JOURNAL OF
MORAL AND CIVIC EDUCATION

# Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia

***Muhammad Prima Ersya***
Prodi Pendidikan Kewarganegaraan Universitas Negeri Padang
mprimaersya@gmail.com

***ABSTRAK***

*Perkembangan pemikiran manusia ke arah kemajuan teknologi banyak memberikan aspek positif bagi kehidupan manusia namun kemajuan teknologi juga membawa permasalahan tersendiri, khususnya dalam aspek tindak pidana. Kemajuan teknologi juga dapat dimanfaat-kan oleh pelaku tindak pidana (siber) dalam menuntaskan niat jahatnya, sehingga pada hari ini untuk melakukan kejahatan antar negara pelaku tindak pidana tidak harus hadir di negara tertentu namun ia dapat melakukannya tetap dengan berada di negaranya sekalipun di dalam kamar tidurnya. Tindak pidana siber merupakan salah satu jenis tindak pidana dengan modus yang relatif baru, tindak pidana ini merupakan jenis tindak pidana yang high tech dengan mempergunakan peralatan atau teknologi informasi yang canggih sehingga dibutuhkan respon regulasi hukum baru untuk menjangkaunya, yakni hukum siber atau cyber law dengan mempergunakan pendekatan teknologi, sosial budaya (etika) dan hukum. Metode penelitian yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mendalami aspek peraturan-peraturan hukum yang terkait dengan tindak pidana siber, sehingga hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi pihak-pihak yang ingin mendalami permasalahan hukum siber di Indonesia.*

**Kata kunci**: *tindak pidana siber; teknologi informasi; hukum siber*

***ABSTRACT***

*The development of human thinking towards the advancement of technology gives a lot of positive aspects for human life. However, technological progress also brings its own problems, especially in the aspect of criminal acts. Technological advances can also be exploited by the perpetrators of criminal acts in conducting their evil intentions, therefore, nowadays to commit international crimes, the perpetrators do not have to be present in certain countries but they can do so by staying in their country even in their bedroom. Cyber crime is a relatively new type of crime, a type of high-tech crime by using sophisticated equipment or information technology. This development required a new regulatory response to solve it, namely the law of cyber or cyber law by using technological, socio-cultural (ethical) and legal approaches. This article uses normative research method with descriptive model to deeply elaborate aspect of law in regulation about cyber crime. This research is expected to give minimum contribution for those who want to deepen the problem of cyber law in Indonesia.*

**Keywords:** *cyber crime, information technology, cyber law*



*Received: April 25 2017* *Revised: July 30 2017* *Accepted: July 31 2017*

## PENDAHULUAN

Kita telah berada dalam millenium ke III, yang ditandai dengan era teknologi informatika yang memperkenalkan kepada kita media dunia maya (*cyberspace*),

internet, yang mempergunakan komunikasi tanpa kertas (*paperless document*) (Badrulzaman, 2000). Saat ini penetrasi teknologi informasi ke dalam segala hal aspek kehidupan dirasakan bukan sebagai sesuatu hal yang awam, keseharian kita telah secara langsung maupun tidak langsung telah bersentuhan dengan media teknologi informasi ini. Oleh karena itu, kegiatan-kegiatan yang dilakukan melalui media elektronik perlu didukung perangkat hukum dalam rangka melindungi masyarakat global. Mengingat bahwa kegiatan dengan mempergunakan media elektronik telah berkembang di Indonesia maka kegiatan itu perlu didukung dengan perangkat hukum, yaitu hukum maya yang kadang-kadang disebut dengan hukum telematik, hukum elektronik. Sementara penulis lebih cenderung memilih istilah "hukum siber" sebagai padanan *cyberlaw* yang mengikuti pendapat Mariam Darus Badrulzaman (2001: 271) sebagai terjemahan dari *cyberlaw*. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara. Dengan demikian, kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer yang kemudian melahirkan piranti baru yang disebut internet (Wahid dan Labib, 2005: 103).

