# KONSTRUKSI HUKUM DALAM PEMBUKTIAN TERHADAP KEJAHATAN MAYANTARA

Ni Luh Ketut Dewi Yani Putri, Program Studi Magister Ilmu Hukum Fakultas Hukum Universitas Udayana, E-mail: Dewi_yaniputri@yahoo.com

doi: https://doi.org/10.24843/KS.2020.v08.i08.p08

***ABSTRAK***

*Tujuan penulisan ini untuk memenuhi dan melengkapi persyaratan untuk memperoleh gelar Magiter Ilmu Hukum pada Fakultas Hukum Universitas Udayana. Tujuan khusus dari penulisan ini yaitu untuk mengetahui pembuktian serta yurisdiksi kejahatan mayantara dalam persidangan dan konstruksi hukum dalam peraturan perundang-undangan di Indonesia. Metode yang digunakan merupakan metode penelitian hukum normatif melalui pendekatan perundang-undangan dan pendekatan konsep. Teknik yang digunakan melalui studi kepustakaan yang diperoleh langsung dari bahan hukum primer berupa peraturan perundang-undangan dan literatur hukum yang terkait. Hambatan proses pembuktian dan yurisdiksi cyber crime yakni belum diaturnya alat bukti elektronik secara sah dalam KUHAP, masih diperdebatkannya kesaksian de auditu, serta sulit menemukan saksi yang berkompeten dalam menyaksikan kegiatan cyber crime. Mengenai yurisdiksi dalam kegiatan cyber crime juga perlu diatur kembali mengingat sangatlah sukar untuk memastikan dimana kejadiannya, kapan dilakukannya dan bagaimana perbuatan pelakunya, mengingat kejahatan ini merupakan global crime yang tidak jelas yurisdiksinya di samping berkaitan dengan cyber space yang pelakunya tidak kasat mata. Adapun Kebijakan Terhadap Kejahatan Mayantara (Cyber Crime) yakni melalui modernisasi hukum pidana adapun beberapa alternative seperti Menghilangkan beberapa pasal- pasal pada Undang- Undang Cyber Crime yang tidak dipakai lagi (usang), Mengamandemen KUHP, Mengamandemen KUHAP, Mengamandemen Undang-Undang Teknologi Informasi, Dalam Pembuktian cyber crime aparat penegak hukum terutama hakim harus berani melakukan "rechtsvinding".*

***Kata kunci:****Konstruksi Hukum, Pembuktian, Kejahatan, Mayantara*

***ABSTRACT***

*The purpose of this writing is to fulfill and supplement the requirements for the Magiter degree of legal sciences at the Faculty of Law of Udayana University. The specific purpose of this writing is to know the evidence and the jurisdiction of crime between the law in the trial and the construction of laws in Indonesia's laws and regulations. The method used is a normative legal research method through a statutory approach and a concept approach. Techniques used through literature studies obtained directly from the primary legal material in the form of legislation and related legal literature. The barriers to the proving process of cyber crime and jurisdiction are not in the legitimate electronic proof tool in the criminal CODE, still in the testimony of De Auditu, and difficult to find witnesses who are competent in witnessing cyber crime activities. Regarding the jurisdiction in cyber crime activities also need to be rearranged considering that it is difficult to ensure where the event, when it does and how the perpetration, considering this crime is a global crime that is unclear its jurisdiction in addition to the cyber space that the perpetration of invisible eyes. The policy on Cyber Crime is through the modernization of criminal law as some alternative such as eliminating some of the articles on Cyber Crime laws that are not used anymore (obsolete), amend KUHP, amend KUHAP, amend the Information Technology law, in proving Cyber Crime law enforcement officials, especially the judges must dare to do "rechtsvinding".*

***Keywords:*** *Legal Construction, Prove, Cyber Crime*

## I. Pendahuluan

### 1.1 Latar Belakang Masalah

Di Era ini perkembangan kemajuan teknologi sangatlah pesat. Lompatan yang luar bisa telah dialami oleh teknologi yang merupakan salah satu produk dari modernitas. Teknologi memungkinkan aktivitas umat tidak semata-mata dalam dunia nyata, akan tetapi virtual. Hal ini memungkinkan manusia melakukan aktivitas dalam dunia maya. [1] . Dekade terakhir ini, telah menimbulkan penyimpangan melalui demensi terbaru sebagai hasil dari penyalahangunaan internet. Definisi dari Internet adalah sebuah jaringan komputer yang menghubungkan dirinya masing-masing dengan media komunikasi. Ukuran yang kecil dari jaringan komputer ini seperti *Lokal Area Network (LAN)* yang kerap kali digunakan intern dibeberapa Kantor seperti Bank atau perusahaan-perusahaan besar lainnya.[2]

Dunia nyata sama halnya seperti dunia maya, ribuan penjahat beraksi melalui internet dengan tangan-tangan kriminalnya, guna mendapatkan keuntungan materi maupun hanya melampiaskan keisengannya saja. Peristiwa ini menciptakan fenomena khas yang kita kenal dengan kejahatan mayantara (yang selanjutnya disebut dalam bahasa asing yakni (*cyber crime)*. Fenomena ini mengisyaratkan suatu hal yang jelas bahwasanya *locus delicti* dari kejahatan ini adalah dunia maya. Hal ini tentu berbeda dengan kejahatan konvensional yang *locus delictinya* adalah dunia nyata. Oleh karena itu, segala aktivitas manusia di dunia maya seyogyanya tidak akan bisa lepas dari pembatasan dan pengaturan hukum. Pada dasarnya kita sangatlah memerlukan pengaturan serta pembatasan, terlebih lagi karena setiap orang memiliki kewajiban, hak-hak setiap orang tentu dibatasi oleh hukum karena hukum menjamin pengakuan kebebasan setiap insan.

