KAJIAN YURIDIS PEMBUKTIAN KEJAHATAN MAYANTARA *(CYBERCRIME)* DALAM LINGKUP TRANSNASIONAL
(Studi Putusan)

JURNAL

Diajukan untuk Memenuhi dan Melengkapi Syarat-Syarat untuk Memperoleh Gelar Sarjana Hukum Universitas Sumatera Utara

O L E H :

EVI LESTARI SITUMORANG
100200120

Departemen Hukum Pidana

FAKULTAS HUKUM
UNIVERSITAS SUMATERA UTARA
MEDAN
2014

KAJIAN YURIDIS PEMBUKTIAN KEJAHATAN MAYANTARA *(CYBERCRIME)* DALAM LINGKUP TRANSNASIONAL
(Studi Putusan)

JURNAL
Disusun dan Diajukan untuk Melengkapi Persyaratan Memperoleh Gelar Sarjana Hukum pada Fakultas Hukum Universitas Sumatera Utara

Oleh :

EVI LESTARI SITUMORANG
100200120

Departemen Hukum Pidana

Disetujui oleh :
Ketua Departemen Hukum Pidana

Dr. M Hamdan, SH., M.H
NIP : 195703261986011001

Editor

Prof. Dr. Ediwarman, SH., M.Hum.
NIP : 195405251981031003

FAKULTAS HUKUM
UNIVERSITAS SUMATERA UTARA
2014

ABSTRAK

Evi Lestari Situmorang*

Kejahatan mayantara *(cybercrime)* merupakan kejahatan yang terjadi di dunia maya *(cyberspace)* yang tidak mengenal batas yurisdiksi serta penggunaan internet oleh siapa saja dan kapan saja saja di seluruh dunia. Sehingga dapat digolongkan bahwa kejahatan mayantara *(cybercrime)* termasuk kejahatan transnasional. Oleh karena sifatnya yang transnasional, pembuktian kejahatan mayantara *(cybercrime)* juga menjadi hal yang membutuhkan perhatian bagi negara Indonesia dalam rangka penegakan hukum serta menentukan yurisdiksi kejahatan transanasional ini sesuai Hukum Acara yang berlaku di Indonesia. Berdasarkan latar belakang di atas diangkatlah beberapa permasalahan yaitu: bagaimanakah eksistensi kejahatan mayantara (*cybercrime*), bagaimanakah kejahatan mayantara (*cybercrime*) dalam hukum pidana positif di Indonesia, serta bagaimanakah pembuktian kejahatan mayantara (*cybercrime*) dalam lingkup transnasional.

Penelitian skripsi ini merupakan penelitian hukum normatif atau penelitian yuridis normatif yaitu penelitian ilmiah untuk menemukan kebenaran berdasarkan logika keilmuan hukum dari sisi normatifnya. Penelitian ini menitikberatkan pemakaian bahan pustaka dan data sekunder. Data sekunder tersebut terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tertier.

Pembuktian kejahatan mayantara *(cybercrime)* dalam lingkup transnasional yang terjadi di Indonesia menggunakan sistem pembuktian berdasarkan undang-undang secara negatif. Diakuinya alat bukti elektronik sebagai alat bukti yang sah dalam hukum acara Indonesia telah diatur pula di beberapa undang-undang. Munculnya kejahatan mayantara *(cybercrime)* ini disebabkan oleh faktor kesadaran hukum masyarakat yang kurang, faktor keamanan pelaku dalam melakukan kejahatan, faktor budaya hukum, dan masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam hal *cybercrime*, serta peraturan perundang-undangan yang belum berlaku secara efektif dalam menanggulangi kejahatan tersebut. Kebijakan penanggulangan kejahatan ini dapat ditempuh dengan pendekatan penal dan non penal.

* Penulis, Mahasiswi Departemen Hukum Pidana Universitas Sumatera Utara.

A. PENDAHULUAN

Kini lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum teknologi informasi (*law of information technology)*, hukum dunia maya *(virtual world law)*, dan hukum mayantara.[2]

Dengan kemajuan teknologi informasi ini, masyarakat memiliki ruang gerak yang lebih luas. Aktivitas manusia yang semula bersifat nasional telah berubah menjadi internasional. Sehingga wajarlah apabila *cybercrime* dimasukkan ke dalam jenis kejahatan yang sifatnya internasional berdasarkan *United Nation Convention Against Transnational Organized Crime (Palermo Convention)* Nopember 2000 dan berdasarkan Deklarasi ASEAN tanggal 20 Desember 1997 di Manila.[3]

Kenyataannya, hal yang berkaitan dengan pemanfaatan teknologi informasi tidak lagi dapat dilakukan pendekatan melalui sistem hukum konvensional, mengingat kegiatannya tidak bisa dibatasi teritorial suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun misalnya dalam pencurian dana kartu kredit melalui pembelanjaan di internet.

Seringkali penegak hukum di Indonesia mengalami kesulitan saat menjerat pelaku karena masalah pembuktian *(documentary evidence)* yang tidak memenuhi ketentuan sistem hukum pidana Indonesia. Sementara upaya penjeratan terhadap pelaku-pelaku kejahatan mayantara (*cybercrime)* harus tetap dilakukan, upaya perluasan alat bukti menjadi solusi untuk menegakkan hukum.[4]

Pembuktian kejahatan mayantara dalam sistem peradilan pidana Indonesia menjadi topik penting, terlebih dengan ditetapkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam undang-undang ini terjadi perluasan alat bukti dari yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Pengaturan alat bukti harus didasarkan pada sistem dan prinsip pembuktian hukum acara pidana yang berlaku di Indonesia.

Dapat dilihat bahwa kejahatan mayantara (*cybercrime)* ini tidak mengenal batas wilayah serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. Semua aksi itu dapat dilakukan hanya dari depan komputer yang memiliki akses internet tanpa takut diketahui oleh orang lain/saksi mata, sehingga kejahatan ini termasuk dalam *transnational crime*/kejahatan antar negara yang pengungkapannya sering melibatkan penegak hukum lebih dari satu negara. Mencermati hal tersebut dapatlah disepakati bahwa c*ybercrime* memiliki karakter

---

[2]Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)*, Jakarta ; RajaGrafindo Persada, 2012, halaman. 2.