Internet adalah jaringan luas dari komputer yang lazim disebut dengan *worldwide network*. Internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit ataupun gelombang frekuensi. Jaringan komputer ini dapat berukuran kecil seperti *Lokal Area Network* (LAN) yang biasa dipakai secara intern di kantor-kantor, bank atau perusahaan atau biasa disebut dengan intranet, dapat juga berukuran super besar seperti internet (Raharjo, 2002: 59). Sementara *The US Supreme Court* mendefinisikan internet sebagai *International Network Of Intercontnected Computer*, artinya jaringan internasional dari komputer-komputer yang saling hubungan (Wahid dan Labib, 2010: 31).

Hukum siber merupakan hukum yang multidisipliner yang berkaitan dengan cabang-cabang ilmu lain, seperti hukum pidana, hukum perdata, perlindungan konsumen, ekonomi, dan administrasi dengan pendekatan teknologi, sosial budaya (etika) dan hukum. Perkembangan teknologi informasi khususnya internet banyak menimbulkan kemanfaatan di dalam kehidupan. Akan tetapi, ibarat dua sisi mata uang, seiring manfaat yang ditimbulkan, internet juga dapat memiliki dampak negatif dan juga menjadi sarana bagi orang-orang tertentu untuk melakukan kejahatan. Namun secara prinsip, teknologi komputer atau teknologi informasi adalah bersifat netral. Artinya di dalam dirinya tidak terkandung hal-hal yang dirancang untuk maksud yang tidak baik bagi umat manusia. Hanya manusia yang dalam memanfaatkannya yang kadang kala ingin mencari kelemahan-kelemahannya untuk maksud yang tidak baik atau melakukan tindakan yang bertentangan dengan hukum. Kejahatan erat kaitannya dan bahkan menjadi sebahagian dari hasil karya manusia itu sendiri. Ini berarti semakin tinggi tingkat

budaya dan semakin modern suatu bangsa, maka semakin modern juga kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya (Wahab, 2002: 26). Menurut Muladi (1987), yang sangat menarik dari *cyber crime* adalah motivasi dilakukannya perbuatan tersebut. Bahwa pelaku tindak pidana komputer melakukan perbuatannya bukan semata-mata karena uang, melainkan adanya suatu tantangan (*challenge*). Yang dipikirkan oleh mereka bukanlah apa yang akan diperoleh dari perbuatan tersebut (materi) melainkan bagaimana mengakali (*outsmart*) suatu sistem komputer dan menikmati hasil perbuatannya.

Dalam konteks negara Indonesia, Pada tahun 2013, berdasarkan laporan *State of The Internet*, Indonesia berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau *cyber crime* dan Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri Kombespol Agung Setya mengatakan, dalam kurun waktu tiga tahun terakhir, tercatat 36,6 juta serangan *cyber crime* terjadi di Indonesia. Hal ini sesuai dengan data Security Threat yang menyebutkan Indonesia adalah negara paling berisiko mengalami serangan *cyber crime*. Sementara itu pada tahun 2016 merujuk pada rilis portal berita online, kasus kejahatan di dunia maya atau *cyber crime* menjadi kasus paling banyak yang ditangani Ditreskrimsus Polda Metro Jaya di sepanjang tahun 2016. Dari 1.627 kasus yang ditangani, 1.207 kasus merupakan kasus *cyber crime* (www.cnnindonesia, 30 Desember 2016).

Di dalam beberapa literatur, *cyber crime* sering diidentikkan dengan *computer crime*, *The U.S Departement of Justice* memberikan pengertian *computer crime* sebagai "*…any illegal act requiring knowledge of computer technology for its perpetration, investigation or presecution*". Pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu "*any illegal, unethical or unauthorized behaviour relating to the automatic processing and/or the transmission of data*" (www.interpol.go.id, 2 Januari 2013). Sementara itu Barda Nawawi Arief (2003: 255) menggunakan istilah tindak pidana mayantara untuk menunjuk jenis kejahatan ini. Andi Hamzah (1989: 26) menggunakan istilah tindak pidana siber dengan kejahatan komputer, yakni kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan secara ilegal.