Seyogyanya kejahatan dunia maya banyak jenisnya, penipuan kredit dan perbankan adalah salah satu kategori kejahatan yang potensinya amatlah besar terjadi melalui *online banking*. Orang-orang diluar sana banyak mempunyai kemampuan dalam bidang teknologi informasi senantiasa memiliki niat buruk ditengah-tengah kelengahan pihak bank dan nasabah. [3] Kejahatan mayantara memiliki karakteristik karena dalam hal ini target korban tidak ditentukan sebelumnya, maka pengguna jasa internet harus berhati-hati.[4]

---

[1] Danrivanto Budhijanto, *Revolusi Cyberlaw Indonesia Pembaharuan dan Revisi Undang-Undang Informasi dan Transaksi Elektronik* 2016, PT Refika Aditama, Bandung, 2017, h. 26

[2] Agus Raharjo, , *Cybercrime*, PT Citra Aditya Bakti, Bandung, 2002, h. 59.

[3] Tri Kuncoro, Penegakan Hukum Terhadap Cyber Crime Di Bidang Perbankan Sebagai Kejahatan Transnasional, *Jurnal Magister Hukum Udayana*, 2 no. 3 (2013),, Hal: Doi : http:// do.org/10.24843/JMHU.2013.v02.i03. Po8.

[4] Gde Aditya Waisnawa, Kebijakan Formulatif Pengaturan *Cyberbullying* Sebagai Salah Satu Bentuk Tindak Pidana *Cybercrime* Di Indonesia, Jurnal Magister Hukum Udayana, 6 no.4, 2017,, 439-449, Doi: Https://Doi.Org/10.24843/JMHU.2017.V06.I04.P03

Beberapa pelanggaran yang sering terjadi di Indonesia selain pelanggaran diatas yakni antara lain :

- Penipuan terhadap bursa efek,
- Pornografi terhadap anak,
- Penyeludupan narkoba,
- Kejahatan terorisme
- Penyalahgunaan data dan informasi pelanggan oleh perusahaan, seperti :
    - Kasus KTP yang memiliki data dan informasi yang berbeda dengan sebenarnya,
    - Pelanggaran terhadap privasi atas data dan informasi.[5]

Sementara itu di Indonesia banyak terdeteksi kejahatan mkayantara. Perusakan situs web merupakan salah satu kasus yang viral di Indonesia dan terjadi berulang kali, segelintir kasus yang pernah terjadi yakni :

- Ditahun 2001, tepatnya pada bulan April, crakcker telah merusak situs dan file-file penting milik Depag dan Deperindag. Ulah crakcker sama sekali tidak meninggalkan jejak sehingga mengalami kesulitan pendeteksian oleh administrator. Disamping itu sesungguhnya banyak jenis kejahatan yang juga dapat dikategorikan sebagai cyber crime, seperti halnya cyber fraud.
- Definisi Cyber squatting yakni perilaku demi memperoleh, memperjualbelikan serta menggunakan domain dengan itikad baik dan jelek. Kasus yang terjadi antara PT Mustika Ratu dan Tjandra, pihak yang mendaftarkan nama domain tersebut. Kasus ini sudah diputus di Pengadilan Negeri Jakarta Pusat melalui putu/PID.B/2001 /PN.JKT.PST, putusannya membebaskan terdakwa yang bernama Tjandra yang semula didakwa dengan Pasal 382 bis KUHP dan Pasal 48 ayat (1) Jo.Pasal 19 huruf b Undang-Undang Nomor 5 Tahun 1999.

Demikianlah beberapa contoh kasus yang terjadi berkaitan dengan cyber crime. Dari kasus yang ada bahkan jarang sampai keranah litigasi dikarenakan belum konkrit dan masih menjadi polemik dalam regulasinya. Undang-Undang Nomor 19 Tahun 2006 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sudah mengatur seluruh permasalahan di media sosial, meskipun kenyataannya masih lemah dibeberapa aspeknya maka diperlukan pengaturan yang lebih khusus di Indonesia. Sesungguhnya Indonesia sangat rentan akan aturan tersebut. Dari keseluruhan uraian tersebut dapat disimpulkan bahwa kalau melihat unsurnya maka ada sebagian dari *cyber crime* yang bisa dijerat dengan hukum pidana Indonesia, dan sebagian lagi tidak dapat karena merupakan hal yang relatif baru. Namun demikian apabila melihat ketentuan yang mengatur tentang

[5] Sinta Dewi, *Praktik negara-negara dalam mengatur privasi dalam E-commerce*, Widya Padjajaran, Bandung, 2009, h. 58-59.

berlakunya hukum pidana maka sulit sekali. Hal ini dikarenakan *cyber crime* tidak jelas yurisdiksinya atau merupakan *global crime*.

Memerangi kejahatan Mayantara bukan sesuatu yang mudah, karena formulasi hukum di Indonesia tidak bisa menjangkau kejahatan ini. Hambatan yang signifikan yakni alat bukti yang tidak memadai untuk mengungkapkan kasus mengingat sumber dari aplikasi dan media dijalankan dari luar negeri, sudah tentu mempersulit pihak polisi dalam mencari bukti sementara kejahatan dunia maya beraneka ragam akan tetapi sulit untuk membuktikan, terlebih lagi KUHAP dan KUHP belum sepenunya mengatur mengenai pembuktian kejahatan mayantara serta yurisdiksi kejahatan mayantara.