[3]M.A. Erwin MAP, *Kejahatan Transnasional (Transnational Crime)*, Markas Besar Kepolisian Negara Republik Indonesia, Badan Reserse Kriminal, Jakarta, Desember 2002.

[4] M. Arief Mansur dan Elisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informasi*, Bandung ; Refika Aditama, 2005, halaman. 100.

yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara.

Oleh karena itu sistem pembuktian di era teknologi informasi sekarang ini menghadapi tantangan yang besar dan perlu penanganan serius, khususnya dalam upaya pemberantasan kejahatan di dunia maya *(cybercrime)*. Untuk dapat melakukan pembahasan yang mendalam mengenai masalah ini maka perlu dilakukan penelitian yang mendalam agar memberi gambaran yang jelas dalam hal pembuktian kejahatan mayantara (*cybercrime*) baik yang diatur dalam hukum acara pidana Indonesia maupun pembuktian serta kajian yurisdiksi dalam lingkup transnasional.

Oleh karena itu, penulis tertarik untuk mengetahui hal tersebut lebih jauh sehingga berdasarkan latar belakang di atas maka dilakukan penelitian dengan judul :

"KAJIAN YURIDIS PEMBUKTIAN KEJAHATAN MAYANTARA (*CYBERCRIME*) DALAM LINGKUP TRANSNASIONAL (Studi Putusan)"

B. PERMASALAHAN

1. Bagaimanakah Pengaturan Hukum Pembuktian Kejahatan Mayantara *(Cybercrime)* dalam Lingkup Transnasional?
2. Apakah Faktor Penyebab Terjadinya Kejahatan Mayantara *(Cybercrime)* dalam Lingkup Transnasional di Indonesia?
3. Bagaimanakah Kebijakan Penanggulangan Kejahatan Mayantara (*Cybercrime*) dalam Lingkup Transnasional?

C. METODE PENELITIAN

Metode yang digunakan adalah metode penelitian normatif yang merupakan prosedur penelitian ilmiah untuk menemukan kebenaran berdasarkan logika keilmuan hukum dari sisi normatifnya. Penelitian ini menitikberatkan pemakaian bahan pustaka dan data sekunder. Data sekunder tersebut terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tertier. Bahan hukum primer diperoleh melalui Kitab Undang-undang Hukum Pidana, Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan peraturan lain yang terkait. Bahan hukum sekunder adalah semua dokumen yang merupakan informasi, atau kajian yang berkaitan dengan penelitian ini, yaitu seminar-seminar, jurnal-jurnal hukum, majalah-majalah, artikel-artikel, karya tulis ilmiah, dan beberapa sumber dari internet dan bahan hukum tertier adalah bahan hukum yang memberikan petunjuk atau penjelasan bermakna terhadap bahan hukum primer dan sekunder seperti kamus dan ensiklopedia yang relevan.

D. HASIL PENELITIAN

1. Pengaturan Hukum Pembuktian Kejahatan Mayantara *(Cybercrime)* Dalam Lingkup Transnasional

A. *Convention on Cybercrime*

Instrumen hukum internasional yang mengatur masalah kejahatan mayantara *(cybercrime)* yang saat ini paling mendapat perhatian adalah *Convention on Cyber Crime* 2001 yang digagas Uni Eropa. Konvensi ini dibentuk dengan pertimbangan-pertimbangan, antara lain: *Pertama*, bahwa masyarakat internasional menyadari perlunya kerjasama antarnegara dan industri dalam memerangi kejahatan siber dan adanya kebutuhan untuk melindungi kepentingan yang sah di dalam penggunaan dan pengembangan teknologi informasi. *Kedua*, konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. *Ketiga*, saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak asasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Asasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil. Konvensi ini telah disepakati oleh Uni Eropa sebagai konvensi yang terbuka untuk diaksesi oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrumen Hukum Internasional dalam mengatasi kejahatan siber, tanpa mengurangi kesempatan setiap individu untuk tetap mengembangkan kreativitasnya dalam mengembangkan teknologi informasi.[5]

Dalam konvensi ini diatur pula hukum acara/formil bahwa negara anggota harus menerapkan undang-undang dan pendekatan-pendekatan lain yang diperlukan untuk membentuk kewenangan-kewenangan serta prosedur pelaksanaannya untuk tujuan penyidikan tindak pidana yang spesifik. Kewenangan dan prosedur yang dimaksud adalah pada tindak pidana sebagai mana yang disebutkan dalam jenis-jenis *cybercrime* diatas, tindak pidana yang dilakukan melalui sistem komputer, dan pengumpulan bukti elektronik dari suatu tindak pidana (Pasal 14 CoC).

Dalam konvensi ini diatur pula mengenai kerjasama internasional yang mencakup ekstradisi, bantuan timbal balik dan informasi spontan, prosedur-prosedur tentang permintaan bantuan timbal balik dengan tidak adanya perjanjian-perjanjian internasional yang berlaku, dan kerahasiaan dan pembatasan penggunaan, sampai pada jangkauan yang selebar mungkin untuk tujuan penyidikan atau proses-proses mengenai pelanggaran-pelanggaran yang berhubungan dengan sistem dan data komputer, atau untuk pengumpulan data dalam bentuk elektronik dari sebuah pelanggaran (Pasal 23 CoC).

B. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Dua muatan besar yang diatur dalam UU ITE ialah mengenai pengaturan tranksaksi elekronik dan mengenai tindak pidana siber. Materi UU ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional. Pada UU ITE dimuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. Pada pasal 42 UU ITE diatur pula mengenai ketentuan penyidikan yang berbunyi : "penyidikan sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam undang-

[5] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*, Jakarta; Tatanusa, 2012, halaman. 79.

undang ini". Dengan demikian, sistem pembuktian yang dianut adalah sistem/teori pembuktian berdasar undang-undang secara negatif, yaitu sistem yang dianut dalam KUHAP dan berdasar Pasal 183 KUHAP, yang berbunyi sebagai berikut: "hakim tidak boleh menjatuhkan pidana kepada sesorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yangsah ia memperoleh keyakinan bajwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya". Dengan demikian, artinya pembuktian harus didasarkan ketentuan undang-undang, yakni alat bukti yang sah yang diatur dalam Pasal 184 KUHAP disertai keyakinan hakim yang diperoleh dari alat-alat bukti tersebut.