Dalam *background paper* lokakarya Kongres PBB X pada tahun 2000 membagi definisi *cyber crime*, dalam arti sempit (*narrow sense*) dan dalam arti luas (*broader sense*), dimana:

1. *Cybercrime in narrow sense: any illegal behavior directed by means of elctronic operations that targets the security of computer systems and the data processed by them.*
2. *Cybercrime as a broader sense: any illegal behavior commited by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network.* (Arief, 2006: 8)

Di dalam konstelasi hukum pidana Indonesia, tindak pidana siber termasuk ke dalam kategori tindak pidana khusus meskipun dengan unsur yang utamanya dapat dipadankan dengan beberapa pasal-pasal di dalam KUHP tetapi dilakukan dengan cara-cara (modus) yang baru, sehingga dalam memerangi kejahatan ini dibutuhkan suatu instrumen hukum yang lebih jelimet. Seperti yang diterangkan oleh Soerjono Soekanto (2007: 8), bahwa salah satu faktor-faktor yang mempengaruhi penegakan hukum adalah sarana dan prasarana atau fasilitas yang mendukung

penegakan hukum, karena faktor tersebut juga merupakan tolak ukur daripada efektivitas penegakan hukum. Untuk mengakali perkembangan kejahatan yang terjadi melalui media teknologi informasi (internet), semenjak akhir Maret 2008, DPR RI telah mengesahkan Rancangan Undang-Undang Informasi dan Transaksi Elektronik (ITE) menjadi Undang-undang. Regulasi yang telah dirancang sejak tahun 1999 secara umum dapat menjadi instrumen hukum yang memiliki akselerasi yang baik terhadap perkembangan kejahatan dunia maya. Namun, undang-undang ini juga memiliki permasalahan dalam beberapa hal tertentu, baik dari aspek non-hukum maupun dari aspek hukumnya. Permasalahan hukum yang seringkali dihadapi adalah ketika 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. Sehingga berdasarkan latar belakang di atas, dapat dirumuskan suatu permasalah-an, yakni bagaimanakah permasalahan hukum dalam menanggulangi tindak pidana siber (*cyber crime*) di Indonesia? Metode penelitian yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mendalami aspek peraturan-peraturan hukum yang terkait dengan tindak pidana siber, sehingga hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi pihak-pihak yang ingin mendalami permasalahan hukum siber di Indonesia.

## TINDAK PIDANA SIBER DALAM KONSTELASI HUKUM PIDANA

### Bentuk-Bentuk Tindak Pidana Siber

Tindak pidana siber merupakan tindak pidana yang relatif baru, yang dilakukan oleh orang-orang yang ahli atau yang memiliki keahlian di bidang komputer dan teknologi informasi. Jika dilihat dari segi akibat kejahatan, maka kejahatan melalui dunia maya (internet) dapat berdampak di dalam maupun di luar dunia maya.

Tidak terbatasnya ruang dan waktu dalam melakukan aktivitas dengan menggunakan internet sebagai media, menyebabkan sulitnya suatu aktivitas dalam dunia mayantara dideteksi secara konvensional. Komputer yang dulu sebagai alat pengumpul dan penyimpan data saat ini dapat digunakan untuk melakukan kejahatan lama (*old fashioned*) dalam kemasan baru. Jika mengikuti kasus-kasus kejahatan komputer dan siber yang terjadi dan jika hal tersebut dikaji dengan menggunakan kriteria peraturan hukum pidana konvensional, maka ternyata bahwa dari segi hukum, kejahatan komputer dan siber bukanlah kejahatan yang sederhana (Bainbrige, 1993 : 161). Jika dilihat dari dalam peraturan perundang-undangan konvensional, maka perbuatan pidana yang dapat digunakan di bidang komputer dan siber adalah penipuan, kecurangan, pencurian, dan perusakan, yang pada pokoknya dilakukan secara langsung (dengan menggunakan bagian tubuh secara fisik dan pikiran) oleh si pelaku. Sementara jika hal tersebut dilakukan dengan menggunakan sarana siber, maka kejahatan komputer dan siber dapat berbentuk sebagai berikut (Soepraptomo, 2000):

