BAB IV

KENDALA PEMERINTAH INDONESIA DALAM PENANGGULANGAN KEJAHATAN *CYBERCRIME*

Kebijakan-kebijakan pemerintah dibuat untuk mendukung tercapainnya kepentingan nasional sesuai dengan amanah Undang-Undang 1945 bertujuan untuk mensejahterakan kehidupan rakyat banyak dan mencerdaskan kehidupan berbangsa. Kesejahteraan dicapai dengan memanfaatkan dan mengelola sumber daya alam baik pertambangan, kekayaan laut dan pertanian hasil bumi Indonesia, sehingga kualitas sumber daya manusia Indonesia bisa bersaing dalam dunia kerja dan global.

Seiring dengan perkembangan zaman, pesatnya kemajuan teknologi informasi terutama internet yang sangat berperan penting untuk kehidupan manusia seperti halnya Negara Indonesia yang masuk dalam salah satu masyarakat dunia tentunya tidak bisa lepas dari penggunaan fasilitas internet untuk menunjang komunikasi, perbankan dan perdagangan *online (e-commerce*), dengan fakta tersebut maka diperlukan kebijakan-kebijakan yang dapat menunjang dan melindungi penggunaan fasilitas teknologi internet di Indonesia, agar mendapatkan jaminan keamanaan. Namun disamping itu semua semenjak diberlakukanya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang diharapkan dapat memberikan jaminan keamanan bagi penggunaan teknologi informasi dan komunikasi tingkat kejahatan dunia maya (*cyber crime*) di Indonesia masih tinggi dan rawan akan serangan dunia maya baik dari dalam maupun luar negeri.

Hal ini dibuktikan dengan adanya laporan Berdasarkan data dari *Norton Report* tahun 2013, tingkat potensi dan resiko tindak kejahatan *cyber* di Indonesia sudah memasuki status darurat. Diungkapkan terdapat sekitar 400 juta korban kejahatan *cyber* di Indonesia tiap tahunya dengan kerugian finansial mencapai USD 113 Miliar, sementara menurut hasil riset yang dirilis oleh Indonesia *Security Response Team*, di tahun 2011 lalu saja tercatat kurang lebih 1 juta serangan *cyber* yang ditujukan para pengguna internet di Indonesia tiap harinya. Mayoritas serangan tersebut hadir dalam bentuk *malware* ataupun *phisisng* dan

lebih menyasar pada institusi perbankan dan pemerintah. Kejahatan teknologi juga bisa dirasakan dengan adanya SMS penipuan yang menawarkan berbagai macam Hadiah baik berupa uang tunai dan barang. Modus yang digunakan oleh sindikat tersebut berpura-pura sebagai petugas bank yang menghubungi ke sejumlah pemilik nomor telpon nasabah bank tertentu untuk menawarkan hadiah undian. Berdasarkan pengungkapan kasus penipuan SMS tersebut pihak kepolisian telah mengamankan berbagai macam barang bukti seperti telpon seluler, komputer/laptop, modem dan alat komunikasi lainnya. Pada bab ini akan menjelaskan berbagai macam kendala-kendala yang dialami oleh penegak hukum indonesia dalam mengungkap kasus kejahatan dunia maya. Pada bab ini juga akan membandingkan hukum kejahatan dunia maya *cyberlaw* antara Indonesia dengan berbagai Negara didunia yang sudah lebih dulu membuat *cyber law security*.

A. 1 Upaya Pemerintah Indonesia Dalam Menaggulangi *Cyber Crime*

Serangan dunia maya *cyber attack* dapat terjadi kapan saja dan dimana saja, termasuk salah satunya adalah Negara Indonesia. Pemerintah Indonesia sudah melakukan langkah-langkah dalam upaya untuk menangani kejahatan dunia maya yang menggunakan teknologi sebagai tindak kejahatan. Namun perlu kita sadari bahwa perangkat hukum perundang-undangan juga harus disesuaikan dengan jenis kejahatannya, Maka dari itu pada tahun 2008. Pemerintah Indonesia telah memberlakukan undang-undang khusus untuk menangani kejahatan dunia maya yang dikenal dengan Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE) 2008.

