KEBIJAKAN PENEGAKAN HUKUM *CYBERCRIME* DAN PEMBUKTIAN YURIDIS DALAM SISTEM HUKUM PIDANA NASIONAL

CYBERCRIME LAW ENFORCEMENT POLICY AND THE JURIDICAL EVIDENCE IN NATIONAL CRIMINAL LAW SYSTEM

Dwi Nurahman
Fakultas Hukum, Universitas Mitra Indonesia
dwinurahman_shmh@ymail.com;

Abstrak

Penulisan ilmiah ini berorientasi untuk mengetahui bagaimana aspek hukum pembuktian pada *cybercrime* dalam sistem hukum pidana nasional dan kebijakan penegakan hukum terhadap *cybercrime*. Metode yang digunakan adalah penelitian hukum normatif. Berdasarkan hasil kajian dapat diketahui bahwa aspek hukum pembuktian *cybercrime* telah diatur secara tegas dalam beberapa peraturan perundang-undangan dalam hukum positif di Indonesia. Ketentuan mengenai *Cybercrime* dalam regulasi internasional tidak bermaksud mengurangi kesempatan setiap individu untuk tetap mengembangkan kreativitasnya dalam mengembangkan teknologi informasi. Kebijakan penegakan hukum terhadap *cybercrime* dilakukan dengan pendekatan secara penal dan non-penal. Dilihat dari sudut *criminal policy*, upaya penanggulangan *cybercrime* tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik maupun pendekatan bersifat preventif (non-penal).

Kata Kunci: Kebijakan; Penegakan Hukum; *Cybercrime;* Pembuktian; Sistem Hukum Pidana Nasional

Abstract

This writing is oriented to find out how the legal aspects of evidence on cybercrime in the national criminal law system and law enforcement policies against cybercrime. The method uses is normatif legal research. Based on the results of the study it can be seen that the legal aspects of proving cybercrime have been strictly regulated in several laws and regulations in positive law in Indonesia. Provisions regarding Cybercrime are also regulated in international regulations without reducing the opportunity for each individual to continue to develop creativity in developing information technology. Law enforcement policies against cybercrime are carried out with a penal and non-penal approach. Seen from the point of view of criminal policy, efforts to overcome cybercrime certainly cannot be done partially with criminal law (penal), but must also be taken with an integral/systemic approach as well as a preventive approach (non-penal).

Keywords : *Policy; Law enforcement; Cybercrime; Proof; National Criminal Law System*

A. Pendahuluan

Era saat ini 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. Kemajuan teknologi informasi ini menyebabkan masyarakat memiliki ruang gerak yang lebih luas.[1] Aktivitas manusia yang semula bersifat nasional telah berubah menjadi internasional, sehingga wajar 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. Penegak hukum di Indonesia mengalami kesulitan saat menjerat pelaku karena masalah pembuktian *(documentary evidence)* yang tidak memenuhi ketentuan sistem hukum pidana Indonesia.[2]

Kemajuan yang pesat dari perkembangan teknologi telekomunikasi dan teknologi komputer menghasilkan internet yang multifungsi. Perkembangan ini membawa ke ambang revolusi keempat dalam sejarah pemikiran manusia bila ditinjau dari konstruksi pengetahuan umat manusia yang dicirikan dengan cara berfikir yang tanpa batas (*borderless way of thinking*). Percepatan teknologi semakin lama semakin meningkat yang menjadi sebab material perubahan yang terus menerus dalam semua interaksi dan aktivitas masyarakat informasi.

Pemanfaatan teknologi telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat disajikan melalui hubungan jarak jauh dan mereka yang ingin mengadakan transaksi tidak harus bertemu muka, akan tetapi cukup melalui peralatan komputer dan telekomunikasi. Perkembangan teknologi informasi juga membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial dan telah membalikkan segalanya yang jauh jadi dekat yang khayal jadi nyata. Di balik kemajuan itu, juga telah melahirkan

[1] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informasi*, (Bandung : Refika Aditama, 2005), hlm. 113

[2] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, (Bandung : Refika Aditama, 2012), hlm. 48

keresahan-keresahan baru dengan munculnya kejahatan yang canggih dalam bentuk *Cybercrime.*

Upaya menjerat pelaku-pelaku kejahatan mayantara (*cybercrime)* harus tetap dilakukan, upaya perluasan alat bukti menjadi solusi untuk menegakkan hukum. Pembuktian kejahatan mayantara dalam sistem peradilan pidana Indonesia menjadi topik penting, terlebih dengan ditetapkannya Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas 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. 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.[3]

Mencermati hal tersebut dapatlah disepakati bahwa c*ybercrime* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara. 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)*. Dalam rangka mendapat gambaran yang jelas mengenai pembuktian kejahatan mayantara (*cybercrime*) baik yang diatur dalam hukum acara pidana Indonesia maupun pembuktian serta kajian yurisdiksi dalam lingkup transnasional maka perlu dilakukan penelitian.