Adapun rumusan permasalahan dari penelitian ini yaitu bagaimana hambatam dalam pembuktian dan yurisdiksi dalam kejahatan mayantara ? dan bagaimana konstruksi hukum terhadap kejahatan mayantara ? Terdapat tujuan umum dan khusus dalam penelitian ini antara lain tujuan umum yaitu memahami lebih jauh mengenai kejahatan Mayantara (Cyber Crime) serta tujuan khusus yakni mendeskripsikan pembuktian serta konstruksi hukum dalam kejahatan Mayantara.

Penelitian tentang kriminalisasi pembuktian terhadap kejahatan mayantara (cyber crime) ini dari segi substansinya ini menyerupai dengan penelitian yang dilaksanakan sebelumnya yakni: Penelitian oleh Tri Kuncoro, melakukan penelitian pada tahun 2013. Penelitian tersebut berjudul penegakan hukum terhadap Cyber Crime di bidang Perbankan sebagai kejahatan Transnasional, volume 2, No.3, Adapun hasil dari penelitian tersebut yakni macam-macam bentuk dari cyber crime dalam perbankan dan yurisdiksi penegakan hukum dibidang perbankan yaitu yurisdiksi menerapkan segala hal yang ditentukan oleh badan legislative serta yurisdiksi memaksakan segala hal ketentuan hukum oleh badan eksekutif.

Penelitian lain menyerupai dengan penelitian ini yaitu penelitian yang dilakukan oleh Supanto, melakukan penelitian pada tahun 2016, Penelitian tersebut berjudul Perkembangan kejahatan teknologi informasi (cyber crime) dan antisipasinya dengann penal policy, volume 5, No 1, adapun hasil dari penelitian tersebut yakni Undang-Undang Nomor 16 Tahun 2019 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik sebagai bagian dari tata hukum Indonesia dan inventarisasi peraturan perundang-undangan kejahatan terhadap teknologi informasi. Karakteristik cyber world sudah tentu melibatkan yurisdiksi berbagai negara, maka dari itu pengadopsian kebijakan untuk melindungi korban dan menjerat pelaku diluar yurisdiksi dengan perjanjian ekstradisi dengan kulturisasi cyber crime sangatlah hal yang relevan.

Berdasarkan hal itu maka dalam hal ini sangat diperlukan upaya konstruksi hukum atau memperbaharui KUHP dan KUHAP. Dengan demikian ada kekosongan hukum dalam kaitannya dengan *cyber crime*. Maka dari itu perlu pengaturan untuk mengembangkan sistem pengelolaan dan pengolahan data dan informasi yang baik sehingga akan meningkatkan berbagai urusan

yang diperlukan masyarakat. [6] Maka dari itu akan menciptakan hal yang perlu untuk dibahas mengenai "Konstruksi Hukum Dalam Pembuktian Terhadap Kejahatan Mayantara"

## 2. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif. Doktrin serta asas-asas hukum yang telah terkonsep sebagai kaidah yang berlaku tentu menjadi acuan. Pada penelitian ini digunakan pendekatan perundang-undangan dengan menelisik peraturan perundang-undangan yang berhubungan dengan *cyber crime* serta mempergunakan pendekatan konsep *(conceptual approach)* dengan menganalisis bahan hukum yang terkait dengan permasalahan hukum yang ditangani. Sumber bahan hukum yang dipergunakan yakni Bahan hukum primer seperti Undang-Undang Cybercrime, KUHAP, dan Bahan hukum sekunder yang dipergunakan antara lain buku, jurnal maupun artikel lainnya. Penelian ini mempergunakan teknik pengumpulan dengan sistem kartu dengan membuat catatan-catatan penting setelah menemukan semua bahan,[7] kemudian akan dianalisis secara deskriptif kualitatif.

## 3. Hasil Dan Pembahasan

### 3.1 Hambatan Dalam Pembuktian dan Yurisdiksi Kejahatan Mayantara Pembuktian

Hukum pidana menjelaskan perdebatan tentang masih atau tidak relevannya model pembuktian konvensional ketika dihadapkan pada kejahatan *cyber crime*. Sebelum ada putusan hakim yang *inkracht van gewijsde* karena setiap orang tidak dapat dikatakan bersalah begitu saja, sebelum ada pembuktian berdasarkan asas praduga tak bersalah. Dalam hal inilah hukum pembuktian memegang peranan penting, karena pembuktian itu untuk membetulkan kejadian sehingga dapat diterima oleh akal sehat.[8] Oleh karena itu maka hukum acara pidana bukan untuk mencari kebenaran formil akan tetapi kebenaran materiil.[9] Pembuktian perkara pidana memiliki perbedaan dalam bidang pembuktiannya, setiap negara memiliki sistem pembuktian yang tidak sama, begitu juga dengan alat buktinya.[10] KUHAP menganut teori pembuktian

[6] Konsepsi RUU Tentang perlindungan Data dan Informasi Pribadi, h. 3-5

[7] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif*, PT Raja Grafindo Persada, Jakarta, 2007, h. 52.

[8] Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana*, Mandar Maju Bandung, 2003, h. 7.

[9] Andi Hamzah , *Hukum acara Pidana Indonesia Revisi*, Sinar Grafika, Jakarta, 2001, h. 257.

