, sehingga diperlukan penanggulangan secara bersama-sama melalui kerjasama antar pihak yang berkepentingan. Kejahatan sangat erat kaitannya dengan perkembangan masyarakat.. Kejahatanpun menjadi sebagian dari budaya itu sendiri. Hal ini

[1] Artikel Skripsi.

[2] Mahasiswa pada Fakultas Hukum Unsrat, NIM. 14071101362

[3] Khairul Anam, *Hacking vs Hukum Positif dan Hukum Islam.* , Sunan Kalijaga, Yogyakarta 2010, hlm. 3

[4] Deris Setiawan*, Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta, 2005, hlm. 1

[5] Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya,* Laksbang Pressindo, Jogjakarta, 2007, Hal. 4

berarti semakin tinggi budaya dan semakin *modern* suatu bangsa maka semakin *modern* pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya. Secara sederhana, setiap kejahatan yang dilakukan mengarah pada sistem komputer maupun menggunakan komputer sebagai sarana melakukan kejahatan disebut *Cybercrime*.[6]

Pemerintah Indonesia telah berupaya dengan membuat berbagai macam regulasi dan peraturan untuk menghadapi akibat yang timbul dari kejahatan komputer, itu dibuktikan dari gigihnya aparat penegak hukum dengan mencoba menjerat para pelaku kejahatan komputer dengan hukum pidana yang berlaku hingga pengesahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) . Undang-Undang ini diharapkan mampu menjawab berbagai persoalan yang timbul dari kasus yang menyangkut teknologi informasi.[7]

Pembentukan Badan khusus untuk menangani kejahatan tindak pidana khusus cyber atau dunia maya di Indonesia masih dalam proses perencanaan dan wacana. Rencana pembentukan badan khusus tersebut disambut dengan baik oleh pihak kepolisian. Dengan adanya badan khusus dalam menangani kasus-kasus kejahatan dunia maya diharapkan bisa untuk mengurangi kejahatan tersebut di Indonesia yang mana semakin lama semakin tinggi ancamannya.

Pembentukan badan khusus tindak pidana dunia maya ini juga diharapkan melibatkan pihak kepolisian sebagai instansi yang memang bergerak dalam bidang penegakan tindak hukum kriminal. Dengan kata lain dimasa-masa yang akan datang badan khusus ini akan mampu memabantu kepolisian mengungkap dan menagkap para tersangka yang menggunakan teknologi sebagai alat kejahatan.[8]

B. RUMUSAN MASALAH

1. Bagaimana upaya penanggulangan kejahatan komputer dalam sistem elektronik menurut pasal 30 UU No. 11 Tahun 2008?
2. Apakah yang menjadi faktor penghambat dalam penanggulangan kejahatan komputer dalam sistem elektronik?

C. METODE PENELITIAN

Metode penelitian yang digunakan dalam skripsi ini yaitu metode penelitian keperpustakaan (*library research*) yang dilakukan dengan membaca serta mempelajari sumber yang tertulis, kemudian diperoleh melalui buku-buku serta perundang-undangan serta bahan tertulis lainnya.

PEMBAHASAN

A. Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Berdasarkan Pasal 30 UU No. 11 TAHUN 2008

Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sejak tahun 2008 kejahatan yang berkaitan dengan komputer sudah banyak diadili berdasarkan Undang-Undang No. 11 Tahun 2008.[9]

Kejahatan komputer adalah perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, bail untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas kejahatan komputer didefisinikan sebagai perbuatan melawan hukum yang dilakukan dengan penggunaan teknologi komputer yang canggih.

Didalam pasal 30 UU Nomor 11 Tahun 2008 diatur mengenai perbuatan yang dilarang yaitu akses ilegal (*Illegall Access)*. *Cracking* dan

[6] Widodo, *Memerangi Cybercrime,* CV Aswaja Presindo, Yogyakarta, 2013, hlm. 1.
[7] Muzamil Sanusi, *The Genius: Hacking Sang Pembobol Data,* PT Elex Media Komputindo, Jakarta, 2010, hlm. 8
[8] *Ibid.*
[9] Sutarman, *Cyber Crime-Modus Operandi dan Penanggulangannya,* Laksbang Pressindo, Yogyakarta, 2007, hal.5

Hacking merupakan bagian dari akses illegal tersebut. Pasal 30 UU ITE berbunyi :

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik milik orang lain dengan cara apapun.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/ atau dokumen elektronik.
(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik dengan cara apapun melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.[10]

Ketentuan Pidana dari Pasal 30 UU ITE diatur dalam Pasal 46 UU ITE yang berbunyi:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah).
(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).

