TINJAUAN YURIDIS TENTANG KEDUDUKAN ALAT BUKTI DIGITAL DALAM TINDAK PIDANA KEJAHATAN MAYANTARA *(CYBER CRIME)*[1]

Oleh: Vogen L. M. T. Mantik[2]
Ruddy R. Watulingas[3]
Harly Stanly Muaja[4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bagaimana kedudukan alat bukti digital dalam perkara kasus *cyber crime* dan faktor yang mempengaruhi terjadinya kejahatan mayantara (*cyber crime*). Dengan metode penelitian hukum normatif, dengan kesimpulan:1. Yurisdiksi kriminal berlakunya hukum pidana nasional terhadap *cyber crime* tidak cukup dengan menggunakan prinsip yurisdiksi teritorial dan ekstra teritorial yang diakui dalam hukum internasional publik tetapi juga berdasarkan prinsip yurisdiksi yang berlaku terhadap tindak pidana yang dilakukan diluar yurisdiksi negara manapun. Jadi yurisdiksi criminal berlakunya hukum pidana nasional terhadap *cyber crime* menganut quasi yurisdiksi yaitu menggunakan yurisdiksi teritorial, yurisdiksi ekstra teritorial terhadap *cyber crime* yang dilakukan didalam yurisdiksi negara lain dan ekstra territorial terhadap *cyber crime* yang dilakukan diluar yurisdiksi negara manapun.2. hasil penelitian ketiga Putusan yang didapat penulis di lapangan, belum ada pemrosesan alat bukti yang sesuai prosedur, alat bukti digital yang dihadirkan di persidangan telah di explore oleh saksi ahli sebelumnya, sehingga mengurangi keaslian dari sebuah alat bukti itu sendiri, padahal dalam Undang-Undang No. 11 tahun 2008 pada Pasal 43 ayat (2) telah dijelaskan tentang pelaksanaa prosedur penyidikan dalam bidang Teknologi Informasi dan Transaksi Elektronik**.** Sistem pembuktian dalam perkara tindak pidana cyber crime dengan cara perluasan alat bukti dalam KUHAP sebenarnya sudah diatur dalam berbagai perundang-undangan secara tersebar. Dengan demikian email, suara, gambar,kode akses, simbol, dan berbagai dokumen elektronik lainnya mempunyai kekuatan pembuktian yang setara dengan alat bukti lainnya yang diatur didalam KUHAP dan dapat digunakan sebagai alat bukti yang sah.

Kata Kunci : Kedudukan. Alat Bukti Digital, Tindak Pidana, Kejahatan Mayantara.

PENDAHULUAN

A. Latar Belakang

Pada dasarnya setiap undang-undang yang dibuat oleh pembuat undang-undang merupakan jawaban hukum terhadap persoalan masyarakat pada waktu dibentuknya undangundang tersebut. Perkembangan hukum seharusnya seiring dengan perkembangan masyarakat, sehingga ketika masyarakatnya berubah atau berkembang maka hukum harus berubah untuk menata semua perkembangan yang terjadi dengan tertib di tengah pertumbuhan masyarakat modern [5], karena globalisasi telah menjadi pendorong lahirnya era teknologi informasi.[6]

Semakin berkembangnya penggunaan internet dan teknologi informasi sebagai media untuk bertransaksi dan berkomunikasi elektronik, maka akan semakin menjadikan kita akan lebih mudah dan cepat. Di sisi lain, juga memunculkan dampak yang besar terhadap meningkatnya kejahatan di dunia *cyber*. Keamanan Informasi dan Transaksi Elektronik (ITE) dan Kejahatan ITE selalu beradu dalam berbagai persoalan terkait dengan Informasi dan Transaksi Elektronik (ITE).

Sesuai dengan penjelasan pada UU ITE, Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Penyebab perubahan itu akibat masyarakat yang lebih banyak menggunakan ITE, dan hukum atau peraturan yang kurang mejerat para pelaku kejahatan tersebut sehingga banyak munculnya kejahatan seperti *cyber crime* atau kejahatan melalui jaringan internet adanya *cyber crime* telah menjadi ancaman stabilitas bagi negara, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan menggunakan teknologi komputer khususnya internet.

---

[1] Artikel Skripsi.
[2] Mahasiswa Fakultas Hukum UNSRAT, NIM 17071101427
[3] Fakultas Hukum UNSRAT, Doktor Ilmu Hukum
[4] Fakultas Hukum UNSRAT, Magister Ilmu Hukum

[5] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi dan Pengaturan Celah Hukumnya*, Jakarta, 2012
[6] *Ibid*. Hlm 1

Teknologi informasi juga dapat merubah perilaku masyarakat, bahkan sekarang Teknologi Informasi saat ini menjadi pedang bermata dua buat kita karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum sehingga banyak perbuatan pidana terlepas dari jerat hukum.

Perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas sehingga menyebabkan perubahan sosial yang sangat cepat pada masyarakat. Sesuai dengan catatan Polda Metro Jaya Jakarta Selatan, kejahatan dunia *cyber* hingga pertengahan 2018 mencapai 1.603 kasus. Arga mengatakan kasus tersebut meliputi pencemaran nama baik, hate speech, spam, penyalahgunaan jaringan teknologi informasi, dan carding. Data dari Asosiasi Kartu Kredit Indonesia (AKKI) menunjukkan, sejak tahun 2003 hingga kini, angka kerugian akibat kejahatan kartu kredit mencapai Rp 30 milyar per-tahun (Ahmadjayadi, 2008).

Undang-Undang ITE ini dimaksudkan untuk menjawab permasalahan hukum yang seringkali dihadapi yaitu terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.namun kenyataan saat ini adalah ketidakmampuan sistem hukum konvensional dalam mengantisipasi dan menangani kasus kejahatan didunia maya. Hal ini di dasari oleh beberapa hal, misalnya persoalan tentang kegiatan dunia maya yang tidak dapat dibatasi oleh 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.

Melihat kondisi tersebut, Didik M. Arief Mansur dan Alisatris Gultom menyatakan bahwa ketiadaan undang-undang yang menjadi penyebab tidak dapat dihukumnya pelaku kejahatan tidak dapat dibiarkan berlarut-larut, karena apabila hal ini tidak segera diselesaikan akan menimbulkan keresahan di masyarakat dan pada akhirnya hukum akan kehilangan wibawanya.

Selanjutnya dinyatakan, ironis memang, pada saat kejahatan didunia maya (*cyber crime*) semakin meningkat jumlahnya, ternyata masih banyak pelaku yang tidak dapat diadili akibat ketiadaan undang-undang. Akibatnya, sangat wajar apabila kejahatan didunia maya (*cyber crime*) semakin meningkat dari waktu ke waktu.

Sejalan dengan hal diatas, Sutanto dkk menyatakan bahwa persoalan hukum yang muncul bukan hanya akibat adanya suatu kegiatan yang merugikan pihak lain dalam lingkup yang kecil. Berbagai kasus telah mengindikasikan tingkat kejahatan yang dilakukan sudah sedemikian luas, mulai dari kasus pencemaran nama baik, hingga isu-isu yang menimbulkan masalah regional, bahkan global misalnya isu terorisme.

Esensi Undang-Undang Informasi dan Transaksi Elektronik melingkupi seluruh transaksi berbasis elektronik seperti komputer serta jaringan dan memiliki kekuatan hukum. Undang-Undang ITE dipersepsikan sebagai *cyber law* di Indonesia, yang diharapkan bisa mengatur segala urusan dunia internet (*cyber*), termasuk didalamnya memberi hukuman terhadap pelaku *cyber crime* guna melindungi masyarakat dari kejahatan di dunia maya.(Wahono, 2008)

Pada akhirnya, tepat apa yang dikemukakan oleh Ahmad M. Ramli dkk, bahwa kegiatan *cyber* meskipun bersifat virtual tetapi dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis, terhadap ruang *cyber* sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi konvensional untuk dijadikan obyek dan perbuatan. Sebab, jika cara ini ditempuh maka akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan *cyber* adalah kegiatan virtual tetapi berdampak sangat nyata meskipun alat uktinya bersifat elektronik. Oleh karena itu, subyek pelakunya harus dikualifikasikan pula sebagai telah melakukan perbuatan hukum secara nyata. Perkembangan terbaru dalam hukum pidana (khususnya hukum acara pidana) sebetulnya telah berupaya untuk mengakomodasi perkembangan teknologi informasi ini.

Misalnya, dalam UU No. 20 tahun 2001 jo. UU. No.31 tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi telah memasukkan alat bukti elektronik sebagai alat bukti yang sah, dalm bentuk “petunjuk”. Hal ini diatur dalam pasal 26 A dengan menyatakan sebagai berikut:

Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam pasal 188 ayat (2) undang-undang No. 8 tahun 1981

tentang Hukum acara pidana, khususnya untuk tindak pidana korupsi juga diperoleh dari :

1. Alat bukti yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpansecara elektronik dengan alat optikatau yang serupa dengan itu; dan
2. Dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang diatas 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.