[10] *Ibid*, h. 266.

berdasarkan Undang-Undang secara negatif.[11] Dalam hal itu hakim akan terikat akan alat bukti, keyakinan dan hati nurani ketika memutuskan.[12]

Berdasarkan Pasal 183 Kitab Undang-Undang Hukum Acara Pidana (yang seterusnya disingkat (KUHAP) menyimpulkan bahwasanya dalam penjatuhan pidana hakim tidak diperkenankan memutuskan kecuali sekurang-kurangnya ada 2 alat." Di dalam Undang- Undang Nomor 14 Tahun 1970 tentang Ketentuan-ketentuan Pokok Kekuasaan Kehakiman dalam pasal 6 ayat (2) senada menyimpulkan bahwa tidak ada satupun yang dikenakan pidana, kecuali apabila pengadilan karena alat-alat bukti yang sah menurut undang-undang, mendapat keyakinan, bahwa seseorang yang dapat dianggap bertanggung jawab telah bersalah atas perbuatan yang dituduhkan atas dirinya. Berdasarkan hal itu tercantum dua ketentuan antara lain keyakinan yang didasarkan bukti-bukti dan keyakinan Hakim.[13] Selain itu peralatan yang dipergunakan semua berbasis elektronik. Maka perdebatanpun timbul mengenai alat bukti elektronik dalam kejahatan mayantara ini terutama di kalangan praktisi hukum.

Penggunaan alat bukti elektronik sesungguhnya tidak diberi petunjuk didalam KUHAP. Jika diungkap lebih dalam sebenarnya pada kejahatan ini, data elektronik dikategorikan sebagai bukti pada peristiwa pidana tersebut. Namun jika dilihat di KUHAP dalam Pasal 184 menjelaskan bahwasanya alat bukti yang dinyatakan sah yakni saksi, saksi ahli, surat, petunjuk, dan pengakuan terdakwa.

**Saksi**

Permasalahan dalam kasus cyber crime ini adalah alat bukti saksi , karena sangatlah sukar untuk menyaksikan langsung peristiwa yang terjadi, hal itu diakibatkan karena sifatnya yang virtual yang senantiasa sukar diprediksi semuanya. Kondisi itu menyebabkan sangat sukar memperoleh nilai kesaksian. Hal yang paling mungkin kesaksian *de auditu*, artinya keterangan oleh saksi tersebut bukan berasal dari diri sendiri, seumpama pelaku mempunyai forum diskusi dalam internet, namun saling mengetahui dari identitas masing-masing, maka anggota kelompok ini dapat dipanggil untuk diminta keterangannya dalam penyelidikan dan penyidikan.

Secara harfiah arti ketentuan pasal tersebut bahwa kesaksian tersebut tidak dapat dikategorikan sebagai keterangan saksi sekaligus alat bukti karena kesaksian tersebut tidak dilakukan secara langsung, sedangkan dalam Pasal 1 KUHAP pada poin 26 mendefinisikan saksi sebagai seseorang yang mampu memberikan keterangan yang dialami sendiri untuk tujuan penyidikan,

[11] *Ibid*, h. 262.
[12] Hari Sasangka dan Lily Rosita, *Op.Cit*, h. 13.

[13] Edmon Makarim, *Kompilasi Hukum Telematika*, Raja Grafindo Persada, Jakarta, 2003, h. 432.

penuntutan, bahwa artinya kesaksian de auditu tidak selaras dengan essensi dari acara pidana yang ingin mencari kebenaran materil. Walaupun demikian hakim tidak dapat begitu saja mengesampingkan kesaksian ini karena dapat digunakan sebagai pertimbangan yang memperkuat keyakinan hakim dalam putusannya.[14] Di samping itu kesaksian *de auditu* dapat memberi petunjuk bagi hakim dalam mendapatkan bukti yang lain.[15]

Bahwa sesungguhnya di Negara kita kesaksian de auditu masih terjadi pro dan kontra. Seperti halnya Landraad Teluk Betung pada tanggal 14 Juli 1938 menolak. Ketetapan itu diresmikan di Batavia oleh Raad Van Iustitia. Dalam penetapan Landraad Meester Cornelis, pada dasarnya telah setuju untuk membebankan bukti pada kesaksian de auditu. Yurisprudensi yang memperbolehkan kesaksian *de auditu* ini dapat dipertimbangkan mengingat kejahatan tersebut *cyber crime* sangat sulit untuk dibuktikan. Walaupun demikian tidak boleh menggeneralisir masalah. Akan tetapi dalam penggunaan yurisprudensi tersebut harus kasus perkasus. Selanjutnya adalah yang berkenaan dengan alat bukti elektronik. Dalam interaksi di internet sering menggunakan *e-mail*, *chatting* dan sebagainya. Jelasnya semua dokumen atau data bersifat elektronik. Demikian hal ini bersifat elektronik.

**Surat**

Dalam bukti surat antara KUHAP dan KUHPER agak berbeda. Dalam KUHPER ketentuan dalam pasal 187 (1) tersebut ada pembedaan dalam nilai pembuktian. Pada poin a pasal tersebut mempunyai kekuatan pembuktian sempurna. Artinya mengikat hakim sepanjang tidak dibuktikan sebaliknya. Pembedaan ini tidak ditemukan dalam KUHAP. Dalam pasal tersebut point a, b, c sudah jelas, misalnya dalam surat ancaman terdakwa kepada korban pembunuhan. Dalam kasus peretasan maupun kasus cyber diluar sana, server yang merupakan jaringan ISP yang merupakan tempat untuk menyimpan data log ditemukan sebagai bukti elektronik, isinya yakni berupa tangkapan catatan keseharian konsumen internet. Seumpama pada hacking, harus ditentukan penemuan-penemuan surat terlebih dahulu. Terdapat beberapa kemungkinan, yakni surat kertas dan digital seperti email dan lain –lainnya.[16]

*Email* sudah barang tentu dapat dicetakan. Email yang dicetak tersebut ini merupakan bentuk fisik dari surat digital yang disebut dengan *print out*, di mana keterangan itu didapatkan dari Internet Service Provider, yakni sejenis Perseoran Terbatas untuk pelayanan internet dan Perseroan Terbatas untuk telepon. Hasil cetakan itu dapat dijadikan suatu bukti apabila saling berhubungan dengan bukti lainnya, hal tersebut sesuai dengan bunyi pasal 187 ayat I huruf d KUHAP. Hal tersebut sebagai dasar untuk alat bukti dan cetakan

[14] *Ibid*, h. 425-426.
[15] Hari Sasangka dan Lily Rosita, *Op.Cit*, h. 36.