Berikut beberapa alat bukti yang diatur dalam Pasal 184 KUHAP sebagai acuan dalam pembuktian kejahatan mayantara *(cybercrime)*, yaitu:

1. Keterangan saksi

Syarat formal keterangan saksi yang diatur dalam KUHAP ialah, antara lain, dinyatakan di persidangan dan mengucapkan sumpah atau janji sebelum saksi memberikan keterangan. Sedangkan syarat materiil untuk keterangan saksi antara lain: (1) keterangan yang diberikan ialah mengenai peristiwa yang ia dengar, lihat, dan alami sendiri dengan menyebutkan alasan pengetahuannya; (2) bukan pendapat, rekaan, maupun keterangan ahli; (3) ada lebih dari satu orang saksi yang sesuai asas *unus testis nullus testis*; (4) bukan keterangan yang dia peroleh dari orang lain *(testimonium de auditu)*; dan (5) adanya persesuaian antara keterangan saksi yang satu dengan yang lain dan keterangan saksi yang satu dengan alat bukti yang lain.[6]

Pada kasus *cybercrime*, dikarenakan sifatnya yang virtual, maka pembuktian dengan menggunakan keterangan saksi tidak dapat diperoleh secara langsung. Keterangan saksi hanya dapat berupa hasil pembicaraan atau hanya mendengar orang lain. Kesaksian ini dikenal dengan *testimonium de auditum* atau *hearsay evidence*, meskipun kesaksian sejenis ini tidak diperkenakan sebagai alat bukti, akan tetapi dalam praktiknya tetap dapat dipergunakan sebagai bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan. Kemungkinan yang dapat dijadikan keterangan saksi ialah melalui hasil interaksi dalam dunia *cyber*, seperti *chatting* dan *e-mail* antara pengguna internet, atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi.[7]

2. Keterangan ahli

Dalam Pasal 186 KUHAP diatur mengenai syarat formil keterangan ahli bahwa keterangan ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Yang disebut sebagai ahli ialah ahli kedokteran kehakiman dan ahli lainnya. Keterangan ahli menjadi signifikan penggunaannya jika jaksa mengajukan alat bukti elektronik untuk membuktikan kesalahan pelaku *cybercrime*. Peran keterangan ahli disini adalah untuk memberikan suatu penjelasan dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum.

3. Alat bukti surat (Pasal 184 huruf c dan Pasal 187 KUHAP)

---

[6] *Ibid.* halaman.266.

[7] Dikdik M. Arief Mansur dan Elisatris Gultom, *Op.cit,* halaman. 116.

Jenis surat yang diakui berdasarkan alat bukti ialah surat yang dibuat diatas sumpah jabatan atau dikuatkan dengan sumpah sebagaimana yang tertuang dalam pasal 187 KUHAP.

"Surat" dalam kasus *cybercrime* mengalami perubahan dari bentuknya yang tertulis menjadi tidak tertulis dan bersifat *on-line*. Alat bukti dalam komputer yang telah disertifikasi ada dua kategori. *Pertama*, bila sebuah sistem komputer yang telah disertifikasi oleh badan yang berwenang, maka hasil *print out* komputer dapat dipercaya keotentikannya. Contohnya *receipt* yang dikeluarkan oleh suatu bank dalam transaksi ATM. Alat bukti ini mempunyai kekuatan pembuktian meskipun dalam persidangan dibutuhkan keterangan lebih lanjut. *Kedua*, bukti sertifikasi dari badan yang berwenang tersebut dapat dikategorikan sebagai bukti surat, karena dibuat oleh dan atau pejabat yang berwenang. Jenis alat bukti surat lainnya dapat berupa bukti elektronik yang dapat dicetak atau *print out* dan surat yang terpampang dalam layar monitor sebuah jaringan komputer. Selama kedua bukti ini dikeluarkan/dibuat oleh yang berwenang dalam sebuah sistem jaringan komputer dan sebuah sistem jaringan komputer tersebut dapat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP.[8]

4. Alat bukti petunjuk (Pasal 184 (1) huruf d dan Pasal 188 KUHAP)

KUHAP mengatur secara limitatif mengenai sumber petunjuk, yaitu bahwa petunnjuk hanya dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa. Untuk dapat dijadikan sumber petunjuk, ketiga alat bukti tersebut harus sah, dan oleh karena itu, petunjuk yang dihasilkan juga menjadi sah.[9]

Dalam *cybercrime*, pengumpulan alat bukti secara fisik akan sulit dipenuhi. Yang paling mudah dalam melakukan pengumpulan bukti-bukti adalah mencari petunjuk-petunjuk yang mengindikasi telah adanya suatu niat jahat berupa akses secara tidak sah. Misalnya dengan melihat dan mendengarkan keterangan saksi di pengadilan, atau surat elektronik atau hasil *print out* data, atau juga dari keterangan terdakwa di pengadilan.[10]

5. Keterangan terdakwa (Pasal 184 huruf e dan Pasal 189 KUHAP)

Keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri.[11] Agar keterangan terdakwa dapat dinyatakan sah, syarat formil – yaitu dinyatakan di sidang – dan syarat materiil – keterangan tersebut tentang perbuatan yang terdakwa lakukan atau ketahui atau alami sendiri – harus dipenuhi.

Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pasal 5 ayat 1 dan 2 mendeskripsikan bahwa Dokumen Elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. 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 :

---

[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.* halaman. 119.
[11] Pasal 189 ayat (2).

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan;
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).

Informasi Elektronik dan Dokumen Elektronik dapat dijadikan sebagai alat bukti yang sah menurut undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah sebagaimana dimaksud Pasal 184 ayat (1) KUHAP. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik[12] sesuai ketentuan yang diatur dalam UU ITE.