Undang undang tersebut diharapkan bisa dan mampu untuk melindungi masyarakat, dari ancaman dunia maya yang disebabkan oleh teknologi, sehingga akan memberikan jaminan keamanan bagi pengguna teknologi informasi dan komunikasi. Disamping itu juga, undang undang ini akan mampu untuk menjerat pelaku kejahatan dunia maya seperti penipuan kartu kredit, pembobolan kartu ATM, pornografi, pelanggaran hak cipta dan kejahatan lainya yang menggunakan teknologi informasi. Walaupun undang-undang tersebut sudah resmi disahkan, pada sisi lain ternyata tidak sebanding dengan sumber daya manusia. Hal yang dimaksud adalah para aparatur penegak hukum yang mengerti akan hukum mayantara *(cyber*) dan juga terbatasnya jumlah para tenaga ahli teknologi informasi seperti di instansi Polri. Berdasarkan fakta dari hasil statistik yang diperoleh oleh penulis,

tingkat serangan *cyber* dari dan ke Indonesia semakin lama semakin meningkat. Hasil penelitian yang dilakukan oleh Dimitri Mahayana, direktur dari lembaga riset Telematika Sharing Vision yang melakukan penelitian pada tahun 2013 menyatakan bahwa Indonesia bisa mendapat 42.000 serangan di dunia maya per hari. Hal ini cenderung dapat merongrong keamanan perusahaan dan Negara. Ia mengatakan data tersebut menunjukan adanya kerentanan yang perlu diperbaiki, diantaranya melalui penegakan hukum, regulasi undang-undang, dan pembentukan badan khusus yang memntau pergerakan jalur internet atau pasukan *cyber*. Badan khusus yang dimaksud 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 memangani 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.

A. 2 Kendala Pemerintah Indonesia Dalam Menaggulangi *Cyber Crime*

Pada sub bab ini penulis mencoba mendapatkan keterangan dan informasi dari narasumber yang dinilai oleh penulis cukup paham dan ahli dalam bidang IT (*Information Technology*). Penulis mencoba untuk mencari informasi kendala-kendala apa sajakah yang menjadi penghambat untuk penanggulangan *cybercrime* di Indonesia, Pada tahap ini penulis telah menghimpun informasi dari 2 orang narasumber yang pertama adalah Teguh Arifiyadi adalah seorang praktisi dalam bidang IT dan juga ketua umum dari ICLC (*Indonesia Cyber Law Community*) dan kemudian narasumber yang kedua adalah Lukito Edi Nugroho seorang praktisi dan dosen pengajar Jurusan Teknik Elektro Dan Teknologi Informasi Fakultas Teknik Universitas Gadjah Mada. Wawancara dilakukan dengan media elektronik seperti via *facebook* dan *e-mail*. Selain menggunakan metode wawancara *(interview*) dengan para narasumber yang ahli dalam bidang IT (Informasi Teknologi).

Penulis juga mengumpulkan informasi dari kutipan-kutipan situs berita *online* yang memuat tentang apa saja kendala-kendala yang terjadi di indonesia dalam mengungkap kasus kejahatan dunia maya seperti pembobolan kartu kredit nasabah, pencurian data, pencemaran nama baik SARA dan lainya. Pembahasan mengenai kendala dan faktor penghambat dalam bab ini akan disajikan dalam berbagai point untuk memdudahkan pemahaman permasalahan.

B. Kendala Polri Dalam Menaggulangi *Cyber Crime*

Berbicara Mengenai Kendala keterbatasan personil seperti tenaga ahli IT dan *cyber forensic*, fakta ini juga diperkuat oleh laporan dari Wakil Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri Kombes (Pol) Agung Setya. Beberapa waktu lalu kami bertemu dengan pihak polisi china, bekerjasama tentang kejahatan siber. Mereka menggeleng-gelengkan kepala begitu tahu penyidik *cybercrime* Indonesia hanya berjumlah 18 orang, sedangkan jumlah anggota polisis *cyber* di Negara china mencapai 18.000 (delapan belas ribu) orang personil. Agung merasa jumlah personil yang membidangi kejahatan siber di indonesia memang kurang.

Padahal kejahatan jenis ini meningkat pada tahun-tahun terakhir, seharusnya penebalan personil untuk mengantisipasi efek negatif kejahatan ini dilaksanakan segera Disamping itu Subdirektorat *cybercrime* yang bernaung di direktoratnya mencatat, jumlah laporan kejahatan siber pada tahun 2012 hanya 781 laporan. Dari jumlah tersebut, hanya 86 laporan yang berhasil diselesaikan. Tahun 2013 jumlah laporanya melonjak menjadi 1.347 laporan dengan penyelesaian laporan 115 saja. Adapun tahun 2014, terdapat 1.324 laporan dengan penyelesaian perkara sebanyak 307, sementara sepanjang januari hingga oktober 2015, terdapat 1.325 laporan dengan jumlah perkara yang diselesaikan sebanyak 355. Agung mengapresiasi rencana pemerintah untuk membentuk badan *cyber* nasional. Dia hanya berharap pembentukan badan tersebut turut mengikutsertakan kepolisisan sebagai unsur yang penting[1].