[16] Edmon Makarim, *Op.Cit*, h. 435.

ini dapat ditunjang dan dianalogikan terhadap bukti saksi ahli, kemudian diharuskan untuk disertifikasi terlebih dahulu oleh Telkom atau Departemen Pariwisata pos dan telekomunikasi, maka barulah dapat diakui keotentikannya.

Melihat fenomena tersebut dengan melihat dari banyaknya kasus *cyber crime* di Indonesia maka sudah saatnya diakui keberadaan alat bukti elektronik sebagai alat bukti karena sesungguhnya alat bukti elektronik belum terdapat pengaturannya dalam KUHAP sedangkan nantinya dalam proses penyidikan dan penyelidikan mengenai cyber crime mengacu dalam KUHAP.

**Keterangan / saksi Ahli**

Telah dinyatakan dalam KUHAP pada pasal 186 yang menerangkan bahwasanya keterangan ahli merupakan apa yang dinyatakan oleh seorang ahli dalam persidangan Pengadilan sesuai dengan keilmuannya masing-masing. Umumnya pelaku peretas dalam kejahatan mayantara lainnya akan dengan mudah melenyapkan bekas, semisal melalui penghapusan data pada Internet Service Provider. Jika ini berlangsung akan menyebabkan kesulitan dalam membuktikannya. Dalam keadaan ini para saksi ahli dapat menuntun dan dapat dianggap sebagai alat bukti. Maka keterangan yang dilontarkan didepan penyidik bukanlah alat bukti keterangan ahli.

**Yurisdiksi**

Kejahatan Mayantara jika dikaitkan dengan proses Litigasi, dengan jurisdiksi dan penuntutan akan menjadi lebih rumit lagi, mengingat kejahatan ini merupakan global crime yang tidak jelas yurisdiksinya di samping berkaitan dengan *cyber space* yang pelakunya tidak kasat mata. Berkaitan dengan jurisdiksi KUHP memang ada pasal yang berupaya memperluas penuntutan yaitu Pasal 3, pasal 4 ( asas universal), Pasal 5 (asas personal), pasal 7, Pasal 8, akan tetapi ketentuan pasal-pasal itu terbatas pada delik-delik tertentu saja di samping juga subjek hukum tertentu. Dari sini terlihat bahwa KUHP sangat terbatas sekali untuk diterapkan terhadap *cyber crime.* Hambatan lain mucul karena kejahatan mayantara kerap menyusahkan yurisdiksi hukum, namun hal itu bisa diatasi apabila terdapat alat bukti yang cukup, dan pembuktian itu sulit dilakukan karena aktivitas dunia maya tak memiliki batasan oleh territorial negara, dunia maya tak memiliki wujud sehingga peraturan tradisional terkadang sukar dalam mencari alat bukti , hal itu dikarenakan data elektronik bisa diubah, disadap, dan digandakan

Berkenaan dengan yurisdiksi serta kebijakan aktivitas dunia maya ini kemudian terjadi problematika dengan persoalan yakni siapa yang memiliki hak untuk meciptakan regulasi dalam melaksanakan penuntutan dan proses peradilan, mengingat cyber space tidak jelas *locus delictinya* selain itu juga melewati batas teritorial negara. Akhirnya ini berkaitan dengan otoritas mana

yang berhak mengatur internet. Dalam hal ini maka harus ditentukan lebih dahulu ruang lingkup cyber law.[17]

### 3.2 Konstruksi Hukum Terhadap Kejahatan Mayantara

Secara potensial *cyber crime* merugikan sebagian bidang, seperti ekonomi, politik, sosial serta budaya yang menimbulkan sesuatu yang signifikan dan menimbulkan keprihatinkan. Apabila berbanding dengan kejahatan dan pelanggaran yang memiliki intensitas tinggi, dan di zaman modern nanti perekonomian nasional dengan jaringan infrastrukur yang berdasarkan teknologi elektronik dapat terganggu. Melihat kejadian ini maka diperlukan upaya guna mencegah dan menanggulangi kejahatan ini. Salah satu di antara upaya penanggulangan kejahatan adalah melalui proses konstruksi hukum.[18] Berbicara masalah konstruksi hukum sesungguhnya terkait erat dengan penyusunan serta regulasi Perundang-undangan. Didalam pengertian "Penal Policy" Mark Ancel menyatakan bahwa Penal Policy merupakan pengetahuan dan suatu seni yang memiliki tujuan untuk mengizinkan aturan yang bersifat positif, yang bertujuan untuk mengatur peraturan pidana yang baik.[19] Selama ini telah muncul gagasan-gagasan yang berkaitan dengan pengaturan *cyber space*, sehingga munculah berbagai istilah *cyber law, lex informatica, the internet's Law, The telecommunication of law, the information of law on technology* serta hukum telematika.[20]

Dalam pembuktian kejahatan mayantara , sudah seharusnya KUHAP perlu direvisi kembali berkaitan dengan alat bukti elektronik karena dibeberapa negara maju seperti Chili, Jepang, Australia, China dan Singapura telah mengakui keberadaan alat bukti tersebut. Selain itu Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 ITE juga perlu direvisi kembali karena dalam menyusun UU ITE Pemerintah masih mempergunakan sebuah pendekatan politis-pragmatis yang lebih condong terhadap pola pikir secara praktis, akan tetapi di era sekarang sudah seharusnya mempergunakan pendekatan kebijakan publik yang secara langsung mengaitkan seluruh kalangan. Maka tidak heran dalam peraturan ini belum mengatur seluruh kejahatan yang berkaitan dengan teknologi informasi seperti misalnya kelalaian telah diatur dalam KUHP namun dalam UU ITE tidak disebutkan hal itu sehingga *hacker* dengan mudah dan leluasa untuk masuk. Selain itu mengenai transaksi narkoba dalam dunia maya belum juga

---

[17] MasWigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, Global Intiative Indonesia bekerja sama dengan Indonesia Media Law and Policy Center, 2003,.