Berbicara mengenai *illegal access* (akses ilegal) seperti yang sudah dijelaskan dalam Bab II bahwa akses ilegal merupakan akses tanpa ijin ke sistem komputer dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain. *Hacking* merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi. Akses ilegal merupakan salah satu berbagai macam-macam dari kejahatan komputer. Akses illegal sendiri memiliki beberapa jenis yaitu :[11]

1. Akses illegal sebagai tindak kejahatan murni:
   Dimana orang yang melakukan kejahatan yang dilakukan secara disengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian terhadap suatu sistem informasi atau sistem komputer.
2. Akses illegal sebagai tindakan kejahatan abu-abu :
   Dimana kejahatan ini tidak jelas antara kejahatan criminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.
3. Akses illegal yang menyerang individu :
   Yaitu kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba taupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi.
4. Akses illegal yang menyerang hak cipta (hak milik) :
   Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/ umum ataupun demi materi/ non materi.
5. Akses illegal yang menyerang pemerintah :
   Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan atau menghancurkan suatu negara.

Para penegak hukum masih belum terlalu familiar dengan kejahatan dunia maya, sehingga implementasi UU ITE 2008 belum maksimal. Selain itu penyebab yang lebih mendasar adalah kenyataan bahwa transaksi di

[10] Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

[11] Budi Suharyanto, *Op.Cit,* hal. 28

dunia maya memang rawan penerobosan dan potensi keuntungan yang bisa diperoleh dari kejahatan tersebut juga luar biasa besar. Walaupun pada undang-undang ITE 2008 sudah mencantumkan perbuatan yang dilarang dalam dunia maya yang terdapat pada pasal 27 sampai pasal 37. Kenyataan pelanggaran pada dunia maya juga tidak berhenti malah semakin meningkat berdasarkan laporan dari berbagai macam pengamat dan laporan statistik kejahatan dunia maya di Indonesia.[12]

Peluang terjadinya penyalahgunaan data pribadi warga negara kian terbuka, dengan begitu banyaknya aturan yang memberikan ruang bagi institusi pemerintah maupun swasta untuk mengumpulkan dan membuka data-data pribadi warga negara. Situasi ini tergambar paling tidak dari banyaknya undang-undang di Indonesia, yang materinya mengandung konten data pribadi, baik beraspek melindungi maupun sebaliknya, memberi peluang pembukaan data. Studi yang dilakukan ELSAM misalnya menemukan sedikitnya 30 undang-undang di Indonesia, yang memiliki keterkaitan dengan perlindungan data pribadi salah satunya yaitu Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sayangnya ketigapuluh undang-undang tersebut *over lapping* satu sama lain, misalnya dari tujuan pengolahan data, notifikasi, tujuan pembukaan data, durasi pengumpulan dan pembukaan data, penghancuran data, pemberian izin pembukaan data, sanksi, dan pemulihannya.

Pemerintah sendiri, melalui Direktorat Jenderal Informasi dan Komunikasi Publik (IKP), Kominfo, saat ini tengah menyiapkan RUU Perlindungan Data Pribadi. Proses persiapannya telah memasuki tahap harmonisasi di Direktorat Jenderal Peraturan Perundang-undangan, Kemenkumham. Rencananya, RUU ini akan didorong oleh pemerintah untuk menjadi prioritas Program Legislasi Nasional (Prolegnas) 2018. ELSAM sendiri sudah terlibat dalam dua rapat koordinasi yang diselenggarakan oleh Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan; serta Kementerian Hukum dan HAM, untuk secara khusus membicarakan materi dan tahapan formal pengajuan RUU Perlindungan Data Pribadi. [13]

B. Faktor Penghambat Dalam Penanggulangan Kejahatan Komputer Dan/ Atau Sistem Elektronik

1.) Terbatasnya Personil Tenaga Ahli

Terbatasnya jumlah personil tenaga ahli antara Negara Indonesia dan china sangatlah berbeda jauh dalam jumlah personilnya. Lebih ironis lagi laporan tingkat kejahatan siber di Indoensia semakin meningkat, dengan keterbatasan personil dan tenaga ahli di pihak kepolisisan Indonesia maka penyelesaian kasus tersebut tidak bisa diselesaikan dengan cepat. Akibatnya dirasakan langsung oleh pihak korban atau kejahatan siber. Kualitas fasilitas teknologi informasi di Indonesia memang sudah cukup baik, namun tidak sebanding dengan jaminan keamanan oleh para pengguna. Keterbatasan tenaga ahli pada pihak kepolisian memang merupakan factor yang sangat besar, dengan jumlah anggota ahli yang terbatas ini pengungkapan dan penyidikan kasus kejahatan dunia maya tidak bisa diselesaikan dengan waktu yang cepat, sehingga akan membuat para pelaku lebih leluasa dalam beraksi. [14]