1. Penipuan komputer (*computer fraud*) yang mencakup:
    a. Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan menggunakan sarana komputer/siber dengan melawan hukum,

yaitu dalam bentuk penipuan data dan penipuan program, yang terinci adalah:

i. Memasukkan instruksi yang tidak sah, ialah dilakukan oleh seseorang yang berwenang atau tidak, yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (misalnya transfer).
ii. Mengubah data input, yang dilakukan seseorang dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum (misalnya memasukkan data gaji pegawai melebihi yang seharusnya).
iii. Merusak data, ialah dilakukan seseorang untuk merusak *print-out* atau *output* dengan maksud untuk mengaburkan, menyembunyikan data atau informasi dengan itikad tidak baik.
iv. Penggunaan komputer untuk sarana melakukan perbuatan pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnyadigunakan untuk melakukan kejahatan atau mengubah program.

b. Perbuatan pidana penipuan, yang sesungguhnya dapat termasuk unsur perbuatan lain, yang pada pokoknya dimaksudkan menghindarkan diri dari kewajiban (misalnya wajib pajak) atau untuk memperoleh sesuatu yang bukan hak/miliknya melalui sarana komputer.
c. Perbuatan curang untuk memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang yang dapat mengakses komputer menstranfer rekening orang ke rekeningnya sendiri, sehingga merugikan orang lain.
d. Konspirasi penipuan, ialah perbuatan pidana yang dilakukan beberapa orang secara bersama-sama untuk melakukan penipuan dengan sarana komputer.
e. Pencurian ialah dengan sengaja mengambil dengan melawan hukum hak atau milik orang lain dengan maksud untuk dimilikinya sendiri.

2. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri.
3. *Hacking*, ialah melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan komputer yang dapat mengancam berbagai kepentingan.
4. Perbuatan pidana komunikasi, ialah hacking yang dapat membobol sistem *on-line* komputer yang menggunakan sistem komunikasi.
5. Perbuatan pidana perusakan sistem komputer, baik merusak data atau menghapus kode-kode yang menimbulkan kerusakan dan kerugian.termasuk dalam perbuatan ini penambahan atau perubahan program, informasi, media, sehingga merusak sistem, demikian pula sengaja menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan menggunakan sarana komputer/telekomunikasi.

6. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta, dan hak paten, ialah berupa pembajakan dengan memproduksi barang-barang tiruan untuk mendapatkan keuntungan melalui perdagangan.

Sementara itu Asril Sitompul (2001: 91-92) lebih memberikan penggolongan dengan bentuk yang lebih sederhana dalam bentuk-bentuk tindak pidana siber ini, menurutnya kejahatan komputer yang dilakukan lewat internet yang dapat diidentifikasi terdiri dari beberapa golongan, diantaranya:

1. Kejahatan yang berkaitan dengan data, seperti pemutusan transfer data.
2. Kejahatan yang berhubungan dengan jaringan (*network*), seperti penyadapan dan sabotase.
3. Kejahatan yang berkaitan dengan akses ke internet seperti hacking dan penyebaran virus.
4. Kejahatan yang berkaitan dengan komputer seperti membantu kejahatan di *cyberspace*, pemalsuan data lewat komputer untuk mencari keuntungan, dan pemalsuan data lewat komputer untuk digunakan sebagai data asli.
5. Kejahatan yang berhubungan dengan pasar modal.
6. Pornografi, penghinaan, pencemaran nama baik dan tindakan melawan hukum lainnya.