C. Undang-Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

Kemajuan teknologi dan informasi saat ini dapat dijadikan medium bagi pelaku tindak pidana korupsi untuk menyembunyikan perbuatan atau hasil kejahatannya. Unsur utama tindak pidana korupsi yang berkaitan dengan teknologi informasi adalah "memperkaya diri sendiri atau orang lain atau korporasi" secara melawan hukum yang merugikan keuangan negara atau perekonomian negara. Misalnya, ada orang yang dalam sehari dapat membobol bank sebanyak lima miliar, yang kemudian memindahkan ke rekening pribadinya dan sudah dilakukan beberapa kali belum ketahuan. (www.hukumonline.com)

Dalam UU PTPK data elektronik *(electronic record)* diakui sebagai alat bukti (Pasal 26A UU No.20/2001 jo. UU No.31/1999), namun bukan sebagai alat bukti yang berdiri sendiri di samping alat bukti petunjuk yang dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa (Pasal 188 ayat (2) KUHAP).[13] Berdasarkan KUHAP, alat bukti petunjuk hanya dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa. Tetapi, menurut Undang-Undang No. 20 Tahun 2001, bukti petunjuk juga dapat diperoleh dari alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu tetapi tidak terbatas pada data penghubung elektronik *(electronic data interchange)*, surat elektronik *(email)*, telegram, teleks, faksimili, dan dari dokumen, yakni setiap rekaman data atau informasi yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

D. Undang-Undang No. 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang

Kemajuan teknologi semakin canggih, misalnya dengan adanya *online banking*, *money laundering* dapat dilakukan dari dan ke berbagai belahan dunia dengan mudah, cepat dan dalam waktu yang relatif singkat. *Money laundering*

---

[12] Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

[13] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Bandung ; Refika Aditama, 2012. halaman. 188.

melalui internet *(cyberlaundering)* menjadi sangat efektif dan efisien tanpa harus adanya mobilitas orang sebagaimana dilakukan mafia di Amerika Serikat ketika awal perkembangan *money laundering*.[14]

Undang-undang ini dibentuk dimaksudkan untuk mencakup segala perbuatan yang menggunakan teknologi informasi dan komunikasi. Hal ini didasarkan pada ketentuan umum Pasal 1 angka 16 yang memberikan pengertian mengenai dokumen yang diartikan sebagai data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas atau benda fisik apapun selain kertas maupun yang terekam secara elektronik, termasuk tetapi tidak terbatas pada: a. tulisan, suara, gambar; b. peta, rancangan, foto, atau sejenisnya; c. huruf, tanda, angka, simbol atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya. Pengaturan dokumen dalam UU ini tidak hanya sebagai alat bukti tetapi berlaku untuk setiap ketentuan yang terdapat dalam UU ini.

Undang-undang *money laundering* ini merupakan undang-undang yang paling ampuh bagi seseorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam Pasal 2 angka (1q) Undang-undang pencucian uang. Undang-undang ini mengatur juga mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf (b), yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

E. Undang - Undang No. 21 tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang

Dalam undang-undang ini tidak disebutkan secara ekplisit bahwa tindak pidana itu dapat dilakukan pada dunia maya maupun melalui media internet. Namun dapat ditafsirkan secara ekstensif bahwa tindak pidana ini dapat menggunakan media internet dan dilakukan di dunia maya *(cyberspace)*. Dalam hal inilah sisi mayantara kejahatan ini dapat dilihat, bahwa dalam mempersiapkan, merencanakan, ataupun melakukan transaksi perdagangan orang secara ilgal dilakukan pada *cyberspace*. Mengacu pada jenis-jenis kejahatan mayantara *(cybercrime)* yang dikemukakan pada *Convention on Cybercrime*, maka tindak pidana perdagangan orang ini termasuk ke dalam pelanggaran yang berhubungan dengan komputer *(computer related offences)*, baik itu dalam hal pemalsuan maupun penipuan untuk memperlancar dilakukannya tindak pidana perdagangan orang tersebut.

Tindak pidana perdagangan orang semakin mudah seiring perkembangan teknologi informasi, khususnya berkaitan dengan perbuatan perekrutan seseorang untuk menjadi korban perdagangan orang (Pasal 2) dan pemalsuan dokumen untuk memudahkan tindak pidana perdagangan orang (Pasal 19) atau menyampaikan alat bukti palsu dalam sidang pengadilan (Pasal 20). Selain itu,

[14] *Ibid*. halaman 190.

dalam undang-undang ini juga diakui alat bukti lain di luar yang diatur dalam Pasal 184 KUHAP, yang terdapat pada Pasal 29.

F. Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

UU Terorisme mengakui keberadaan alat bukti elektronik, Pasal 27 UU Terorisme mengatur bahwa alat bukti pemeriksaan tindak pidana terorisme dan alat bukti elektronik sebagai alat bukti keenam. Alat bukti elektronik menurut undang-undang ini terdiri dari 2 jenis, yaitu:[15]

1. alat bukti elektronik yang menggunakan alat optik atau serupa dengan itu. UU Terorisme dengan tegas mengatakan bahwa alat bukti elektronik terebut dikategorikan sebagai alat bukti lain, yang tidak termasuk alat bukti yang diatur dalam KUHAP.
2. alat bukti elektronik berupa data, rekaman, atau informasi. Walaupun tidak diatur secara tegas sebagai alat bukti lain, alat bukti ini tetap dikategorikan sebagai alat bukti lain karena pada esensinya sama dengan poin 1 di atas.

Berikut pula dikemukakan kasus yang terjadi di Bandung beberapa tahun yang lalu. Kasus yang dibahas ini mengenai pembuktian *cybercrime,* yaitu kasus *carding* Harry Parlindungan Samosir di Bandung.

Kasus posisi *carding* yang dilakukan oleh Harry P. Samosir (Putusan PT Bandung No. 181/PID/2004/PT Bdg) adalah bahwa Harry Parlindungan Samosir pada sekitar tahun 2002 bertempat di Warnet di Jl. Kebon Bibit Utama No.4 Bandung telah berbelanja memesan barang melalui internet yang pembayarannya menggunakan kartu kredit orang lain tanpa seizin pemilik kartu kredit ke sebuah toko di Amerika Serikat. Nomor-nomor kartu kredit orang lain tersebut dapat diperoleh dari *chanel indo carder* atau *jogja carding*. Barang yang dipesan antara lain 1 set stick golf merk VFT, 1 batang stick golf GBBH, 1 stick golf Mizuno, 1 sepeda "Merlin", 4 gitar (3 merk Takamika, 1 merk Eniebel), 2 laptop, 1 *infocus*, 2 *handycam*, 1 sepeda gunung. Barang-barang tersebut kemudian dikirim ke Singapore dengan nomor pengiriman 8399.8394.7749 atas nama Dhanny Chun dan dengan bantuan Omar Syarif yang bekerja sebagai pegawai Nusantara Express dikirim ke Indonesia melalui PT Antar Benua Sukses Mandiri ke PT Nusantara Express atas Pesanan Raka Iswandi dengan alamat Jl.Anggrek IX No.2 Rancaekek Bandung. Nama Raka Iswandi adalah nama palsu Harry P. Samosir di Indonesia. Omar Syarif kemudian menghubungi Harry P. Samosir dan setelah dibayar ongkos kirimnya barang-barang tersebut diambil dan dijual ke pihak lain.