Kemudian dalam penjelasan pasal demi pasalnya disebutkan bahwa yang dimaksud dengan "disimpan secara elektronik" misalnya data yang disimpan dalam mikro film, compact disk read only memory (CD-ROM) atau write once read many (WORM).

Sedangkan yang dimaksud dengan "alat optik atau yang serupa dengan itu" adalah tidak terbatas pada data penghubung elektronik (elektronic data interchage), surat elektronik (e-mail), telegram, teleks, dan faksmili.

Ketentuan tersebut mengisyaratkan secara eksplisit akan pengakuan secara hukum atas perkembangan penyalahgunaan teknologi informasi. Khususnya penyalahgunaan internet. Dengan kata lain, perkembangan teknologi komputer dan internet dapat dijadikan sebagai sarana untuk melakukan kejahatan. Sarana itulah yang diakui oleh UU No. 20 tahun 2001 sebagai salah satu alat bukti yang sah.

Namun demikian, permasalahan akan muncul tatkala undang-undang tersebut merujuk pada KUHAP sebagai acuan dalam penyidikan, penuntutan maupun pemeriksaan dipengadilan. Hal itu disebabkan dalam KUHAP diatur bahwa alat bukti yang sah hanya meliputi :

1. Keterangan Saksi
2. Keterangan Ahli
3. Surat
4. Petunjuk; dan
5. Keterangan Terdakwa.

Sehubungan dengan itu, banyak kalangan yang mengusulkan bahwa KUHAP juga perlu direvisi. Disesuaikan pengaturan alat buktinya dengan perkembangan teknologi informasi, sebagaimana yang telah diatur dalam UU tindak pidana korupsi, maupun undang-undang yang lainnya, yang telah memasukkan data elektronik sebagai alat bukti.

Dalam upaya menghindari adanya ketidakadilan bagi korban maka diperlukan kemampuan dan keberanian aparat penegak hukum untuk melakukanpenemuan hukum. Hal ini dapat dilakukan dengan menerapkan merode interprestasi (penafsiran) hukum sebelum adanya payung hukum yang memadai. Sehingga, diharapkan tidak akan terjadi kekosongan hukum dalam menuntut dan mengadili para pelaku *cyber crime* di indonesia.

B. Rumusan Masalah

1. Bagaimana kedudukan alat bukti digital dalam perkara kasus *cyber crime*?
2. Faktor yang mempengaruhi terjadinya kejahatan mayantara (*cyber crime*)

C. Metode Penelitian

Penelitian hukum adalah suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi. Dalam pembahasan masalah, penulis sangat memerlukan data dan keterangan dalam penelitian ini. Untuk mengumpulkan data dan keterangan, penulis menggunakan metode sebagai berikut :

1. Tipe Penelitian

   Mengacu pada perumusan masalah, maka penelitian yang dilakukan adalah penelitian Hukum Normatif. Penelitian normatif adalah penelitian yang menggunakan data sekunder yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier, dengan identifikasi secara sistematis Norma-norma Hukum.
2. Sumber Bahan

   Dalam Penelitian ini Penulis melakukan pengumpulan bahan hukum yang mencakup :

   a. Bahan hukum primer, Bahan hukum primer adalah salah satu sumber hukum yang penting bagi sebuah penelitian ilmiah hukum yang bersifat yuridis normatif. Bahan hukum primer meliputi bahan hukum yang mempunyai kekuatan mengikat sebagai landasan utama yang dipakai dalam rangka penelitian. Bahan hukum yang

difokuskan oleh peneliti adalah peraturan perundang-undangan yang berkaitan dengan hukum di bidang kepidanaan. 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.

b. Bahan hukum sekunder, yaitu bahan-bahan yang memberikan penjelasan bahan hukum primer, penulis menggunakan bahan hukum sekunder meliputi; buku literatur, karya ilmiah maupun hasil penelitian, jurnal, artikel, arsip-arsip yang mendukung dan bahan-bahan hukum lainnya yang dimuat dalam media elektronik di internet yang berkaitan untuk dijadikan bahan perbandingan.

c. Bahan hukum tersier, yaitu bahan hukum yang memberi penjelasan terhadap bahan hukum primer dan sekunder seperti kamus hukum dan kamus bahasa Indonesia.