[18] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003,, h. 240.

[19] Al Wisnubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Komputer*, Universitas Atmajaya, Yogyakarta, 1999, h. 11

[20] Agus Raharjo, *Cybercrime : Pemahaman Dan Upaya Pencegahan Berteknologi*, PT Citra Aditya Bakti, Bandung, 2002, h. 215

diatur, maka dari itu perlu dibuatkan regulasi yang berkaitan dengan *cyber law* umunya dan cyber crime secara khusus melalui " Modernisasi Hukum Pidana**"**

Sebagai modernisasi hukum pidana dalam penyusunan cyber law, perlu direvisi kembali mengenai beberapa kebijakan seperti :

- Menghilangkan beberapa pasal- pasal pada Undang- Undang *Cyber Crime* yang tidak dipakai lagi (usang).
- Mengamandemen KUHP
- Mengamandemen KUHAP
- Mengamandemen Undang-Undang Teknologi Informasi
- Dalam Pembuktian *cyber crime* aparat penegak hukum terutama hakim harus melakukan "*rechtsvinding*"

Adapun beberapa model untuk meregulasi *cyber space*, yakni diantaranya :

a. Model ketentuan payung untuk meningkatkan keharmonian dalam hukum. Model ini digunakan untuk membuat aturan mengenai segala aktivitasnya dicyber space. Adapun kelebihan dari model ini adalah dapat menciptakan karya besar melalui pemahaman keberagaman dari hal yang ingin diatur. Akan tetapi kekurangannya yakni akan timbul logis dalam menyiapkan jangka waktu yang singkat untuk semua rancangan peraturan perundang-undangan yang sifatnya mengkhusus maupun dalam pengaturan pelaksanaannya. Hal ini dilakukan untuk menghindari kekosongan hukum. Model ini bisa mengatur :

    1. Hanya materi pokok yang dimana pengaturannya yang melihat seluruh beberapa keadaan misalnya, konsumen, pihak pemerintah, aparat penegak hukum, dan pelaku usaha

    2. Adanya kaitan antara aturan hukum yang digunakan terdahulu dengan dimasa yang akan datang untuk menciptakan hubungan yang sinergis

b. Model Triangle Regulations yang digunakan untuk antisipasi dalam menghadapi lajunya aktivitas cyber space. Triangle regulations ini merupakan langkah baik menertibkan segala permasalahan yang mana yang harus diprioritaskan agar nantinya dapat seefisien dan seefktif mungkin terantisipasi, karena pengaturan ini lebih memiliki spesifikasi yang menukik. Maka dari itu sangat diperlukan pengaturan yang dimana dapat mengandung segala aktivitas pada cyber space. Dengan beralaskan skala prioritas 3 regulasi yang telah tersusun , yakni :

1. Dalam transaksi perdagangan Elektronika memuat digital signature, pembuktian, pajak, asuransi, serta perlindungan konsumen.

2. Dalam aturan mengenai perlindungan privasi terhadap pelaku bisnis dan konsumen, maka dimuat perlindungan database elektronik, catatan perusahaan individual.

3. Aturan cyber crime, yang sebenarnya dimuat yurisdiksi dan peradilan yang berkompeten dalam menangani cyber space seperti kejahatan penipuan, pemerasan, penghujatan, perdagangan anak, kejahatan seksualitas yang tidak pantas ditransmisikan.[21] Maka dalam hal ini negara-negara anggota dihimbau untuk meningkatkan anak dalam kegiatan yang positif maupun berbasis nasional atau internasional dengan tujuan untuk menanggulangi *cyber crime* , dan mengharmonisasi segala peraturan-peraturan yang berkaitan dengan kriminalisasi antara kebijakan penal dengan suatu negara, pembuktian dan segala prosedur. Berhubungan dengan karakter dari cyber wold yang memasuki batas-batas dan memiliki kompetensi dalam pelibatan yurisdiksi dari negara-negara, oleh karena itu dibutuhkan pertimbangan untuk diadopsinya segala kebijakan mengenai perlindungan korban dan dapat mempidanakan pelaku yang berada diluar negara Indonesia, yaitu mampu dengan pengkulturisasian cyber crime kedalam perjanjiana ekstradisi.[22]

Dengan demikian jika dikaitkan dengan dua model tersebut di atas pendapat ini cenderung pada pendekatan model pertama (*Umbrela Provision*). Model ini lebih sistematis dan fleksibel dalam mengikuti perkembangan dunia internet yang sangat cepat. Sebab apabila tidak ada kerangka dasar yang demikian, maka dikhawatirkan akan terjadi tumpang tindih atau bahkan saling tidak sinkron diantara beberapa peraturan. Dengan artian yang berbeda *commo ground* tersebut merupakan asas dari pengaturan *cyber space*.

Sebagaimana pengaturan *cyber law* pengaturan *cyber crime* juga menimbulkan kontroversi. Agus Raharjo tampaknya cenderung pada pendekatan yang digunakan Muladi dalam membahas Kejahatan Mayantara. Adapun beberapa Pendekatan-pendekatannya yakni :

a. Pendekatan (1) pendekatan global (*global approach*), dalam pendekatan ini memunculkan adanya peraturan baru yang tidak memiliki sifat khusus terhadap computer. Adapun cakupan bentuk perbuatannya seperti manipulasi, perusakan, pencurian dan penggunaa komputer secara melawan hukum dan tanpa kewenangan.

