PRASADA JURNAL PRASADA

Jurnal Prasada, Vol. 4, No. 1, ,Maret 2017, 1-11
Available Online at https://ejournal.warmadewa.ac.id/index.php/prasada
DOI: 10.22225/jhp.4.1.161.1-11

HUKUM TINDAK PIDANA MAYANTARA (*CYBER CRIME*) DALAM PERSPEKTIF AKADEMIK

Simon Nahak
Universitas Warmadewa
Simonnahak1964@gmail.com

Abstract
Philosophical foundation created law is to protect human dignity, and then fit the philosophical grounding one of the functions of the criminal law is as a means to control and reduce the occurrence of the crime of using criminal sanctions. Of the various types of sanctions it appears that administrative sanctions and civil penalties is less effective to instill a deterrent for the perpetrators. Therefore the use of criminal sanctions is still the best means available to deal with crime, especially for crime prevention Cyber Crime. Cyber Crime crime prevention in criminal theory should pay attention to three (3) concepts namely, act, guilt and punishment, while in practice criminal system through the Criminal Justice System, the author describes 5 (five) concept in the face of the criminal case; actors, documentary evidence / witnesses, penal mediation of peace between the perpetrator to the victim either at the level of police, prosecutors and courts to justify the consideration of the demands of the public prosecutor, Advocate Actors plea and verdict the judges to alleviate even liberate the perpetrators ".

Keywords: *Penal,Cyber Crime, Academic*

Abstrak
Landasan filosofis diciptakannya hukum adalah untuk melindungi harkat manusia, selanjutnya sesuai landasan filosofis tersebut salah satu fungsi dari hukum pidana adalah sebagai sarana untuk mengendalikan dan mengurangi terjadinya tindak pidana dengan menggunakan sanksi pidana. Dari berbagai jenis sanksi itu tampak bahwa sanksi administratif dan sanksi perdata dirasa kurang efektif untuk menimbulkan rasa jera bagi pelakunya. Maka dari itu penggunaan sanksi pidana masih merupakan sarana terbaik yang tersedia untuk menghadapi kejahatan, khususnya untuk penanggulangan kejahatan mayantara. Penanggulangan kejahatan mayantara dalam teori pidana harus memperhatikan 3 (tiga) konsep yakni, perbuatan, kesalahan dan pidana, sedangkan dalam praktek sistem pemidanaan melalui proses Sistem Peradilan Pidana penulis menguraikan 5 (lima) konsep dalam menghadapi perkara pidana yakni; pelaku, bukti surat/saksi, mediasi penal berupa perdamaian antara pelaku dengan korban baik pada tingkat Kepolisian, Kejaksaan maupun Pengadilan untuk dijadikan dasar pertimbangan tuntutan Jaksa Penuntut Umum, pledoi Advokat Pelaku dan Vonis Majelis Hakim untuk meringankan bahkan membebaskan pelaku".

Kata Kuci: Pidana, Kejahatan Mayantara, Akademik

1.PENDAHULUAN

Kecanggihan kejahatan pada dunia maya (DUMA) ini, tidak diantisipasi dalam KUHP yang berlaku di Indonesia. Penegak hukum masih menggunakan hukum positip yang diterapkan tidak dapat menjangkau kejahatan pada dunia maya. Oleh karena itu dalam kasus penanganan kejahatan mayantara (***cyber crime***) yang ditangani oleh kepolisian sering tidak tuntas. Contohnya; dalam dunia pendidikan kita dari sekolah dasar hingga Perguruan Tinggi (Mahasiswa/i) oleh para Guru, Dosen sering menugaskan para siswa dan mahasiswa untuk membuat tugas dengan mencari dan menggunakan internet, namun jarang ada Guru atau Dosen memberikan sanksi kepada siswa atau mahasiswanya ketika siswa atau mahasiswa menyalahgunakan internet bukan untuk membuat tugas tetapi mencari gambar-gambar porno lewat situs porno, atau catting-cattingan, pacaran melalui facebook, whatchap, bahkan lebih dashyat lagi, mencari teman kencan lewat situs porno seperti "situs mencari cinta siswi SMU dalam mobil, dll". Dengan demikian maka terdapat dampak penggunaan teknologi informasi yakni berdampak positif jika digunakan dengan baik untuk dijadikan sarana positif, dan berdampak negative jika disalahgunakan untuk memenuhi keinginan dan kepentingan yang bersifat negative.