PEMBAHASAN

A. Kedudukan Alat Bukti Digital Dalam Perkara *Cyber Crime*

Dalam menangani kasus *cyber crime* aparat penegak hukum harus memperhatikan mengenai alat bukti digital yang digunakan oleh pelaku dalam melakukan perbuatannya. Karena alat bukti digital tersebut mempunyai kedudukan yang sangat penting dalam rangka proses pembuktian di Persidangan Pengadilan. Dari alat bukti digital tersebut yang nantinya juga akan menentukan apakah perbuatan yang dilakukan oleh terdakwa benar bersalah menurut hukum.

Pertimbangan hakim dalam mengungkap fakta di persidangan dengan menggunakan alatbukti digital ialah pada Pasal 5 ayat (1) Undang-Undang No. 11 tahun 2008 tentang InformasI dan Transaksi Elektronik menjelaskan "Informasi Elektronik dan/atau Dokumen Elektronikdan/atau hasil cetaknya merupakan alat bukti hukum yang sah". Untuk mengungkap alat buktidigital maka hakim memerlukan saksi ahli dalam menjelaskan alat bukti tersebut seperti yang tercantum pada Pasal 1 angka 1 dan angka 4 yang menjelaskan "angka 1 : Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan,suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses,simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya, angka 4 : Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital,elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara,gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, symbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya". Sehingga dapat kita ketahui kedudukan alat bukti digital dalam ketiga putusan diatas adalah bahwa dalam pengungkapan fakta di persidangan dalam rangka menemukan kebenaran materiil, Majelis Hakim membutuhkan alat bukti digital dalam perkara *cyber* crime dan peran saksi ahli dalam menguatkan peran kedudukan alat bukti digital tersebut, karena dalam Pasal 1 angka 1 dan angka 4 Undang-Undang No. 11 tahun 2008 menjelaskan bahwa Informasi Elektronik dan Dokumen Elektronik hanya bisa dipahami oleh orang yang mampu memahaminya, orang yang mampu memahaminya berarti mempunyai keahlian dalam bidang.

Informasi dan Transaksi Elektronik, dalam hal ini disebut saksi ahli, yang didalam putusan diatas saksi ahli diperintahkan untuk menjelaskan kedudukan alat bukti digital kepada majelis hakim. Karena kedudukan alat bukti digital dalam putusan diatas mempengaruhi pertimbangan hakim untuk membuat putusan.

Berdasarkan 3 Putusan *cyber crime* di atas dapat diketahui alat bukti digital diatas yang digunakan adalah :

1. Laptop
2. Email
3. CD
4. Software (Uniblue Spyerasser)
5. Smartphone
6. CPU (Central Processing Unit)
7. Flashdisk
8. Data

9. Konten Film Porno
10. Rekaman CCTV
11. SMS

Alat bukti digital adalah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi persyaratan formil dan persyaratan materiil yang diatur dalam Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Barang bukti dapat dikatakan alat bukti digital karena berbentuk Informasi Elektronik dan/atau Dokumen Elektronik yang sesuai dengan kriteria Pada Pasal 1 angka 1 dan angka 4 Undang-Undang No. 11 tahun 2008 yang meliputi tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya dan bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya, yang dalam putusan diatas merupakan alat bukti yang mempunyai kedudukan untuk menjelaskan suatu tindak *cyber crime* yang mungkin dilakukan oleh tersangka, sehingga alat bukti digital ini memperjelas fakta yang terjadi dengan didukung alat bukti lainnya.

Yang membedakan antara Informasi Elektronik dan Dokumen Elektronik ialah sarana yang dipakai dalam pembuktian alat bukti digital tersebut, sesuai dengan Pasal 1 angka 1, Informasi Elektronik hanya terbatas pada orang yang mampu memahami Informasi yang selanjutnya dapat mengartikan Informasi Elektronik tersebut , sedangkan pada Pasal 1 angka 4 menggunakan sarana komputer dan/atau sistem elektronik untuk menerjemahkan Informasi yang ada dalam Dokumen Elektronik. Yang dimaksud Sistem Elektronik ialah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik (Penjelasan Pasal 1 angka 5 Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik). Sehingga dalam pengungkapan fakta ketiga putusan diatas harus bias membedakan Informasi Elektronik dan Dokumen Elektronik untuk meminimalisir multitafsir yang mungkin terjadi oleh hakim pengadilan. Dalam Pasal 183 KUHAP "*Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya*".