[21] *Ibid*, h. 222-224

[22] Supanto, Perkembangan Kejahatan Teknologi Informasi (*Cyber Crime)* Dan Antisipasinya Dengan *Penal Policy*, 5 no.1 (2016), Doi: http://dx.doi.org/10.20961/yustisia.v5i1.8718.

b. Pendekatan (2) yakni pendekatan evolusioner (*evolutionary approach*) yang mengusahakan dalam pengadaan pembaharuan mengenai rumusan kejahatan dan pelanggaran tradisional dengan maksud memasukan objek dan teknik-teknik yang dipakai dalam menjalankan kejahatan ini dalam rumusannya.

c. Pendekatan (3) merupakan suatu kompromi antara dua pendekatan yakni pendekatan global dengan pendekatan evolusioner. Kompromi tersebut dilaksanakan dengan cara pencantuman computer didalam Hukum Pidan yang telah dikodifikasikan.

Dalam rangka upaya untuk penanggulangan kejahatan mayantara, maka dalam Resolusi Kongres PBB No VIII pada Tahun 1990 mengenai kejahatan terkait computer mengusulkan kebijakan-kebijakan yakni :

1. Dalam rangka mengintensifkan upaya dalam menanggulangi penyelewengan Komputer maka dimohonkan himbauan negara anggota agar semakin efisien dan efektif melalui pertimbangan beberapa kebijakan antara lain :

    a. Kebijakan menciptaka hukum pidana yang dimodernisasi secara materiil dan formil.

    b. Melakukan pengembangan pencegahan dan keamanan Komputer

    c. Menciptakan kepekaan terhadap masyarakat, aparatur penegak hukum baik itu Badan Peradilan, Kejaksaan, Lembaga Permasyarakatan, Polisi, serta Advokat terhadap urgensi dalam mencegah cyber crime

    d. Melaksanakan pelatihan untuk semua aparatur penegak hukum dalam penanggulangan kejahatan ekonomi dan *Cyber crime* .

    e. Mengembangkan aturan etika untuk penerapan teknologi dan pengajarannya melalui informasi yang sudah terkurikulum

    f. Diadopsinya pengaturan perlindungan korban kejahatan mayantara berdasarkan Deklarasi Perserikatan Bangsa-Bangsa mengenai korban serta diambilah tindakan-tindakan guna mendorong mengajukan laporan adanya *Cyber crime*.

2. Memberikan himbauan terhadap negara-negara anggota dalam peningkatan kegiatan nasional sebagai penegakan guna menanggulangi *Cyber crime* .

3. Membuat rekomendasi kepada Komite Pengendalian dan Pencegahan kejahatan

Selain itu, hal ini akan lebih baik lagi jika berbarengan dengan beberapa institusi di Indonesia yang saling berkaitan melalui sederetan tindakan yang proaktif serta antisipatif. Misalnya tindakan yang direncanakan penerapan perlindungan konsumen oleh Asosiasi yang menaungi para *Internet Service Provider (ISP)* serta Warnet Indonesia. [23] Pada dasarnya yakni untuk mengupayakan kriminalisasi Cyber Crime ini sebenarnya dikaji permasalahan harmonisasi antara substansi dari kejahatan cyber crime dengan kebijakan formulasi kejahatan *cyber crime*. Setelah ini dilanjutkan dengan harmonisasi eksternal bersifat absolut dan sangat dibutuhkan, mengingat lagi Cyber Crime yang bersifat hakiki sebagai kejahatan dunia. Di samping memodernisasi hukum pidana nasional Indonesia juga harus aktif dalam kesepakatan internasional tentang kejahatan ini. Terutama sekali terhadap konvensi tentang ekstradisi yang berkenaan dengan *cyber crime*.

Menjawab permasalahan yurisdiksi diatas memang dalam bidang hukum pidana, kita mempunyai asas yang memperluas tuntutan pidana (ketentuan Pasal 4 sampai Pasal 8), yang memberi wewenang dalam melakukan proses peradilan pidana atas perbuatan yang dilakukan di luar wilayah Indonesia. Namun demikian, tanpa adanya kesepakatan internasional, semisal ekstradisi tentu tidak akan bisa memaksakan berlakunya hukum nasional kepada negara lain. Di samping itu juga, dalam berlakunya perluasan jangkauan penuntutan terbatas pada delik dan subjek hukum (pelaku) tertentu saja.

Kualifikasi kejahatan yang berkaitan dengan cyber crime, sudah seharusnya diciptakan dengan sejelas mungkin untuk menciptakan kepastian hukum, keadilan hukum dan kemanfaatan hukum bagi konsumen jasa internet dan masyarakat luas. Dalam hal ini SDM penyidik sangat perlu diperhatikan lagi dengan diberikan edukasi khusus mengenai Cyber Crime agar nantinya dapat memahami permasalahan Cyber Crime, selain itu juga penyidik dalam hal ini harus diberikan kompetensi khusus untuk melaksanakan kebijakan yang dibutuhkan dalam rangka proses penyidikan maupun penyelidikan mengenai kasus Cyber Crime. Menciptakan fasilitas komputer forensik dan meningkatkan penanggulangan kejahatan, pencegahan dan melakukan kerja sama.[24]

---

[23] M.E. Fuady. "Cybercrime" Fenomena Kejahatan melalui Internet di Indonesia, *Mediator Jurnal Komunikasi*, 6 (2), (2005). Doi: https://doi.org/10.29313/mediator.v6i2.1194