**Bentuk-Bentuk Tindak Pidana Siber dalam UU ITE**

Dalam sistem hukum pidana Indonesia, kejahatan siber termasuk ke dalam kategori tindak pidana khusus meskipun dengan unsur yang utamanya dapat dipadankan dengan beberapa pasal-pasal di dalam KUHP tetapi dilakukan dengan cara-cara yang baru (*new design*). Saat ini, Indonesia telah memiliki Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang disahkan pada bulan Maret tahun 2008 dan telah dirubah dengan Undang-Undang No. 19 Tahun 2016 yang disahkan dan diundangkan pada tanggal 25 November 2016, terdapat bentuk-bentuk pengaturan hukum pidana yang baru yang menambah aturan hukum pidana baik secara materiil maupun secara formiil, yang secara asasnya dapat dipakai berdasarkan ketentuan yang terdapat dalam Pasal 103 KUHP dan Pasal 284 ayat (2) KUHAP.

Jika diperhatikan, undang-undang informasi dan transaksi elektronik merupakan aturan hukum yang komplek, yang mengatur aspek hukum perdata, pidana, dan administrasi. Di dalam beberapa bagian pasal (Bab VII, Pasal 27 sampai Pasal 37) yang terdapat di dalam UU ITE ini menyebutkan ada sebelas bentuk perbuatan-perbuatan yang dilarang, yakni:

1. Pasal 27 melarang:
   a. Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.
   b. Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian.

c. Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
d. Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

2. Pasal 28 melarang:
   a. Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
   b. Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antar golongan (sara).
3. Pasal 29 melarang:
   Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
4. Pasal 30 melarang:
   a. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
   b. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
   c. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
5. Pasal 31 melarang:
   a. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
   b. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.
6. Pasal 32 melarang:
   a. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi,

merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik.

b. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.

7. Pasal 33 melarang:
   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.
8. Pasal 34 melarang:
   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
   a. Perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33;
   b. Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33.
9. Pasal 35 melarang:
   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.
10. Pasal 36 melarang:
    Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 yang mengakibatkan kerugian bagi orang lain.
11. Pasal 37 melarang:
    Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 36 di luar wilayah indonesia terhadap sistem elektronik yang berada di wilayah yurisdiksi indonesia.

## PERMASALAHAN HUKUM DALAM MENANGGULANGI TINDAK PIDANA SIBER

### Sistem Pembuktian dalam Hukum Acara Pidana

Untuk dapat terciptanya suatu keputusan hakim, hakim tidak harus menemukan seluruh alat bukti[1] yang telah ditetapkan, akan tetapi berdasarkan Pasal

[1] Dalam Pasal 184 ayat (1) Kitab Undang-Undang Hukum Acara Pidana (KUHAP) menyebutkan alat bukti dalam hukum acara pidana adalah keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Dan berdasarkan Putusan Mahkamah Konstitusi Nomor 65/PUU-VIII/2010 tentang Pengujian Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana dilakukan perluasan definisi saksi yang termasuk ke dalamnya adalah orang-orang melihat, mendengar, mengalami sendiri suatu tindak pidana, tetapi juga setiap orang yang punya pengetahuan yang terkait langsung terjadinya tindak pidana wajib didengar sebagai saksi.

183 KUHAP putusan pidana dapat dijatuhkan hakim dengan sekurang-kurangnya dua alat bukti yang sah dan ia benar-benar memperoleh keyakinan bahwa tindak pidana memang telah terjadi dan terdakwalah yang melakukan tindak pidana tersebut. R. Subekti (1991: 12) menamakannya sistem "negatif menurut undang-undang", sistem negatif menurut undang-undang mempunyai maksud sebagai berikut:

1. Untuk mempersalahkan seorang terdakwa (tertuduh) diperlukan suatu minimum pembuktian, yang ditetapkan dalam undang-undang.
2. Namun demikian, biarpun bukti bertumpuk-tumpuk, melebihi minimum yang ditetapkan dalam undang-undang tadi, jikalau hakim tidak berkeyakinan tentang kesalahan terdakwa ia tidak boleh mempersalahkan dan menghukum terdakwa tersebut.

Mengenai sistem pembuktian negatif (*negatief wettelijk stelsel*) menurut undang-undang ini, Yahya Harahap (2006: 278) juga menyatakan hal yang sama, yakni sistem pembuktian menurut undang-undang secara negatif merupakan teori antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan hakim atau *conviction in time*.