---

[1] http://nasional.kompas.com/read/2015/12/19/19450071/Polisi.Cyber.Crime.RI.Cuma.18.Personel.Polisi.China.Geleng-geleng.Kepala (diakses pada 25 april 2016)

B. 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.

Keterbatsan 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. Terlebih lagi diketahui bahwa jumlah anggota *cyber police* Indonesia hanya berjumlah 18 orang, jumlah tersebut tidak sebanding dengan banyaknya kasus yang masuk dalam laporan kepolisisan tentang kejahatan dunia maya, yang paling marak ialah kejahatan perbankan.

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. Keterbatasan personil yang ahli juga memang diakui oleh Teguh Arifiyanto ketua umum ICLC (*Indonesia Cyber Law Community*) yang juga sering ikut terjun langsung dilapangan bekerjasama dengan polri dalam mengungkap kasus kejahatan dunia maya, selain pihak kepolisisan pihak lain yang ikut membantu adalah

Kementrian Komunikasi Dan Informasi (KOMINFO) yang mana memang terkait langsung pada kebijakan penggunaan fasilitas teknologi informasi dan internet di Indonesia. Dari informasi yang didapat penulis anggota kepolisian masih belum terlalu melek akan teknologi, bahkan banyak diantara anggota *cyber police* Indonesia masih baru memakai computer. Bisa dikatakan kemampuan polisis indonesiadalam 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 IT.

Para praktisi juga bisa memebrikan peran penting dalam memberikan masukan-masukan kepada pihak pemerintah dalam keamanan jaringan computer 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

B. 2 Terbatasnya Anggaran Operasional

Kendala lain yang krusial adalah terbatasnya dana anggaran operasional, penulis mengutip pernyataan dari Direktur Tindak Pidana Ekonomi Khusus (Tipideksus) Barskrim Brigjen Pol A Kamil Razak, masalah yang cukup krusial selain perangkat hukum, yaitu SDM yang belum mencukupi, anggaran serta sarana dan prasarana untuk menunjang pengungkapan kasus-kasus *cyber crime*. Sekarang ini anggaran yang ada hanya cukup untuk satu perkara per satu bulan. Padahal kenyataanya satu bulan bisa sampai 15 kasus[2].

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 mengahruskan pemerintah Amerika Serikat karena menambah anggaran yang cukup besar tersebut disebabkan oleh

[2] http://news.detik.com/berita/2714416/penanganan-kasus-cyber-crime-terganjal-regulasi-dan-anggaran (diakses pada tanggal 9 mei 2016)

ancaman dunia maya (*cyber*) di Amerika Serikat juga angat meningkat tajam. Pemerintah amerka serikat dibawah kordinasi langsung presiden barack obama peningkatan anggaran untuk keamanan cyber di amerka tidak lepas dari berbagai ancaman-ancaman yang cukup besar terutama yang datang dari luar Negara amerika, selain ancaman pencurian data intelejen, pencurian data diri warga sipil Amerika dan perbankan, ancaman yang paling serius ialah *cyber terrorism*.

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 satya 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 Presiden Amerika serikat Barack Obama juga bisa diterapkan di Indoensia 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.

B.3 Lemahnya Pengawasan Pemerintah

Lemahnya pengawasan penggunaan internet berpotensi besar akan menciptakan peluang terjadinya kejahatan *cyber crime* (dunia maya). Karena kejahatan dengan

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

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.[4]

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*).

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

[4] Wawancara teguh arifiyadi 4 mei 2016

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.

B.4 Kendala Prosedural Hukum UU ITE 2008

Maraknya kasus kejahatan dunia maya di Indonesia dinilai banyak kalangan terdapat adanya celah hukum yang ada di indonesia yang dapat dimanfaatkan oleh pelaku kejahatan dunia maya, dari data laporan serangan dunia maya yang telah dicantumkan oleh penulis pada bab 2 penulis juga mencari informasi dari narasumber yaitu Bapak Lukito Edi Nuigroho yang merupakan dosen di Fakultas Teknik Jurusan Teknik Informatika Universitas Gadjah Mada Yogyakarta Beliau berpendapat bahwa Undang-Undang Informasi Dan Transaksi Elektronik No 11 Tahun 2008 (UU ITE 2008) masih belum diterapkan secara efektif. Dikarenakan 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 dunia maya memang rawan penerobosan dan potensi keuntungan yang bisa diperoleh dari kejahatan tersebut juga luar biasa besar[5]. 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. 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.