Pembuktian menggunakan alat bukti digital, hakim harus bisa mengungkap fakta dan mendapat minimal 2 alat bukti untuk memperoleh keyakinan bahwa suatu tindak pidanabenar-benar terjadi dan bahwa terdakwalah yang melakukannya. Hakim Pengadilan Negeri Surakarta Kun Maryoso, S.H, M.H menjelaskan *cyber crime* merupakan kejahatan dunia maya, pengungkapannya menggunakan alat bukti digital dan saksi ahli yang benar-benar ahli di bidangnya untuk memberikan pengertian tentang peristiwa menurut kacamata ahli, hal ini untuk meminimalkan multi tafsir dengan hakim yang lain karena, kedudukan alat bukti digital ini sebagai petunjuk atau surat dan/atau dokumen elektronik yang dijelaskan dalam Undang- Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.20 Kedudukan alat bukti digital ketiga putusan tersebut sebagai petunjuk atau surat dan/atau dokumen elektronik yang telah dijelaskan dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, sehingga dibutuhkan saksi ahli untuk memahaminya seperti yang dijelaskan pada Pasal 1 angka 1 dan angka 4 Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dalam Undang-Undang No. 11 tahun 2008 dalam Pasal 5 ayat 1 "*Informasi Elektronik dan/atau Dokumen Elektronik merupakan alat bukti yang sah".* Sehingga dalam hal menentukan tentang tata cara pembuktian alat bukti digital Bhudhi Kuswanto, S.H menjelaskan sebagai berikut :

1. Saksi ahli diperintahkan untuk memaparkan tentang pengetahuannya mengenai kasus yang sedang di sidangkan.
2. Kemudian Penyidik dari Polisi wajib menyalin/meng*copy* atau informasi elektronik tersebut dalam satu perangkat yang baru, kemudian bukti

digital tersebut dihadirkan di muka persidangan.

3. Lalu saksi ahli membuat analisis tentang alat bukti digital tersebut untuk menjadi pertimbangan hakim.

Untuk menjaga keaslian dari bukti digital maka penegak hukum mempunyai prosedur sendiri dalam menangani alat bukti digital yang menjadi barang bukti di Pengadilan, Prosedur yang digunakan ialah sebagai berikut :

1. Proses Acquiring dan Imaging
   Setelah pe nyidik menerima barang bukti digital, maka harus dilakukan proses acquiring dan imaging yang mengkopi (mengkloning/menduplikat) secara tepat dan presisi 1:1 dari hasil kopi tersebutlah maka seorang ahli forensik dapat melakukan analisis karena analisis tidak boleh dilakukan dari barang bukti digital yang asli karena dikhawatirkan akan mengubah barang bukti.
2. Melakukan Analisis
   Setelah melakukan proses Acquiring dan imaging, maka dapat dilanjutkan untuk menganalisis isi data terutama yang sudah dihapus, disembunyikan, di-enkripsi, dan jejak log- yang ditinggalkan. Hasil dari analisis barang bukti digital tersebut yang akan dilimpahkan penyidik kepada Kejaksaan untuk selanjutnya dibawa ke Pengadilan.

Dalam prosedur pembuktian alat bukti digital di pengadilan ditegaskan pada Pasal 43 ayat (2) Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyebutkan “Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud, dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan Peraturan Perundang-Undangan”, Penegak hukum belum sepenuhnya memperhatikan prosedur yang sudah ditetapkan, seperti contohnya pada ketiga putusan diatas, yang rata-rata memberikan kebebasan bagi saksi ahli untuk langsung mengeksplore isi dari alat bukti digital yang berupa laptop, seharusnya penegak hukum sebelum menghadirkan alat bukti digital harus mencopy data dari laptop tersebut ke perangkat yang baru, sesuai dengan prosedur Acquiring and imaging, sehingga meminimalkan perubahan alat bukti yang sedang dihadirkan di Pengadilan dan tidak mengurangi nilai keaslian alat bukti tersebut. Bhudhi Kuswanto menjelaskan bahwa alat bukti digital ini sangat rentan untuk dirubah, bisa saja dirubah dalam hitungan menit tanpa diketahui siapa pun, sehingga sangat disayangkan apabila prosedur yang sudah ada tidak diimplementasikan dalam pembuktian alat bukti digital ini.

Dapat disimpulkan bahwa pemrosesan alat bukti digital pada ketiga putusan tersebut belum sepenuhnya mematuhi prosedur yang sudah digunakan, sangat dimungkinkan adanya perubahan keaslian alat bukti digital yang dihadirkan di pengadilan, tak bisa di pungkiri bahwa tersangka mungkin dikenakan putusan bebas karena, tidak terbukti melakukan suatu hal tertentu karena alat bukti nya sudah dirubah karena, kedudukan alat bukti digital ini mempengaruhi pertimbangan hakim dalam mengambil putusan.