Jika kita melihat Negara china *cyber police* Negara itu memiliki jumlah anggota personil sebanyak 18.000 orang. Ini bukti bhwa pemerintah china sudah menganggap serius betapa besarnya ancaman dari dunia maya di Negara itu. Dengan adanya kerjasama pemerintah indonesia dan china diharapkan para penegak hukum bisa lebih paham dan cepat dalam bertindak. Kementrian Komunikasi Dan Informasi (KOMINFO) yang mana memang terkait langsung pada kebijakan penggunaan fasilitas teknologi informasi dan internet di Indonesia. Dari informasi yang didapat

[12] *Ibid.*

[13] http://elsam.or.id/2017/05/kebutuhan-akan-uu-perlindungan-data-pribadi-kian-mendesak/, diakses pada tanggal 19 April 2018.

[14] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penaggulangan Kejahatan*, Jakarta: Kencana, 2007, hlm. 237.

penulis anggota kepolisian masih belum terlalu melek akan teknologi, bahkan banyak diantara anggota *cyber police* Indonesia masih baru memakai computer. Bisa dikatakan kemampuan polisis Indonesia dalam dunia maya masih dalam tahap standar atau pemula. Keterbatasan jumlah personil tenaga ahli sebenarnya bisa diatasi dengan adanya pelatihan-pelatihan baik oleh kepolisian atau pihak universitas dan perguruan tinggi negri atau swasta yang terdapat fakultas teknologi informasi. Langkah ini perlu dilakukan untuk merekrut tenaga-tenaga ahli teknologi informasi terutama sekali para pelajar dan mahasiswa yang memiliki keahlian dibidang IT (*Information technology*)pihak dosen dan mahasiswa memiliki peran yang sangat startegis sebab merekalah yang paling bisa mengikuti perkembangan.[15]

Para praktisi juga bisa memberikan peran penting dalam memberikan masukan-masukan kepada pihak pemerintah dalam keamanan jaringan komputer dan internet. Mendesaknya kebutuhan tenaga ahli juga harus diimbangi dengan adanya sarana dan prasarana serta fasilitas peralatan yang canggih dan maju dalam mendukung keamanan jaringan dan juga untuk memudahkan pelacakan pelaku kejahatan agar kasus kejahatan dunia maya dapat di atasi dengan cepat. Jumlah anggaran yang kurang menjadi penyebab faktor yang sangat besar dalam pengungkapan kasus kejahaatan siber, dengan keterbatasan anggaran maka akan berdampak langsung pada peralatan yang digunakan oleh pihak kepolisian untuk melacak pelaku kejahatan siber.Seperti yang dikutip dari situs berita kriminalitas.com, Sebagai contoh perbandingan penulis membandingkan rancangan anggaran cyber di Amerika Serikat yang mencapai USD 19.miliar dollar pada tahun 2017, keadaan ini mengaharuskan pemerintah Amerika Serikat karena menambah anggaran yang cukup besar tersebut disebabkan oleh ancaman dunia maya (cyber) di Amerika Serikat juga angat meningkat tajam. [16]

Mantan Presiden obama juga menandatangani perintah eksekutif untuk memebntuk dewan privasi federal, sebuah lembaga kordinasi untuk yang bertugas mengembangkan buku acuan komprhensif mengenai pengumpulan dan penyimpanan data pribadi warga, selain tiu ususlan anggaran pemerintah akan mengalokasikan dana sebesar 62 juta dolar untuk mempekerjakan pakar dunia maya bagi pemerintah.3 Sudah saatnya pemerintah melalui KOMINFO dan pihak institusi kepolisisan mulai menambah anggaran untuk keamanan *cyber* agar kasus penyalahgunaan teknologi informasi dapat diminimalisir. Program kerja yang dilakukan oleh presiden amerika barack obama tersebut selain menambah anggaran untuk keamanan dunia maya, pemerintah Amerika Serikat juga iukut melibatkan dan memberdayakan para pakar-pakar dan tenaga ahli dunia maya agar dapat ambil bagian untuk menjaga keamanan dunia maya dinegara tersebut.