[5] Wawancara Lukito Edi Nugroho Yogyakarta 8-mei 2016

Hal senada juga disampaikan oleh teguh arifiyadi. Lemahnya perangkat hukum UU ITE 2008 dipastikan teekndala 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.

Pasal ini sering kali dikeluhkan sebab penindakan terhadap pelaku hanya bisa dilakukan jika sudah mendapat izin dari kantor pengadilan setempat, pasal ini dinilai kurang efektif karena kantor pengadilan hanya buka pada 5 hari kerja seangkan pada hari sabtu dan minggu kantor pengadilan akan tutup, jika seandainya pelaku yang terduga kuat tidak segara ditindak maka akan dikhawatirkan akan menghilangkan barang bukti berupa jejak kejahatan. Jika barang bukti tidak ditemukan maka pelaku tidak dapat dijerat secara hukum sesuai dengan perundang-undangan yang berlaku, pasal 43 ayat 3 tersebut perlu diadakanya revisi. Sebagai pebandingan pihak otoritas *cyber police* singapura berhak menahan pelaku yang terduga kuat sebagai pelaku kejahatan dunia maya tanpa harus terlebih dahulu mengantongi suart izin penahanan dari kantor pengadilan.

Langkah ini dilakukan untuk menghindari hilangnya barang bukti yang digunakan oleh pelaku dalam menjalankan aksinya. 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 menagdakan 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*.

Menyangkut anggaran juga tidak kalah pentingnya untuk dibahas, sebab dengan anggaran yang cukum maka pihak penegak hukum akan mampu memiliki peralatan yang memadai baik untuk memantau maupun melacak para pelaku kejahatan cyber, dengan anggaran yang cukup juga kasus-kasus dunia maya juga akan semakin banyak bisa ditangani dengan cepat sehingga akan dapat membrikan rasa aman bagi para pengguna. Kemudian dalam pengawasan pemerintah masih cenderung kurang dalam pengawasan dikarenakan penyedia jasa internet atau ISP 95 % masih sepenuhnya diekendalikan pihak swasta dalam undang-undang ITE pasal 13 sampai 16 hanya menitikberatkan pada sertifikasi penyelenggaran jasa elektronik tanpa menacantumkan pengawasan dan pembatasan pengguna internet. Adapun untuk lebih memperjelas isi dari UU ITE 2008 pasal 13 sampai 16 adalah sebagai berikut.

BAB IV
PENYELENGGARAAN SERTIFIKASI ELEKTRONIK DAN SISTEM ELEKTRONIK

Bagian Kesatu
Penyelenggaraan Sertifikasi Elektronik

Pasal 13

(1) Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.

(2) Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.

(3) Penyelenggara Sertifikasi Elektronik terdiri atas:

a. Penyelenggara Sertifikasi Elektronik Indonesia; dan

b. Penyelenggara Sertifikasi Elektronik asing.

(4) Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.

(5) Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.

(6) Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 14

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:

a. metode yang digunakan untuk mengidentifikasi Penanda Tangan;

b. hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik; dan

c. hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Bagian Kedua

Penyelenggaraan Sistem Elektronik

Pasal 15

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 16

(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

(2) Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Dengan adanya aturan perundang-undangan mengenai pembatasan penggunaan internet dan memperketat pemasangan jaringan koneksi internet hal ini merupakan langkah preventif bagi pemerintah dalam pengawasan penggunaan internet di indonesia sehingga akan meminimalisir penyalahgunaan jaringan internet (*internet misue*).

Kendala prosedural juga dinilai sebagai terhambatnya penindakan hukum bagi pelaku yang terduga kuat sebagai pelaku kejahatan dunia maya pasal 43 ayat 3 merupakan batu sandungan, pasal ini mengharuskan penegak hukum harus mengantongi suart izin penahandari pengadilan setempat, langjah ini kurang repat karena akan memberikan waktu kepada pelaku untuk menghilangkan barang bukti, perlu adanya revisi pada pasal tersebut agar memudahkan pengak hukum mengadili dan mengamankan pelaku kejahatan dunia maya. Adapun bunyi pada pasal 43 ayat 3 adalah sebagai berikut

(3) Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.

Demikianlah beberapa celah dalam perundang-undangan ITE tahun 2008 yang sering menjadi kendala prosedural bagi pihak penegak hukum.