Belum ada pemrosesan alat bukti yang sesuai prosedur, alat bukti digital yang dihadirkan di persidangan telah di explore oleh saksi ahli sebelumnya, sehingga mengurangi keaslian dari sebuah alat bukti itu sendiri, padahal dalam Undang-Undang No. 11 tahun 2008 pada Pasal 43 ayat (2) telah dijelaskan tentang pelaksanaan prosedur penyidikan dalam bidang Teknologi Informasi dan Transaksi Elektronik.

Jadi ketiga putusan diatas, belum sepenuhnya menggunakan prosedur pemrosesan alat bukti yang benar dari penyidik, sehingga mengurangi keaslian alat bukti digital, karena kedudukan alat bukti ketiga perkara tersebut sangat menentukan putusan hakim. Dalam Undang-Undang No. 11 tahun 2008 tentang Transaksi dan Informasi Elektronik pada Pasal 5 ayat (1) menjelaskan bahwa “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah”. Sehingga dalam pemrosesan alat bukti tersebut harus memperhatikan prosedur yang berlaku sesuai Pasal 43 ayat (2) Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

B. Faktor yang Mempengaruhi Terjadinya Kejahatan Mayantara *(Cyber Crime*)

Soerjono Soekamto mengemukakan bahwa secara konsepsional intidan arti

penegakan hukum terletak pada kegiatan menyerasikian hubungan nilai-nilai yang terjabarkan di dalam kaidah-kaidah yang mantap dan mengejewantah sikap tindak sebagai rangkaian penjabaran nilai terhadap akhir, untuk menciptakan memelihara dan mempertahankan kedamaian pergaulan hidup. Sebagai suatu proses penegakan hukum pada kakikatnya merupakan penerapan diskresi yang menyatakan pembuat keputusannya tidak secara ketat diatur oleh kaidah hukum. Akan tetapi mempunyai unsur penilaian pribadi demikian menurut Wayn Lafawel.[7]

Sehubungan dengan pandangan diatas menurut Soerjono Soekamto ada beberapa faktor yang mempengaruhi penegakan hukum yaitu :

a. Faktor undang-undang

b. Faktor penegak hukum

c. Faktor sarana dan fasilitas yang mendukung penegakan hukum

d. Faktor budaya dan hukum masyarakat

e. Faktor kerjasama internasional

Kelima faktor diatas merupakan faktor-faktor yang terkait satu sama lain.

Merupakan esensi dari penegakan hokum dan bekerjanya hukum dalam masyarakat. Kaitannya dengan penegakan hokum terhadap tindak pidana *cyber crime*, efesiensi maupun efektifitasnya juga tergantung pada salah satu factor sebagaimana yang dikemukakan diatas yaitu :

a. Faktor Undang-undang

Meskipun eksistensi pengaturan tindak pidana *cyber crime* tidak hanya dalam undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi juga terdapat didalam Undang-undang khusus lainnya di luar KUHP, namun masih terdapat bentukbentuk tindak pidana *cyber crime* yang belum mendapatkan pengaturan, khususnya yang menyangkut penyalahgunaan teknologi canggih. Salah satu asas dalam hukum pidana menentukan bahwa tiada perbuatan yang dapat dihukum pidana dan dan diancam dengan pidana jikalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan perundangundangan (asas legalitas). Maka pengaturan atas tindak pidana *cyber crime* yang masih belum terakomodir dalam perundangundangan dimaksud sifatnya cukup penting. Menurut Muladi bahwa secara oprasional perundang-undangan pidana mempunai kedudukan strategis terhadap system peradilan pidana. Sebab hal tersebut memberikan defenisi tentang perbuatan-perbuatan yang dirumuskan sebagai tindak pidana.

Mengendalikan usaha-usaha pemerintah untuk memberantas kejahatan dan memidana sipelaku, memberikan batasan tentang pidana yang dapat diterapkan untuk setiap kejahatan . dengan perkataan lain perundang-undangan pidana yang menciptakan legislated environment yang mengatur segala prosedur dan tata cara yang harus dipatuhi didalam berbagai perangkat system peradilan pidana.[8]