**Alat Bukti Elektronik**

Saat ini selain alat bukti yang talah diatur dalam Pasal 184 ayat (1) KUHAP juga telah ada alat bukti baru yang dikenal dengan alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai bentuk perkembangan dan perluasaan alat bukti yang telah ada. Dalam Pasal 44 UU ITE disebutkan selain yang telah ada di KUHAP juga dikenal dengan alat bukti yang 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) UU ITE.

Berdasarkan Pasal 1 angka (1) UU ITE yang termasuk ke dalam 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.

Sementara itu menurut Pasal 1 angka (4) disebutkan yang dimaksud dengan 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, simbol atau perforasi yang memiliki makan atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Di dalam Pasal 5 juga dikuatkan eksistensi dari alat bukti elektronik ini sebagai alat bukti yang sah, yakni sebagai berikut:

1. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

2. Informasi elektronik dan/atau dokumen 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.
3. Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini.

Pengakuan alat bukti elektronik selain diatur dalam UU ITE juga telah datang sebelumnya melalui UU No. 8 Tahun 1997 tentang Dokumen Perusahaan, di dalam Pasal 15 ayat (1) menyebutkan bahwa dokumen perusahaan yang telah dimuat dalam mikrofilm[2] atau media lainnya[3] sebagaimana dimaksud dalam Pasal 12 ayat (1) dan atau hasil cetaknya merupakan alat bukti yang sah.

**Permasalahan Hukum dalam Menanggulangi Tindak Pidana Siber di Indonesia**

Ekstensifikasi alat bukti konvensional sebagaimana yang terdapat dalam Pasal 184 ayat (1) KUHAP mengintroduksi alat bukti baru yang bersifat progresif dan responsif terhadap perkembangan jaman, akan tetapi di dalam penerapannya sebagai alat bukti, data elektronik atau alat bukti elektronik ini memiliki beberapa permasalahan, yaitu seperti:

1. Permasalahan mengenai *locus delicti* (tempat kejadian tindak pidana), dalam tindak pidana siber penyidik dapat menemukan kesulitan dalam menentukan lokasi atau tempat yang akurat terjadinya tindak pidana. Karena pelaku dapat merubah atau menghapus "jejak digital" perangkat yang dipergunakannya untuk melakukan tidak pidana siber maupun mensetting lokasi yang berbeda dengan lokasi yang sebenarnya.
2. Permasalahan mengenai *tempus delicti* (waktu kejadian tindak pidana), penyidik tidak bisa menentukan kapan terjadinya tindak pidana secara tepat, karena para pelaku tindak pidana siber biasanya juga memiliki kemampuan untuk dapat mengacaukan waktu dan tanggal perbuatannya dilakukan.
3. Permasalahan barang bukti juga menjadi promblematik tersendiri bagi aparat penegak hukum. Barang bukti yang dicari adalah terkait dengan segala sesuatu yang dipergunakan untuk mempersiapkan, melakukan dan hasil tindak pidana siber sangat sulit untuk melacaknya karena karena dibalik kecangihan sistem jaringannya internet juga memiliki celah bagi orang-orang yang memiliki keahlian untuk menghapus atau memalsukan identitasnya di dunia maya. Di sisi lain, teknologi informasi adalah teknologi dengan sistem yang terbuka yang tidak mustahil untuk dapat dibajak atau dikloning secara ilegal, dimana setiap orang yang memiliki keahlian di bidang tersebut dapat memanipulasi data, mengubah data, seperti menjadikan data palsu (*fake data*) menjadi data yang asli. Sementara itu Asril Sitompul menyampaikan siapa dan bagaimana bentuk kesaksian yang dapat diajukan untuk peristiwa hukum yang terjadi di media

[2] Mikrofilm adalah film yang memuat rekaman bahan tertulis, tercetak dan tergambar dalam ukuran yang sangat kecil. (Penjelasan Pasal 12 ayat (1) UU Dokumen Perusahaan)

[3] Media lainnya adalah alat penyimpanan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan, misalnya *Compact Disk-Read Only Memory* (CD-ROM), dan *Write Once Read Many* (WORM). (Penjelasan Pasal 12 ayat (1) UU Dokumen Perusahaan).

internet. Dapatkah pegawai internet atau karyawannya (web-designer, programmer, data entier dan pegawai lainnya) diajukan sebagai saksi bahwa di media yang dikelolanya telah terjadi pelanggaran hukum, misalnya tentang pencemaran nama baik, penghinaan, atau tindak pidana penipuan, pornografi atau yang lainnya.