Dakwaan dan Tuntutan:

Atas perbuatan tersebut Jaksa Penunut Umum mendakwa pelaku dengan ketentuan sebagai berikut:

Dakwaan:

Kesatu :

Primair : Pemalsuan Surat (Pasal 263 ayat (1) KUHP)

Subsidair : Menggunakan surat palsu (Pasal 263 ayat (2) KUHP)

Kedua : Pencurian (Pasal 362 KUHP)

[15] Josua Sitompul, *Op.cit*. halaman. 274

Dalam perkara Harry P. Samosir Jaksa Penuntut Umum menuntut bahwa dakwaan kesatu subsidair menggunakan surat palsu (Pasal 263 ayat (2) KUHP dan dakwaan Kedua dinyatakan tidak perlu dibuktikan karena saksi yang dirugikan tidak hadir karena berada di Amerika Serikat. Dalam putusan, Majelis Hakim dalam perkara ini telah memeriksa dengan dimulai dari dakwaan kesatu primair, membuat surat palsu (Pasal 263 ayat (1) KUHP), namun karena tidak cukup bukti Majelis memutus dakwaan kesatu primair tidak terbukti. Kemudian perbuatan Harry P. Samosir, menurut Majelis terbukti melanggar dakwaan kesatu subsidair, menggunakan surat palsu (Pasal 263 ayat (2) KUHP). Majelis hakim selanjutnya memeriksa dakwaan kedua, pencurian (Pasal 362 KUHP) dan menyatakan terbukti secara sah dan meyakinkan melakukan tindak pidana pencurian.

Perkara Harry P. Samosir Majelis Hakim telah mengadili perkara *cybercrime (carding)* sesuai dengan teori, asas-asas, dan hukum positif yang berlaku baik dalam hukum pidana materiil maupun hukum acara pidananya yaitu pembuktian unsur-unsur tindak pidana yang didakwakan dan memeriksa dan mengadili sesuai dengan bentuk surat dakwaan yang disusun Jaksa Penuntut Umum.

Berkaitan dengan tindak pidananya, kesulitan untuk membuktikan tindak pidananya adalah Jaksa Penuntut Umum tidak dapat membuktikan bahwa pelaku telah membuat surat palsu dalam hal ini KTP dengan menggunakan komputer sehingga Majelis Hakim memutus tidak cukup bukti telah terjadi pemalsuan surat. Demikian pula dengan dakwaan kedua: pencurian, tidak dituntut oleh Jaksa Penuntut Umum di samping kesalahan pemahaman mengenai jenis tindak pidana pencurian juga tidak adanya *electronic record* yang dapat membuktikan pencurian telah terjadi.

Walaupun dalam putusannya Majelis Hakim menyatakan tindak pidana pencurian (Pasal 362 KUHP) terbukti secara sah dan meyakinkan, namun bukan untuk perbuatan menggunakan kartu kredit orang lain tetapi mengambil barang-barang yang dipesan dari tujuan pengiriman tanpa biaya pembayaran dari terdakwa. Hal ini menunjukkan bahwa tidak adanya barang bukti dan alat bukti menyulitkan dalam pembuktian tindak pidana yang sesungguhnya dilakukan terdakwa.

Jika mengacu pada jenis-jens kejahatan mayantara *(cybercrime)* kejahatan yang dilakukan Harry P. Samosir ini pada dasarnya termasuk kedalam pencurian melalui kartu kredit *(carding)* meskipun dalam kasus ini tidak dapat dibuktikan karena tidak ditemukannya bukti elektroniknya. Jika pemalsuan surat dalam hal ini pemalsuan KTP dengan komputer dapat dibuktikan, maka kejahatan ini memenuhi unsur-unsur kejahatan mayantara *(cybercrime)*.

Kasus ini terjadi sebelum lahirnya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sehingga pada saat itu bukti elektronik belum diakui sebagai alat bukti yang sah. Alat bukti yang diakui saat itu adalah alat bukti sebagaimana yang tercantum pada pasal 184 KUHAP. Dalam menggunakan alat-alat bukti konvensional atas kejahatan *cyber*, hakim memegang peranan penting dalam penyelesaian perkara dengan wajib menggali hukum yang hidup dalam masyarakat. Hakim harus membuat terobosan hukum jika belum ada undang-undang yang mengaturnya. Keyakinan hakim untuk menerima alat bukti di persidangan menjadi hal yang signifikan adanya. Begitu pentingnya peran

hakim dalam kasus *cybercrime*, hakim harus mempunyai kemampuan dalam ilmu teknologi informasi dan pandangan yang luas dalam penafsiran hukum.

2. Faktor Penyebab Terjadinya Kejahatan Mayantara *(Cybercrime)* Dalam Lingkup Transnasional Di Indonesia

A. Faktor Kesadaran Hukum Masyarakat

Apa yang dilakukan masyarakat akan berpengaruh besar terhadap potret penegakan hukum. Ketika salah seorang warga masyarakat terjerumus dalam perbuatan melanggar hukum, maka perilaku masyarakat ini sama artinya dengan menantang aparat penegak hukum untuk mengimplementasikan *law in books* menjadi *law in action*.[16]

Fungsi hukum pidana di bidang teknologi informasi secara umum adalah mengatur kehidupan manusia dalam kaitannya dengan kegiatannya dalam dunia maya agar tercipta tatanan masyarakat yang tertib dan damai. Sedangkan fungsi khususnya adalah sebagai berikut:[17]

a. Melindungi kepentingan hukum seluruh anggota masyarakat, baik orang per orang, kepentingan hukum masyarakat, maupun kepentingan hukum negara (misalnya keamanan negara) dalam pemanfaatan teknologi informasi agar dapat mencapai kesejahteraan.
b. Melindungi kepentingan hukum bagi setiap orang (manusia dan badan hukum) yang diduga atau telah terbukti menjadi pelaku kejahatan di bidang teknologi informasi.
c. Melindungi korban tindak pidana di bidang teknologi informasi.