b. Faktor Penegak Hukum

Keberhasilan misi hukum pidana untuk mengulangi tindak pidana *cyber crime* tidak hanya ditentukan oleh sempurnanya hukum yang dirumuskan dalam hukum positif. Melainkan telah lebih dari itu keberhasilannya sangat tergantung kepada aparat yang melaksanakannya (penegak hukumnya) mulai dari tingkat penyidikan hingga tingkat eksekusi. Hal ini dikarenakan karasteristik yang khas dari tindak pidana *cyber crime* sebagai suatu tindak pidana yang bersifat virtual. Konsekuensinya logisnya, apparat penegak hukum harus memiliki kemampuan lebih dan profesi didalam menagani tindak pidana *cyber crime*, profesionalisme dan keberanian moral aparat penegak hukum hukum dituntut sekaligus diuji untuk melakukan penemuan hukum sehingga tidak ada alasan klasik yang bersembunyi dibalik asas legalilitas sempit bahwa aturan perundang-undangan tidak lengkap atau belum ada perundangundangan yang mengaturnya.

c. Faktor Sarana dan Fasilitas yang Mendukung Penegakan Hukum

Sarana dan Prasarana Faktor ini dapat dikatakan sebagai tulang punggung penegak hokum terhadap tindak pidana *cyber crime*. Sebab eksistensinya merupakan penopang keberhasilan untuk menemukan suatu kebenaran materil. Oleh karena itu jalinan kerja sama harmonis antara lembaga penegak hukum dengan beberapa pakar spesialis dibidangnya seperti ahli forensik, fakar telematika serta dana operasional yang menandai adalah merupakan faktor pendukung guna mengadili dan memidana atau pun mempersempit ruang gerak
pelaku tindak pidana *cyber crime*.

---

[7] Soerjono Soekamto, *Faktor-faktor yang mempengaruhi Penegakan Hukum*, Rajawali Press, Jakarta, 1983, hal. 4

[8] Muladi, *Kapita Selekta Peradilan Pidana*, Badan Penerbit UNDIP, Semarang, 1995, hal. 2

d. Faktor Budaya dan Hukum Masyarakat

Tidak kalah penting dengan faktorfaktor yang lain, faktor budaya hukum masyarakat ini juga memiliki pengaruh dan memainkan peranan penting dalam proses penegakan hukum terhadap tindak pidana *cyber crime*. Pluralisme budaya hukum ditengah masyarakat merupakan fenomena yang unik dan mengandung resiko yang potensial, sehingga sering kali menempatkan posisi dan profesi aparat penegak hukum kedalam kondisi dilematis yang pada gilirannya dapat menimbulkan ambivalensi dalam pelaksaanan peranan aktualnya.

e. Faktor Kerjasama Internasional

Melakukan kerjasama dalam melakukan penyidikan kasus kejahatan *cyber* karena sifatnya yang borderless dan tidak mengenal batas wilayah sehinggah kerja sama dan kordinasi dengan apparat penegak hukum negara lain merupakan hal yang sangat penting untuk dilakukan. Pengamanan Sistem Informasi akan memudahkan aparat kepolisian diberbagai belahan dunia melakukan identifikasi dan medapatkan bantuan dari investigator dan negara lain. Kerja sama internasional juga meliputi perjanjian kerja sama diantara negara-negara baik dalam ekstradisi maupun dalam hal pembantuan dalam upaya menghadirkan korban yang berada diluar toritorial negara.

Sebagai upaya lebih efektif dan efesiensi waktu hendaknya dalam upaya pembaharuan hokum pemeriksaan korban dan saksi dalam tindak pidana teknologi informasi dapat dilakukan melalui cara e-mail atau mesengger yang ditanda tangani dengan tanda tangan digital sebagai sahnya penyidikan, serta pemeriksaan berupa teleconfrence dalam persidangan di pengadilan.

Penerapan alat bukti informasi dan data elektronika dalam perundangundangan sering mengakibatkan multitafsir diantara aparat penegak hukum terutama pada saat pemeriksaan pengadilan. Hal tersebut dikarenakan belum adanya rambu-rambu yang jelas terhadap pengakuan alat bukti tersebut. Konsep Rancangan Unadang-undang KUHP 2000, dimana konsep ini mengalami perubahan sampai dengan 2008 telah mengatur alat bukti elektronik yaitu :[9]

Dalam Buku I (ketentuan Umum) Dibuat ketentuan mengenai alat bukti :

1. Pengertian barang (Pasal 174/178) yang didalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer.
2. Pengertian anak kunci (pasal178/182) yang termasuk kode rahasia, kunci masuk komputer, kartu magnetic, silly dan yang telah diprogram untuk membuka sesuatu. Menurut Agus Raharjo,[10] maksud dari anak kunci ini kemungkinannya adalah password atau kode-kode tertentu seperti privat atau public key infrastructure.
3. Pengertian surat (188/192) termasuk data tertulis atau tersimpan dalam disket, pita magnetic, media penyimpanan komputer atau penyimpanan data elektronik lainnya.
4. Pengertian ruang (189/193) termasuk bentangan atau terminal komputer yang dapat diaskes dengan cara-cara tertentu. Maksud dari ruang ini kemungkinan termasuk pula dunia maya atau maya atau antara *cyberspace* atau *virtual reality*.
5. Pengertian masuk (190/194) termasuk mengakses komputer atau masuk kedalam sistem komputer.