4. Tindak pidana siber ini memiliki karakteristik dilakukan oleh satu orang dalam ruangan tertutup, sehingga untuk beberapa bentuk tindak pidana siber biasa penyidik sulit untuk mendapatkan saksi yang menyaksikan langsung pelaku saat sedang melakukan tindak pidana siber, sehingga saksi yang dimiliki terbatas pada saksi korban. Dalam hal tindak pidana siber terkait dengan perbankan, bisa saja pihak perbankan cenderung menutupi telah terjadinya serangan tindak pidana siber terhadap mereka, karena hal ini menjadi aib yang dapat menghilangkan kepercayaan masyarakat secara umum dan nasabah penyimpan dana di bank tersebut.
5. Yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara komunikasi multimedia bersifat internasional, multi yurisdiksi, dan tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi (Arief dan Gultom, 2005: 34). Dengan demikian terkait kewenangan hukum (yurisdiksi) dalam penindakannya juga dapat menumbulkan permasalahan yang serius, hal ini disebabkan karena internet tidak mengenal batas wilayah. Sehingga mungkin saja terjadi tarik menarik kewenangan oleh beberapa negara yang merasa dirugikan oleh tindak pidana siber dalam penegakan hukumnya.
6. Terbatasnya kemampuan penegak hukum dalam hal ini penyidik Polri dalam menangani tindak pidana siber ini, keterbatasnya baik dalam hal sumber daya manusianya maupun dalam hal peralatan-peralatannya. Unit kejahatan siber di kepolisian pun baru terbentuk secara khusus di Reskrim Polri di bawah Direktorat Tindak Pidana Siber pada tanggal 3 Februari 2017 (www.kompas.com, 3 Februari 2017). Sebelumnya tindak pidana siber ini penanganan berada di Direktorat Tindak Pidana Ekonomi Khusus (DIT TIPPID EKSUS) di Subdirektorat V yang menangani tindak pidana antara lain tindak pidana yang terkait dengan *cyber crime*, tindak pidana informasi dan transaksi elektronik (www.reskrimsus.metro.polri.go.id, 11 April 2017).

## SIMPULAN

Pembuktian dan alat bukti merupakan hal yang sangat penting dan memegang peranan kunci dalam proses peradilan. Disaat adanya perkembangan tindak pidana baru yang menggunakan media dan cara-cara (modus) yang baru, maka untuk merespon itu dibutuhkan suatu perkembangan aturan yang baru yang dapat mengikuti perkembangan tindak pidana tersebut. Salah satu perkembangan yang dilakukan oleh hukum pidana Indonesia melalui UU Informasi dan Transaksi Elektronik adalah ekstensifikasi alat bukti sebagaimana yang telah diatur sebelumnya dalam Pasal 184 ayat (1) KUHAP dengan memasukan alat bukti

elektronik yang berupa informasi elektronik dan dokumen elektronik (Pasal 44 UU ITE).

Tetapi dalam penerapan alat bukti elektronik sebagai alat bukti yang sah di dalam sistem peradilan pidana Indonesia memiliki beberapa kendala yang cukup rawan, seperti: mengenai permasalahan *locus* dan *tempus delicti*, keotentikan data elektronik tersebut, saksi, yurisdiksi dan kemampuan penegak hukum dalam menindaknya.

**REFERENSI**

Abdul Wahab (2002) *Kriminologi dan Kejahatan Kontemporer*, Malang: Lembaga Penerbitan Fakultas Hukum Unisma.