[24] Fiorida Mathilda, Cyber crime dalam Sistem hukum Indonesia, Jurnal Polban, 4 no. 2, (2012),, Doi : https://jurnal.polban.ac.id/index.php/sigmamu/article/view/870/74

## 4. Kesimpulan

Hambatan dalam proses pembuktian dan yurisdiksi *cyber crime* yakni belum diaturnya alat bukti elektronik secara sah dalam KUHAP, masih diperdebatkannya kesaksian *de auditu*, serta sulit menemukan saksi yang berkompeten dalam menyaksikan kegiatan *cyber crime*, mengingat aktivitas cyber crime dilakukan secara virtual. Mengenai yurisdiksi dalam kegiatan *cyber crime* juga perlu diatur kembali mengingat sangatlah sukar untuk memastikan dimana kejadiannya, kapan dilakukannya dan bagaimana perbuatan pelakunya, mengingat kejahatan ini merupakan global crime yang tidak jelas yurisdiksinya di samping berkaitan dengan *cyber space* yang pelakunya tidak kasat mata. Berkaitan dengan jurisdiksi KUHP ada pasal yang berupaya memperluas penuntutan yaitu Pasal 3, pasal 4 ( asas universal), Pasal 5 (asas personal), pasal 7, Pasal 8, akan tetapi ketentuan pasal-pasal itu terbatas pada delik-delik tertentu saja di samping juga subjek hukum tertentu. Dari sini terlihat bahwa KUHP sangat terbatas sekali untuk diterapkan terhadap *cyber crime*

- Adapun Kebijakan Terhadap Kejahatan Mayantara (Cyber Crime) yakni melalui modernisasi hukum pidana adapun beberapa alternative seperti
    - Menghilangkan beberapa pasal- pasal pada Undang- Undang Cyber Crime yang tidak dipakai lagi (usang).
    - Mengamandemen KUHP
    - Mengamandemen KUHAP
    - Mengamandemen Undang-Undang Teknologi Informasi
    - Dalam Pembuktian *cyber crime* aparat penegak hukum terutama hakim harus berani melakukan "*rechtsvinding*"

Regulasi tersebut diciptakan dengan mempertimbangkan 2 model yakni :

- Model ketentuan payung guna menciptakan keharmonisasian dalam hukum. Dalam hal ini dimuatlah ketentuan pokok melalui segala keterkaitan dengan aturan Undang-Undang,
- *Model Triangle Regulations* guna antisipasi perkmbangan aktivitas di *cyberspace.*

## Daftar Pustaka

### Buku

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

Sinta Dewi, *Praktik negara-negara dalam mengatur privasi dalam E-commerce*, Widya Padjajaran, Bandung, 2009,

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif*, PT Raja Grafindo Persada, Jakarta, 2007.

Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana*, Mandar Maju Bandung, 2003.

Andi Hamzah , , *Hukum acara Pidana Indonesia Revisi*, Sinar Grafika, Jakarta, 2001

Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana*, Mandar Maju, Bandung, 2003.

Edmon Makarim, *Kompilasi Hukum Telematika*, Raja Grafindo Persada, Jakarta, 2003.

Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003.

Al Wisnubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Komputer*, Universitas Atmajaya, Yogyakarta, 1999.

Agus Raharjo, *Cybercrime : Pemahaman Dan Upaya Pencegahan Berteknologi*, PT Citra Aditya Bakti, Bandung, 2002.

MasWigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, Global Intiative Indonesia bekerja sama dengan Indonesia Media Law and Policy Center, 2003.

Danrivanto Budhijanto, *Revolusi Cyberlaw Indonesia Pembaharuan dan Revisi Undang-Undang Informasi dan Transaksi Elektronik* 2016, PT Refika Aditama, Bandung, 2017.

### Jurnal

Tri Kuncoro, Penegakan Hukum Terhadap Cyber Crime Di Bidang Perbankan Sebagai Kejahatan Transnasional, *Jurnal Magister Hukum Udayana*, 2 no 3 (2013), Doi : http:// do.org/10.24843/JMHU.2013.v02.i03. Po8

Gde Aditya Waisnawa, Kebijakan Formulatif Pengaturan *Cyberbullying* Sebagai Salah Satu Bentuk Tindak Pidana *Cybercrime* Di Indonesia, Jurnal Magister Hukum Udayana, 6 no. 4, (2017), 439-449, Doi: Https://Doi.Org/10.24843/JMHU.2017.V06.I04.P03

Supanto, Perkembangan Kejahatan Teknologi Informasi (*Cyber Crime)* Dan Antisipasinya Dengan *Penal Policy*, 5 no. 1, (2016), Doi: http://dx.doi.org/10.20961/yustisia.v5i1.8718

M.E. Fuady. "Cybercrime" Fenomena Kejahatan melalui Internet di Indonesia, *Mediator Jurnal Komunikasi*, 6 no. 2, (2005). Doi: https://doi.org/10.29313/mediator.v6i2.1194

Fiorida Mathilda, Cyber crime dalam Sistem hukum Indonesia, Jurnal Polban, 4 2, (2012), Doi : https://jurnal.polban.ac.id/index.php/sigmamu/article/view/870/74

Dharmawan, N. Keberadaan Pemegang Saham Dalam Rups Dengan Sistem Teleconference Terkait Jaringan Bermasalah Dalam Perspektif Cyber Law. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal), 4* no. 1, (2015). doi:10.24843/JMHU.2015. v04.i01.p15

**Peraturan Perundang-Undangan**

KUHAP

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

Undang- Undang Nomor 14 Tahun 1970 tentang Ketentuan-ketentuan Pokok Kekuasaan Kehakiman