PENUTUP

A. Kesimpulan

1. Yurisdiksi kriminal berlakunya hukum pidana nasional terhadap *cyber crime* tidak cukup dengan menggunakan prinsip yurisdiksi teritorial dan ekstra teritorial yang diakui dalam hukum internasional publik tetapi juga berdasarkan prinsip yurisdiksi yang berlaku terhadap tindak pidana yang dilakukan diluar yurisdiksi negara manapun. Jadi yurisdiksi criminal berlakunya hukum pidana nasional terhadap *cyber crime* menganut quasi yurisdiksi yaitu menggunakan yurisdiksi teritorial, yurisdiksi ekstra teritorial terhadap *cyber crime* yang dilakukan didalam yurisdiksi negara lain dan ekstra territorial terhadap *cyber crime* yang dilakukan diluar yurisdiksi negara manapun.

[9] Barda Nawawi Arief, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*, PT.Citra Aditya Bakti, Bandung, 2005, hal.131-133

[10] Agus Raharjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* PT.Citra Aditya Bakti, Bandung, 2002, hal. 236

2. Kedudukan alat bukti digital ini mempengaruhi pertimbangan hakim dalam mengambil putusan. Serta sebagai pelengkap alat bukti surat seperti yang dijelaskan pada Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Sehingga dalam pemrosesan alat bukti digital harus di jaga keaslian alat bukti tersebut untuk meminimalisir berubahnya alat bukti digital karena, dapat mempengaruhi proses persidangan. Dari hasil penelitian ketiga Putusan yang didapat penulis di lapangan, belum ada pemrosesan alat bukti yang sesuai prosedur, alat bukti digital yang dihadirkan di persidangan telah di explore oleh saksi ahli sebelumnya, sehingga mengurangi keaslian dari sebuah alat bukti itu sendiri, padahal dalam Undang-Undang No. 11 tahun 2008 pada Pasal 43 ayat (2) telah dijelaskan tentang pelaksanaa prosedur penyidikan dalam bidang Teknologi Informasi dan Transaksi Elektronik**.** Sistem pembuktian dalam perkara tindak pidana cyber crime dengan cara perluasan alat bukti dalam KUHAP sebenarnya sudah diatur dalam berbagai perundang-undangan secara tersebar. Dengan demikian email, suara, gambar,kode akses, simbol, dan berbagai dokumen elektronik lainnya mempunyai kekuatan pembuktian yang setara dengan alat bukti lainnya yang diatur didalam KUHAP dan dapat digunakan sebagai alat bukti yang sah.

B. Saran

1. Dalam pengaturan yuridiksi *cyber crime* kerja sama internasional sangat penting dalam memberantas tindak pidana *cyber crime* terutama dalam proses penyelidikan dan penyidikan. Disini perlu ditingkatkan kemampuan sumber daya aparat penegak hukum terutama dibidang *cyber crime* ditingkatkan sarana dan prasarana dalam bidang teknologi informasi dan komunikasi.
2. Penegak hukum pada system pembuktian dalam perkata tindak pidana *cyber crime* harus lebih meningkatkan upaya dengan cara mementingkan efektif dan efesiensi waktu, hendaknya dalam upaya pembaharuan hukum pemeriksaan korban dan saksi dalam tindak pidana teknologi informasi dapat dilakukan melalui cara e-mail atau mesengger yang ditanda tangani.

DAFTAR PUSTAKA

Arief Nawawi Barda, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*, PT.Citra Aditya Bakti, Bandung, 2005

Muladi, *Kapita Selekta Peradilan Pidana*, Badan Penerbit UNDIP, Semarang, 1995

Raharjo Agus, *Cybercrime,* PT Citra Aditya Bakti, Bandung, 2002

Suhariyanto Budi, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi dan Pengaturan Celah Hukumnya*, Jakarta, 2012

Soekamto Soerjono dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Raja Grafindo Persada, Jakarta, 1995

Perundang-Undangan

Undang-Undang Nomor 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana

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

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

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