Secara umum yang dimaksud dengan kejahatan komputer atau kejahatan di dunia maya (*Cybercrime*) adalah ”upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer

[3] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime),* (Jakarta : Raja Grafindo Persada, 2012), hlm. 51

yang dimasuki atau digunakan.[4] Munculnya banyak jenis-jenis kejahatan baru yang tidak saja bersifat lintas batas (transnasional), tetapi juga berwujud dalam tindakan-tindakan virtual telah menyadarkan masyarakat internasional tentang perlunya perangkat hukum internasional baru yang dapat digunakan sebagai kaidah hukum internasional dalam mengatasi kasus-kasus *Cybercrime* (kejahatan didunia maya).

Kejahatan yang berhubungan dengan komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer. Kejahatan tersebut dibedakan menjadi dua kategori yakni *Cybercrime* dalam pengertian sempit dan dalam pengertian luas. *Cybercrime* dalam pengertian sempit merupakan kejahatan terhadap sistem komputer, sedangkan *Cybercrime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.

Adapun teori yang digunakan dalam penulisan ini adalah teori penegakan hukum. Hipotesis dalam penulisan ilmiah ini adalah aspek hukum pembuktian kejahatan *cybercrime* telah diatur secara tegas dalam beberapa perturan perundang-undangan yakni Kitab Undang-undang Hukum Acara Pidana Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan sebagainya. Ketentuan mengenai *Cybercrime* juga diatur dalam regulasi internasional (*Convention on Cybercrime*) yakni *Convention on Cyber Crime* Tahun 2001 yang digagas Uni Eropa. Kebijakan penegakan hukum terhadap kejahatan *cybercrime* dilakukan dengan pendekatan secara penal dan non-penal.

B. Metode Penelitian

Penulisan ilmiah ini menggunakan metode penelitian hukum normatif yang menitikberatkan pada hukum sebagai norma (kaidah). Penelitian ini bertujuan untuk menggambarkan realita yang sesuai dengan fenomena secara rinci dan tuntas, serta pengumpulan data dari latar alami dengan memanfaatkan diri peneliti sebagai instrumen kunci sebagai pengupas dari permasalahan yang akan diteliti. Penulisan ilmiah ini menggunakan metode

[4] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta : Aswaja Pressindo, 2013), hlm.49

pendekatan kualitatif sebagai proses penelitian yang menghasilkan data deskriptif berupa data tertulis atau lisan yang diamati.

C. Pembahasan

1. Aspek Hukum Pembuktian Kejahatan *Cybercrime* dalam Sistem Hukum Pidana Nasional

Substansi penting yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ialah mengenai pengaturan tranksaksi elekronik dan mengenai tindak pidana siber. Materi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. Ketentuan Pasal 42 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur pula mengenai ketentuan penyidikan yakni : "penyidikan sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam undang-undang ini".

Sistem pembuktian yang dianut adalah sistem/teori pembuktian berdasar undang-undang secara negatif, yaitu sistem yang dianut dalam KUHAP dan berdasar Pasal 183 Kitab Undang-undang Hukum Acara Pidana, yang menyatakan: "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".[5] Pembuktian harus didasarkan ketentuan undang-undang, yakni alat bukti yang sah yang diatur dalam Pasal 184 Kitab Undang-undang Hukum Acara Pidana disertai keyakinan hakim yang diperoleh dari alat-alat bukti tersebut.

Berikut beberapa alat bukti yang diatur dalam Pasal 184 Kitab Undang-undang Hukum Acara Pidana sebagai acuan dalam pembuktian kejahatan mayantara *(cybercrime)*, yaitu:

1) Keterangan saksi

[5] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara*, (Bandung : Refika Aditama, 2005), hlm. 37

Syarat formal keterangan saksi yang diatur dalam Kitab Undang-undang Hukum Acara Pidana 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)*;
(5). adanya persesuaian antara keterangan saksi yang satu dengan yang lain dan keterangan saksi yang satu dengan alat bukti yang lain.

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.

2) Keterangan ahli

Dalam Pasal 186 Kitab Undang-undang Hukum Acara Pidana 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 Kitab Undang-undang Hukum Acara Pidana)

Jenis surat yang diakui berdasarkan alat bukti ialah surat yang dibuat diatas sumpah jabatan atau dikuatkan dengan sumpah sebagaimana yang tertuang dalam Pasal 187 Kitab Undang-undang Hukum Acara Pidana. "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 Kitab Undang-undang Hukum Acara Pidana.

4) Alat bukti petunjuk (Pasal 184 (1) huruf d dan Pasal 188 Kitab Undang-undang Hukum Acara Pidana)

Kitab Undang-undang Hukum Acara Pidana 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.

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.

5) Keterangan terdakwa (Pasal 184 huruf e dan Pasal 189 Kitab Undang-undang Hukum Acara Pidana)

Keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. 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.