Langkah yang dilkukan oleh Mantan Presiden Amerika Serikat Barack Obama juga bisa diterapkan di Indonesia dengan memberdayakan dan mempekerjakan para pakar dan tenaga ahli dunia maya di Indonesia untuk keamanan jaringan, walaupun membutuhkan waktu yang tidak sebentar setidaknya langkah tersebut bisa diterapkan oleh pemerintah Indonesia untuk mengurangi keterbatsan tenaga ahli. Kejahatan dunia maya diindonesia yang paling banyak ialah kejahatan perbankan dengan motif untuk mendapatkan keuntungan berupa uang. Walau masih bersifat kejahatan perbankan, namun jika terus dibiarkan maka bukan tidak mungkin cepat atau lambat *cyber terorrism* juga akan mengancam Indonesia. [17]

2.) Lemahnya Pengawasan Pemerintah

[15] http://kriminalitas.com/khawatir-dengan-cyber-crime-obama-naikkan-anggaran-keamanan-cyber/,di akses pada tanggal 10 Desember 2017 Pukul 07.21

[16] Barda Nawawi, Op.Cit, hal. 20

[17] http://azamul.files.wordpress.com/2007/06/thesis-cybercrime-di-indonesia.pdf, diakses pada 12 desember 2017 pukul 01. 22

Lemahnya pengawasan penggunaan internet berpotensi besar akan menciptakan peluang terjadinya kejahatan *cyber crime* (dunia maya). Karena kejahatan dengan menggunakan teknologi terjadi jika ada akses internet yang cukup memadai. Fasilitas internet Di Indonesia bisa dikatakan sudah memadai baik dari segi kecepatan akses dan kemduahan pemasangan jaringan akses internet. Dalam hal pengawasan pemerintah telah mengontrol pengawasan trafik konten negatif internet yang dapat diakses di indonesia.

Seperti pemblokiran situs-situs porno, SARA, kekerasan dan situs-situs website yang dianggap menyalahi norma kesusilaan. Dari segi prosedur pemasangan jaringan koneksi internet di indonesia dari yang dipaparkan oleh narasumber hamper 95% persen dikandalikan oleh pihak swasta, peran dari pemerintah hanya 5% saja, jika ISP *(Internet Service Provider*) seluruhnya pihak swasta yang menegendalikan maka berakibat pada akan terjadi lemahnya pengawasan oleh pihak pemerintah, biaya yang cukup murah serta akses kecepatan internet yang cukup memadai maka akan sangat rawan dalam penyalahgunaan penggunaan jaringan internet. Seperti halnya *provider* XL dan Indosat yang hamper semua sahamnya dimiliki oleh pihak asing merupakan lahan bisnis yang sangat besar bagi pihak swasta untuk meraup keuntungan dari penyediaan jasa internet di indonesia, tongginya pengguna internet di indoensia juga salah satu faktor pihak sawasta melakukan ekspansi ke indonesia. Dengan leluasanya pihak swasta mengendalikan jaringan koneksi di Indonesia dinilai salah satu penyebab maraknya menyalahgunaan internet (*Internet Misuse*).[18]

Tidak adanya kebijakan dan langkah prventif menjadi faktor utama, para pengguna bisa dengan bebas mengakses data-data tertentu yabg mana bisaa disalahginakan oleh pengguna yang tidak bertamggung jawab. Dalam jangka panjang maka alamat *Ip Address* dan *domain name* asal indonesia akan di black list oleh dunia internasional sehingga kerugianpun akan ditanggung oleh rakyat indonesia Penggunaan fasilitas internet sangatlah dibutuhkan oleh pengguna teknologi informasi dalam hal ini pihak yang bertanggung jawab adalah penyedia jasa layanan internet atau ISP (*internet service provider)* yang harus menyediakan pelayanan maupun servis ketika ada kerusakan, namun dikarenakan dikendalikan oleh pihak swasta Maka penulis berpendapat ada celah hukum yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab dalam menyalahgunakan fasilitas internet, jika dilihat dari Undang-Undang No 11 Informasi Dan Transaksi Elektronik Tahun 2008 misalnya yang terdapat pada pasal 13, pasal 14, pasal 15 dan pasal 16. Pasal tersebut lebih fokus untuk menitikberatkan penyelenggaraan sistem elektronik harus sesuai dengan apa yang dibutuhkan oleh pengguna jasa elektronik. Sedangkan pasal 23, pasal 24, pasal 25 dan pasal 26 yang mengatur tentang Nama Domain, Hak Kekayaan Intelektual Dan Perlindungan Hak Pribadi, Tidak ada satupun pada pasal-pasal tersebut yang menyebutkan pengawasan penggunaan internet .