Sampai saat ini, kesadaran hukum masyarakat Indonesia akan fungsi tersebut dan dalam merespon aktivitas kejahatan mayantara masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan mayantara. Kurangnya pengetahuan ini menyebabkan upaya penanggulangan kejahatan mayantara mengalami kendala dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan *(controlling)* masyarakat terhadap setiap aktiitas yang diduga berkaitan dengan tindak pidana mayantara.

Melalui pemahaman yang komprehensif mengenai kejahatan mayantara, peran masyarakat menjadi sangat penting dalam upaya pengawasan. Namun ketika masyarakat memiliki pengetahuan yang minim maka peran mereka akan menjadi mandul. Misalnya, dalam masyarakat yang memiliki pengetahuan minim tentang kejahatan mayantara datang seorang mahasiswa yang membawa seperangkat komputer dan di tempatnya yang baru ini si mahasiswa memesan barang-barang mewah melalui *carding*. Oleh karena masyarakat tidak mengetahui dan memahami *carding*, maka tidak ada kecurigaan atas perbuatan si mahasiswa ini, bahkan sebaliknya masyarakat cenderung terkesan dengan pola tingkah mahasiswa dimaksud.

B. Faktor Keamanan

Rasa aman tentunya akan dirasakan oleh pelaku kejahatan mayantara pada saat menjalankan aksinya. Hal ini tidak lain karena nternet lazim dipergunakan di

---

[16] Abdul Wahid dan Mohammad Labib, *Op.cit*. halaman. 136.

[17] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Yogyakarta ; Aswaja Pressindo, 2013. halaman. 18.

tempat-tempat yang relati tertutup, seperti di rumah, kamar, tempat kerja, perpustakaan bahkan warung internet (warnet). Akivitas yang dilakukan oleh pelaku di tempat-tempat tersebut sulit untuk diketahui oleh pihak luar. Akibatnya, pada saat pelaku sedang melakukan tindak pidan mayantara ini sangat jarang orang luar mengetahuinya. Hal ini sangat berbeda dengan kejahatan-kejahatan yang sifatnya konvensional, yang mana pelaku akan meudah diketahui secara fisik ketika sedang melakukan aksinya.

Begitu pula, ketika pelaku sedang beraksi di tempat terbuka, tidak mudah orang lain mengetahui aksinya. Misalnya di warnet yang tidak mempunyai penyekat ruangan, sangat sulit bagi orang awam untuk ngetahui bahwa seseorang sedang melakukan tindak pidana. Orang lain akan beranggapan bahwa plaku sedang menggunakan komputer untuk keperluan biasa, padahal sebenarnya ia sedang melakukan kejahatan. Kondisi ini akan membuat pelaku menjadi semakin berani. Di samping itu, apabila pelaku telah melakukan tindak pidana, maka dengan mudah pelaku dapat menghapus semua jejak kejahatan yang telah dilakukan mengingat internet menyediakan fasilitas untuk menghapuskan data/*file* yang ada. Akibatya pada saat pelaku tertangkap sukar bagi aparat penegak hukum untuk menemukan bukti-bukti kejahatan.

C. Faktor Budaya Hukum

Budaya hukum dapat diartikan sebagai sikap manusia terhadap hukum dan sistem hukum, kepercayaan, nilai serta harapannya (Lawrence M Friedman: 1969). Sebagaimana dikutip Hein Wangania, Friedman juga membedakan budaya hukum menjadi budaya hukum internal dan eksternal. Budaya hukum internal merupakan budaya hukum dari warga masyarakat yang melaksanakan tugas-tugas hukum secara khusus, seperti polisi, jaksa, dan hakim. Sedangkan budaya hukum eksternal merupakan budaya hukum masyarakat pada umumnya.[18]

Blankenburg mengemukakan budaya hukum juga merupakan keseluruhan sikap, kepercayaan, dan nilai-nilai yang berkaitan dengan hukum. Budaya hukum itu sendiri adalah sebagai sub-budaya yang bertalian dengan penghargaan dan sikap tindak manusia terhadap hukum sebagai realitas sosial.[19]

Budaya tidak sekedar berarti kumpulan bentuk tingkah laku dan pemikiran yang saling terlepas akan tetapi budaya diartikan sebagai kategori sisa sehingga didalamnya termasuk keseluruhan nilai sosial yang berhubungan dengan hukum, berikut sikap-sikap yang mempengaruhi bekerjanya hukum, termasuk didalamnya rasa hormat atau tidak hormat kepada hukum, kesediaan orang untuk memilih cara-cara informal untuk menyelesaikan suatu sengketa. Termasuk pula ke dalam budaya hukum adalah sikap-sikap dan tuntutan-tuntutan terhadap hukum yang diajukan oleh kelompok-kelompok etnis, ras, agama, lapangan pekerjaan dan kelas-kelas sosial yang berbeda-beda.[20]

---

[18] Tb. Ronny Rachman Nitibaskara, *Budaya Hukum dalam Pemberantasan Korupsi (Studi Awal Dimensi Budaya terhadap Perilaku Menyimpang)*, www.mahupiki.com/assets/news diakses tanggal 14 Mei 2014.

[19] Tb. Ronny Rachman Nitibaskara, *Perangkap Penyimpangan dan Kejahatan*, Jakarta : YPKIK, 2009.

[20] Hartoyo, Budaya Hukum dalam Implementasi Kebijakan Pemerintah terhadap Persyaratan Pengelolaan Apotik di Kota, eprints.undip.ac.id. 2007.

Budaya hukum merupakan tanggapan yang bersifat penerimaan atau penolakan terhadap suatu peristiwa hukum, ia menunjukkan sikap perilaku manusia terhadap masalah hukum dan peristiwa hukum yang terbawa ke dalam masyarakat.