Ketentuan Pasal 5 ayat (1) dan (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 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 :

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) Kitab Undang-undang Hukum Acara Pidana Indonesia. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai ketentuan yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 terkait dengan Pasal tentang Pasal 5 ayat (1) dan ayat (2) dan Pasal 44 huruf b Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka dibutuhkan pengaturan kembali tentang kedudukan bukti elektronik dan prosedur perolehannya dalam sistem peradilan pidana Indonesia. Mahkamah Konstitusi telah menyatakan frasa "informasi elektronik dan/atau dokumen elektronik" dalam ketentuan di atas bertentangan dengan Undang-Undang

Dasar 1945. Mahkamah Konstitusi kemudian mengganti frasa tersebut menjadi "Khususnya Informasi Elektronik dan/atau dokumen elektronik sebagai alat bukti dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang sebagaimana ditentukan dalam Pasal 31 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik".[6]

Ketentuan Pasal 5 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik :

1) Khususnya Informasi Elektronik dan/atau dokumen elektronik sebagai alat bukti dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang sebagaimana ditentukan dalam Pasal 31 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2) Khususnya Informasi Elektronik dan/atau dokumen elektronik sebagai alat bukti dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang sebagaimana ditentukan dalam Pasal 31 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Ketentuan Pasal 44 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah "alat bukti lain berupa Khususnya Informasi Elektronik dan/atau dokumen elektronik sebagai alat

[6] Barda Nawawi Arief, *Tindak Pidana Mayantara : Perkembangan Cyber Crime di Indonesia*, (Jakarta : RajaGrafindo Persada, 2006), hlm. 86

bukti dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang sebagaimana ditentukan dalam Pasal 31 ayat (3) UU No 11 Tahun 2008 tentang informasi dan Transaksi Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)".

Putusan Mahkamah Konstitusi mengubah status dari informasi elektronik dan dokumen elektronik dalam penegakan hukum pidana yang akibatnya seluruh informasi elektronik/dokumen elektronik yang dapat menjadi bukti harus diperoleh berdasarkan prosedur sesuai pasal 31 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, di luar itu maka informasi elektronik/dokumen elektronik tidak diperbolehkan sebagai bukti.

2. Kebijakan Penegakan Hukum terhadap Kejahatan *Cybercrime*

a. Pendekatan Secara Penal

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. 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* juga 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*).[7]

Kebijakan penanggulangan *cybercrime* dengan hukum pidana, workshop mengenai *"computer related crime"* yang diselenggarakan dalam kongres PBB X Tahun 2000 menyatakan, bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan

[7] Mahmud Mulyadi, *Criminal Policy Pendekatan Integral Penal Policy dan Non-Penal Policy dalam Penanggulangan Kejahatan Kekerasan, (*Medan : Pustaka Bangsa Press, 2008), hlm. 63

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.

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.

b. Pendekatan Secara 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).* Kebijakan penanggulangan kejahatan secara "non penal" lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan.[8] 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.

Kejahatan mayantara (*cybercrime)* membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Beberapa langkah penting yang harus

[8] Lagazio M, Sherif N, Cushman M, *A Multi-level Approach to Understanding the Impact of Cyber Crime on the Financial Sector*, *Computers & Security,* Volume 45 September 2014, hlm. 11

dilakukan setiap negara dalam penanggulangan *cybercrime* adalah:

1) Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
2) Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
3) Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*
4) Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi.
5) Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaty*.

Harmonisasi mengenai masalah yurisdiksi untuk menegakkan kedaulatan negara yang berlaku karena sifatnya transnasional.

D. Kesimpulan

Aspek hukum pembuktian kejahatan cybercrime telah diatur secara tegas dalam beberapa perturan perundang-undangan dalam hukum positif di Indonesia yakni: Kitab Undang-undang Hukum Acara Pidana Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 dan sebagainya. Ketentuan mengenai Cybercrime juga diatur dalam regulasi internasional (Convention on Cybercrime) yakni Convention on Cyber Crime 2001 yang digagas Uni Eropa. Konvensi Dewan Eropa tersebut sebagai Perlindungan Hak Asasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil dalam mengatasi kejahatan siber, tanpa mengurangi kesempatan setiap individu untuk tetap mengembangkan kreativitasnya dalam mengembangkan teknologi informasi.

Kebijakan penegakan hukum terhadap kejahatan cybercrime dilakukan dengan pendekatan secara penal dan non-penal. Penal, dapat berupa kriminalisasi guna mengefektifkan hukum positif yang berkaitan dengan kejahatan cybercrime. 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.

Daftar Pustaka

Buku

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

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

Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime),* Jakarta : Raja Grafindo Persada, 2012.

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

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

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

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

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

Karya Ilmiah :

Lagazio M, Sherif N, Cushman M, *A Multi-level Approach to Understanding the Impact of Cyber Crime on the Financial Sector*, Computers & Security, Volume 45 September 2014.

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Acara Pidana Indonesia.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.