Pasal 23 hingga pasal 26 lebih cenderung fokus pada hak kekayaan intelektual atau semacam hak paten. Dengan adanya campur tangan pemerintah dalam mengawasi perizinan pemasangan akses jaringan internet diharapkan tingkat kejahatan dunia maya dapat diminimalisir.[19]

3.) Kendala Prosedural Hukum UU ITE

Walaupun pada undang-undang ITE 2008 sudah mencantumkan perbuatan yang dilarang dalam dunia maya yang terdapat pada pasal 27 sampai pasal 37. Kenyataan pelanggaran pada dunia maya juga tidak berhenti malah semakin meningkat berdasarkan laporan dari berbagai macam pengamat dan laporan statistik kejahatan

[18] Juju, Dominikus. *Tekhnik Menagkal Kejahatan Internet*. Jakarta: Elek Media Komputindo, 2008, hlm 25.

[19] *Ibid.* hlm. 27

dunia maya di Indonesia. Walaupun jumlah pengguna internet di indonesia masuk pada nomor urut yang terbesar ke 6 di dunia, tidak dapat langsung diakitkan dengan jumlah serangan dunia maya di indonesia. Lemahnya perangkat hukum UU ITE 2008 dipastikan terkendala dari pihak personil penegak hukum itu sendiri, masih banyak para penegak yang belum memahami makna dari UU ITE 2008 terutama mengenai perbuatan yang dilarang pada pasal 27 hingga 37. Kendala ini berdampak tidak maksimalnya penerapan hukum UU ITE tersebut di indonesia, kendala lain yang terdapat pada UU ITE yaitu pada bab 10 (X) pasal 43 ayat 3 tentang penyidikan yang berbunyi "Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat". Pasal 43 ayat 3 tersebut bisa dikatakan sebagai batu sandungan oleh pihak penyidik dalam menagkap pelaku atau tersangka kejahatan dunia maya.[20]

Dengan menerapkan langkah hukum yang sama dengan *cyber police* singapura maka pemerintah Indoensia dalam hal ini penegak hukum seperti kepolisisan akan mampu menangani kasus kejahatan dunia maya lebih cepat dibandingkan dengan harus terlebih dahulu mengurus suart izin penahanan pada pengadilan setempat. Maka dari itu revisi undang-undang ITE 2008 pada pasal 43 ayat 3 perlu segera dilakukan untuk memudahkan pengungkapan dan penanganan kasus agar jaminan keamanan dan kenyamanan pengguna internet bisa terjamin. Dari berbagai rangkuman Kendala-kendala pemerintah Indonesia dalam menaggulangi kejahatan *cyber crime* diatas maka dapat disimpulkan bahwa secara garis besar adalah terbatasnya personil tenaga ahli, terbatasnya anggaran, lemahnya pengawasan pemerintah dan masalah prosedural hukum UU ITE 2008. Selain masalah teknis seperti keterbatasaan jumlah anggota personil yang ahli dalam bidang *cyber crime* langkah yang dapat dilakukan adalah dengan menagadakan pelatihan-pelatihan anggota polri yang fokus dalam kejahatan khusus *cyber*, dan alangkah baiknya ikut membuat kerjasama kepada para praktisi-praktisi dan juga para pelajar atau mahasiswa yang ahli dalam bidang dunia maya atau *cyber*.[21]

PENUTUP

A. KESIMPULAN

1. Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Digunakannya hukum pidana di Indonesia sebagai sarana untuk menanggulangi kejahatan tampaknya tidak menjadi persoalan. Hal ini terlihat dari prakteknya dalam perundangan-undangan selama ini yang menunjukan bahwa penggunaan hukum pidana merupakan bagian dari kebijakan hukum yang dianut di Inonesia.
2. Walaupun pada Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sudah mencantumkan perbuatan yang dilarang dalam dunia maya yang terdapat pada Pasal 27 sampai Pasal 37. Kenyataan pelanggaran pada dunia maya juga tidak berhenti malah semakin meningkat berdasarkan laporan dari berbagai macam pengamat dan laporan statistik kejahatan dunia maya di Indonesia.