Salah satu akar masalah ini penyebab terjadinya kejahatan mayantara *(cybercrime)* sebenarnya adalah sikap budaya para pelaku hukum di negara kita. Di satu pihak kita selalu menempatkan hukum sebagai bagian dari nilai-nilai yang ideal dari masyarakat kita. Sikap ini tentu saja bukanlah sikap yang tidak terpuji, secara tak sadar kita menempatkan hukum dalam sebuah menara gading. Jauh dari realitas kehidupan masyarakat sehari-hari. Padahal hukum, sebagai suatu gejala sosial sebenarnya harus realistis, membumi, memecahkan persoalan kemasyarakatan yang dihadapinya.[21]

D. Faktor Penegak Hukum

Faktor penegak hukum sering menjadi penyebab maraknya kejahatan siber *(cybercrime)*. Secara umum penyidik masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah:

a. Kurangnya pengetahuan tentang komputer
b. Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *cybercrime* masih terbatas
c. Faktor sistem pembuktian yang menyulitkan para penyidik.

Selain itu perlu juga diketahui bahwa dalam melakukan penyidikan terhadap kejahatan mayantara *(cybercrime)*, Kepolisian maupun penyidik dari Pegawai Negeri Sipil harus berkoordinasi dan dapat meminta bantuan ahli yang diperlukan dalam melakukan penyidikan, bahkan Kepolisian dan penyidik dari Pegawai Negeri Sipil tersebut dapat meminta bantuan dari penyidik negara lain untuk berbagi informasi dan alat bukti.[22]

3. Kebijakan Penanggulangan Kejahatan Mayantara (*Cybercrime*) Dalam Lingkup Transnasional

1. Penal

Dilihat dari kebijakan kriminal (kebijakan penanggulangan kejahatan), hukum pidana bukan merupakan sarana kebijakan yang utama/strategis. Kebijakan yang mendasar/strategis adalah mencegah dan meniadakan faktor-faktor penyebab atau kondisi yang menimbulkan kejahatan.[23]

Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cybercrime*) tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu bentuk dari *high tech crime*, merupakan hal yang wajar jika upaya penanggulangan *cyber crime* (CC) juga

---

[21] Setiawan, *Hukum yang Terlelap*. Forum Keadilan, No.3 Tahun VII, 1998.

[22] Bab X Pasal 45 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Informasi.

[23] Barda Nawawi Arief, *"Kebijakan Hukum Pidana Menghadapi Perkembangan Cyber Crime di Bidang Kesusilaan (Cybersex/Cyberporn)"*, Jurnal ilmiah, halaman 51.

harus ditempuh dengan teknologi *(techno prevention)*. Disamping itu diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan global (kerjasama internasional) karena *cyber crime* dapat melampaui batas-batas negara (bersifat *transnational/transborder*).[24]

Walaupun sarana penal mempunyai keterbatasan, namun dilihat dari sudut "perencanaan kebijakan penanggulangan kejahatan dengan hukum pidana" *(penal policy)*, tahap kebijakan legislasi/formulasi merupakan tahap paling strategis. Kesalahan/kelemahan kebijakan legislatif merupakan kesalahan strategis yang dapat menjadi PENGHAMBAT upaya pencegahan dan penanggulangan kejahatan pada tahap aplikasi dan eksekusi.[25]

Dalam upaya atau kebijakan penanggulangan *cybercrime* dengan hukum pidana, lokakarya/workshop mengenai *"computer related crime"* yang diselenggarakan dalam kongres PBB X (April 2000) menyatakan, bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur. Jadi masalahnya bukan sekedar bagaimana membuat kebijakan hukum pidana (kebijakan kriminalisasi, formulasi, dan legislasi) di bidang penanggulangan *cybercrime*, tetapi bagaimana ada harmonisasi kebjakan penal di berbagai negara. Ini berarti, kebijakan kriminalisasi tentang masalah *cybercrime* bukan semata-mata masalah kebijakan nasional (Indonesia) tetapi juga terkait dengan kebijakan regional dan internasional.[26]

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakekatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal *(criminal policy)* dengan menggunakan sarana hukum pidana (penal), dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" *(penal policy)*, khususnya kebijakan formulasinya.[27]

Ketentuan hukum pidana positif yang dikriminalisasi terkait kejahatan mayantara *(cybercrime)* dapat kita lihat pada Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana yang dimuat pada Pasal 27 sampai dengan Pasal 36. Terdapat pula pada Undang-undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, dimana sisi mayantara dari tindak pidana korupsi ini adalah bahwa kejahatan tersebut telah menggunakan media internet sebagai alat untuk melakukan korupsi ataupun memperlancar tindak dilakukannya tindak pidana tersebut meskipun tidak secara eksplisit diatur dalam undang-undang ini.

Beberapa peraturan perundang-undangan yang mengkriminalisasi kejahatan mayantara di dalamnya adalah : Undang-undang Nomor 44 Tahun 2008

---

[24] Barda Nawawi, *Tindak Pidana Mayantara : Perkembangan Cyber Crime di Indonesia*, Jakarta ; RajaGrafindo Persada, 2006. halaman. 182-183.

[25] Barda Nawawi Arief, *"Kebijakan Hukum Pidana…",Op. cit.* halaman. 53.

[26] Barda Nawawi, *Perbandingan Hukum Pidana*, Jakarta ; Raja Grafindo, 2002. halaman. 269.

[27] *Ibid.*

tentang Pornografi, Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme, Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, dan Undang-undang Nomor 35 Tahun 2009 tentang Narkotika.

2. Non Penal

Pendekatan non penal menurut Hoefnagels adalah pendekatan pencegahan kejahatan tanpa menggunakan sarana pemidanaan (*prevention without punisment*), yaitu antara lain perencanaan kesehatan mental masyarakat (*community planning mental health*), kesehatan mental masyarakat secara nasional (*national mental health*), *social worker and child welfare* (kesejahteraan anak dan pekerja sosial), serta penggunaan hukum civil dan hukum administrasi *(administrative & civil law).*[28]

Kebijakan penanggulangan kejahatan lewat jalur "non penal" lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan. Oleh karena itu, sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan yang berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuhsuburkan kejahatan. Dengan demikian dilihat dari kebijakan penanggulangan kejahatan, maka usaha-usaha non penal ini mempunyai kedudukan yang strategis dan memegang peranan kunci yang harus diintensifkan dan diefektifkan. [29]