Abdul Wahid dan Mohammad Labib (2005) *Kejahatan Mayantara* (*Cyber Crime*), Jakarta: Refika Aditama.

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

Andi Hamzah (1989) *Aspek-Aspek Hukum Pidana di Bidang Komputer*, Jakarta: Sinar Grafika.

Asril Sitompul (2001) *Hukum Internet (Pengenalan Mengenai Masalah Hukum Di Cyberspace)*, Bandung: Citra Aditya Bakti.

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

---------- (2006) *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: Rajawali Grafindo Persada

---------- (2007) *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group

Didik M. Arief dan Elisatris Gultom (2005) *Cyber Law (Aspek Hukum Teknologi Informasi)*, Bandung: Refika Aditama.

David I. Bainbrige (1993) *Komputer dan Hukum*, terjemahan dari "*Computer and the Law*", Cetakan I, Jakarta: Sinar Grafika.

Heru Soepraptomo, *Kejahatan Komputer dan Siber Serta Antisipasi Pengaturan Pencegahannya Di Indonesia*, Makalah ini disajikan dalam Seminar Hukum Tentang E-Commerce dan Mekanisme Penyelesaian Masalahnya Melalui Arbitrase/Alternatif Penyelesaian Sengketa. Diselenggarakan oleh Law Offices of Remy &Darus, bekerja sama dengan dengan Partnership for Economic Growth (PEG), USAID dan Bank Ekspor Indonesia (BEI) di Hotel Mulya Senayan Jakarta pada tanggal 3 Oktober 2000.

http://www.cnnindonesia.com/nasional/20161230232449-12-183255/cyber-crime-kasus-kejahatan-terbanyak-di-2016/. Diakses pada tanggal 14 April 2017, pukul 23:14 WIB.

http://www.interpol.go.id/en/transnational-crime/cyber-crime/89-cybercrime-sebuah-fenomena-di-dunia-maya. Diakses pada tanggal 11 April 2017, pukul 10:34 WIB.

http://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal. Cyber.Crime.di.Dunia. Diakses pada tanggal 11 April 2017, pukul 10:40 WIB.

http://nasional.kompas.com/read/2017/02/03/22470631/unit.kejahatan.dunia.maya.di.polri.segera.beroperasi. Diakses pada tanggal 14 April 2017, pukul 23:42 WIB.

http://www.reskrimsus.metro.polri.go.id/StrukturOrganisasi/BaganSO.aspx?Id=1&Menuid=0. Diakses pada tanggal 11 April 2017, pukul 10:22 WIB.

Mariam Darus Badrulzaman, *Seminar tentang Arbitrase dan E-Commerce*, diselenggarakan oleh Law Offices Remy & Darus, Surabaya, 6 September 2000.

Mariam Darus Badrulzaman (2001) *Kompilasi Hukum Perikatan*, Bandung: Citra Aditya Bakti.

Muladi, Penanggulangan Kejahatan Komputer Dengan Menggunakan Hukum Pidana, Makalah disampaikan pada seminar tanggal 17 Desember 1987 di hotel Borobudur Jakarta.

R. Subekti (1991) *Hukum Pembuktian*, Jakarta: Pradnya Paramita.

Soerjono Soekanto (2007) *Faktor-faktor yang Mempengaruhi Penegakkan Hukum*, Jakarta: Raja Grafindo Persada.

Undang-Undang No. 8 Tahun 1981 Tentang Hukum Acara Pidana (LN 1981/76; TLN NO. 3209)

Undang-Undang No. 8 Tahun 1997 Tentang Dokumen Perusahaan (LN 1997/18; TLN NO. 3674)

Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik (LN 2008/58; TLN NO. 4843)

Undang-Undang No. 19 tahun 2016 Tentang Perubahan atas Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik (LN 2016/251; TLN NO. 5952)

Yahya Harahap (2006) *Pembahasan Permasalahan dan Penerapan KUHAP (Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali)*, Edisi Kedua, Jakarta: Sinar Grafika.