B. SARAN

1. Segera membuat regulasi yang berkaitan dengan *cyber law* pada umumnya dan *cyber crime* pada khususnya.
2. Kepada pemerintah supaya lebih tegas lagi dalam menangani kasus-kasus *cyber crime*. Dan kepada para pakar IT supaya dalam membuat program pengamanan data lebih optimal lagi sehingga kasus-kasus kejahatan di dunia maya dapat diminimalkan. Perlunya Dukungan Lembaga Khusus: Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara

[20] Ahmad M. Ramli, *Cyber Law Dan HAKI*, Bandung: Refika Aditama, 2006, hlm. 4

[21] *Ibid*, hlm. 12

intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime.

DAFTAR PUSTAKA

LITERATUR

Antonius, *Relasi dengan Dunia, PT Elex Media Komputindo,* Jakarta, 2005.

Arief Barda Nawawi, *Tindak Pidana Mayantara*, PT Raja Grafindo Persada,Jakarta 2006.

Arief Barda Nawawi, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penaggulangan Kejahatan*, Jakarta: Kencana, 2007.

Anam Khairul, *Hacking vs Hukum Positif dan Hukum Islam.* , Sunan Kalijaga, Yogyakarta 2010.

Ahmad M Ramli, *Cyber Law Dan HAKI*, Bandung: Refika Aditama, 2006.

Asmarawati Tina, *Pidana dan Pemidanaan dalam sistem Hukum di Indonesia.* Deepublish, Yogyakarta, 2015.

Irwansyah Edy, *Pengantar Teknologi Informasi*, Deepublish, Yogyakarta, 2014.

Juju, Dominikus. *Tekhnik Menagkal Kejahatan Internet*. Jakarta: Elek Media Komputindo, 2008.

Kuswayanto Lia, *Mahir Berkomputer,* PT. Grafindo Media Pratama, Bandung, 2006.

Mansur Dikdik M. Arief dan Gultom Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi,* Refika ditama, Bandung,2005.

Maskun dan Meilarati Wiwik, *Aspek Hukum Penipuan Berbasis Internet,* Bandung, CV Keni Media, 2017.

Marbun Rocky, *Kiat Jitu Menyelesaikan Kasus Hukum,* Transmedia Pustaka, Jakarta, 2011.

Riswandi Budi Agus, *Hukum Dan Internet Di Indonesia*, yogyakarta: UII Pres, 2003.

Suharyanto Budi, *Tindak Pidana Teknologi Informasi Urgensi Pengaturan dan Celah Hukumnya,* PT Raja Grafindo Persada, Jakarta, 2012.

Setiawan Deris*, Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta, 2005.

Sanusi Muzamil, *The Genius: Hacking Sang Pembobol Data,* PT Elex Media Komputindo, Jakarta, 2010.

Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya,* Laksbang Pressindo, Jogjakarta, 2007.

Widodo, *Memerangi Cybercrime,* CV Aswaja Presindo, Yogyakarta, 2013.

Yesmil dan Adang, *Pembaharuan Hukum Pidana,* Grasindo, Jakarta, 2008.

PERUNDANG-UNDANGAN

Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Kitab Undang-Undang Hukum Pidana

SUMBER-SUMBER LAIN

http://www.academia.edu/7154436/menanggulangi-kejahatan-komputer

https://atinsambry.wordpress.com/kejahatan-komputer/

http://www.mandalamaya.com/pengertian-virus-komputer-dan-cara-penyebaran-virus/.

http://journal.uinjkt.ac.id/index.php/salam/article/downloadSuppFile/1541/115

Hikmah Aryani, https://hikmaharyani.wordpress.com/2017/07/06/penerapan-cyberlaw-di-indonesia/.

https://news.detik.com/berita/d-3460864/kasus-pembobolan-situs-tiket-online-ini-penjelasan-citilink.

http://mesamanth4.blogspot.co.id/2015/04/kasus-illegal-acces.html

Pristika Handayani, Jurnal Hukum: "*Penegakan Hukum terhadap Kejahatan Teknologi Informasi".*

http://kriminalitas.com/khawatir-dengan-cyber-crime-obama-naikkan-anggaran-keamanan-cyber/.

http://elsam.or.id/2017/05/kebutuhan-akan-uu-perlindungan-data-pribadi-kian-mendesak/.