Beberapa masalah dan kondisi sosial yang dapat merupakan faktor kondusif penyebab timbulnya kejahatan, jelas merupakan masalah yang tidak dapat diatasi semata–mata dengan "penal". Di sinilah keterbatasan jalur "penal" dan oleh karena itu, harus ditunjang oleh jalur "nonpenal". Salah satu jalur "nonpenal" untuk mengatasi masalah–masalah sosial seperti dikemukakan diatas adalah lewat jalur "kebijakan sosial" *(social policy)*, dimana G.P. Hoefnagels juga memasukkan dalam jalur "*prevention without punishment*". Kebijakan sosial pada dasarnya adalah kebijakan atau upaya-upaya rasional untuk mencapai kesejahteraan masyarakat. Jadi identik dengan kebijakan atau perencanaan pembangunan nasional yang meliputi berbagai aspek yang cukup luas dari pembangunan.[30]

Kejahatan mayantara (*cybercrime)* membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cybercrime* adalah:

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

---

[28] Mahmud Mulyadi, *Criminal Policy Pendekatan Integral Penal Policy dan Non-Penal Policy dalam Penanggulangan Kejahatan Kekerasan*, Medan, ; Pustaka Bangsa Press, 2008. halaman. 58.

[29] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana Perkembangan Penyusunan Konsep KUHP Baru*, Kencana, Jakarta, 2011, halaman. 49

[30] *Ibid*. halaman. 44.

c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*
d. Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi.
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaty*.
f. Harmonisasi mengenai masalah yurisdiksi untuk menegakkan kedaulatan negara yang berlaku karena sifatnya transnasional.

E. PENUTUP

1. Kesimpulan

Berdasarkan uraian diatas dapat disimpulkan sebagai berikut:

a. Pengaturan hukum pembuktian kejahatan mayantara *(cybercrime)* dalam lingkup transnasional dapat dilihat pada:
   1. *Convention on Cybercrime*
   2. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   3. Undang-Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi
   4. Undang-Undang No. 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang
   5. Undang - Undang No. 21 tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang
   6. Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme
b. Faktor penyebab terjadinya kejahatan mayantara *(cybercrime)* dalam lingkup transnasional di Indonesia disebabkan oleh:
   1. Faktor kesadaran hukum masyarakat
   2. Faktor keamanan pelaku dalam melakukan kejahatan
   3. Faktor budaya hukum
   4. Faktor penegak hukum
c. Kebijakan penanggulangan kejahatan mayantara *(cybercrime)* dalam lingkup transnasional dapat berupa:
   1. Penal, dapat berupa kriminalisasi guna mengefektifkan hukum positif yang berkaitan dengan kejahatan mayantara.
   2. Non Penal, berupa pendekatan melakukan upaya pencegahan terjadinya kejahatan mayantara *(cybercrime)* seperti peningkatan pengetahuan aparat penegak hukum tentang teknologi dan informasi, peningakatan sarana dan prasana dalam upaya pembuktian, serta peningkatan kerjasama internasional.

2. Saran

1. Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan

penyidikan dan penyelidikan guna memperlancar pembuktian kejahatan mayantara *(cybercrime)* tersebut. Peningkatan sarana prasarana dan kemampuan aparat penegak hukum di bidang teknologi dan informasi, pengetahuan, keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia.

2. Perlu peningkatan kelengkapan alat teknologi informasi dan komunikasi untuk memperlancar proses pembuktian kejahatan tersebut serta peningkatan kerjasama internasional dalam rangka penegakan hukum untuk memberantas kejahatan mayantara *(cybercrime).* Salah satunya kerjasama internasional dalam hal penyidikan, jadi bukan hanya dalam hal informasi dan alat bukti saja seperti yang dikemukakan Pasal 43 UU ITE.

DAFTAR PUSTAKA

A. Buku

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

Mulyadi, Mahmud, ***Criminal Policy Pendekatan Integral Penal Policy dan Non-Penal Policy dalam Penanggulangan Kejahatan Kekerasan***, Medan, ; Pustaka Bangsa Press, 2008.

Nawawi Arief, Barda, ***Tindak Pidana Mayantara : Perkembangan Cyber Crime di Indonesia***, Jakarta ; RajaGrafindo Persada, 2006.

----------, ***Perbandingan Hukum Pidana***, Jakarta ; Raja Grafindo, 2002.

----------, ***Bunga Rampai Kebijakan Hukum Pidana Perkembangan Penyusunan Konsep KUHP Baru***, Jakarta ; Kencana, 2011.

Nitibaskara, Tb. Ronny Rachman , ***Perangkap Penyimpangan dan Kejahatan***, Jakarta : YPKIK, 2009.

Suhariyanto, Budi, ***Tindak Pidana Teknologi Informasi (Cybercrime)***, Jakarta ; RajaGrafindo Persada, 2012.

Suseno, Sigid, ***Yurisdiksi Tindak Pidana Siber***, Bandung ; Refika Aditama, 2012

Wahid, Abdul dan Mohammad Labib, ***Kejahatan Mayantara***, Bandung ; Refika Aditama, 2005.

Widodo, ***Aspek Hukum Pidana Kejahatan Mayantara***, Yogyakarta ; Aswaja Pressindo, 2013.

B. Peraturan Perundang-undangan

Convention on Cybercrime

Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP)

Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
Undang-undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang
Undang-undang Nomor 40 Tahun 2008 tentang Pornografi
Undang-undang Nomor 35 Tahun 2009 tentang Narkotika
Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang

C. Artikel Makalah

Barda Nawawi Arief, "*Kebijakan Hukum Pidana Menghadapi Perkembangan Cyber Crime di Bidang Kesusilaan (Cybersex/Cyberporn)*", Jurnal ilmiah,

Erwin MAP, M.A., *Kejahatan Transnasional (Transnational Crime)*, Markas Besar Kepolisian Negara Republik Indonesia, Badan Reserse Kriminal, Jakarta, Desember 2002

Setiawan, Hukum yang Terlelap. Forum Keadilan, No.3 Tahun VII, 1998.

D. Internet

Tb. Ronny Rachman Nitibaskara, Budaya Hukum dalam Pemberantasan Korupsi (Studi Awal Dimensi Budaya terhadap Perilaku Menyimpang), www.mahupiki.com/assets/news

Hartoyo, Budaya Hukum dalam Implementasi Kebijakan Pemerintah terhadap Persyaratan Pengelolaan Apotik di Kota, eprints.undip.ac.id. 2007.