Negara Kesatuan RI menjamin kesejahteraan tiap-tiap warga negaranya, termasuk

perlindungan hak setiap orang (anak-anak, muda-tua, kaya miskin, dll) yang merupakan hak asasi manusia, karena setiap hidup dan kehidupan manusia adalah amanah dan karunia Tuhan Yang Maha Esa, yang dalam dirinya melekat harkat dan martabat sebagai manusia seutuhnya.Mahasiswa adalah tunas, potensi, dan generasi muda penerus cita-cita perjuangan bangsa, memiliki peran strategis dan mempunyai ciri dan sifat khusus yang menjamin kelangsungan eksistensi bangsa dan negara masa depan, oleh karenanya dampak negatif penggunaan teknologi informasi terhadap Mahasiswa patut ditanggulangi.

Bahwa landasan filosofis diciptakannya hukum adalah untuk melindungi harkat manusia, selanjutnya sesuai landasan filosofis tersebut salah satu fungsi dari hukum pidana adalah sebagai sarana untuk mengendalikan dan mengurangi terjadinya tindak pidana dengan menggunakan sanksi pidana. Dari berbagai jenis sanksi itu tampak bahwa sanksi administrative dan sanksi perdata dirasa kurang efektif untuk menimbulkan rasa jera bagi pelakunya. Maka dari itu penggunaan sanksi pidana masih merupakan sarana terbaik yang tersedia untuk menghadapi kejahatan, khususnya untuk penanggulangan kejahatan *Cyber Crime*.

Perkembangan Internet dan umumnya dunia *cyber* tidak selamanya menghasilkan hal-hal yang postif. Salah satu hal negatif yang merupakan efek sampingannya antara lain adalah kejahatan di dunia *cyber* atau, *cybercrime*. Hilangnya batas ruang dan waktu di Internet mengubah banyak hal. Seseorang cracker di Rusia dapat masuk ke sebuah server di Pentagon tanpa ijin. Salahkah dia bila sistem di Pentagon terlalu lemah sehingga mudah ditembus? Apakah batasan dari sebuah cybercrime? Seorang yang baru "mengetuk pintu" (*port scanning*) komputer anda, apakah sudah dapat dikategorikan sebagai kejahatan? Apakah ini masih dalam batas ketidaknyamanan (*inconvenience*) saja? Bagaimana pendapat anda tentang penyebar virus dan bahkan pembuat virus? Bagaimana kita menghadapi *cybercrime* ini? Bagaimana aturan / hukum yang cocok untuk mengatasi atau menanggulangi masalah *cybercrime* di Indonesia? Banyak sekali pertanyaan yang harus kita jawab.

Fenomena cybercrime memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya.

Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas perkembangan cybercrime ini. Saat ini regulasi yang dipergunakan sebagai dasar hukum atas kasus-kasus cybercrime adalah Undang-undang Telekomunikasi transaksi elektronika dan Kitab Undang-Undang Hukum Pidana (KUHP). Namun demikian, interpretasi yang dilakukan atas pasal-pasal KUHP dalam kasus cybercrime terkadang kurang tepat untuk diterapkan. Oleh karena itu urgensi pengesahan RUU Cyberlaw perlu diprioritaskan untuk menghadapi era cyberspace dengan segala konsekuensi yang menyertainya termasuk maraknya cybercrime belakangan ini.

2. PEMBAHASAN

Pengertian Cyber Crime

Kejahatan dengan menggunakan teknologi informasi khususnya Komputer dan pendaftaran nama domain melalui internet, kredit card, serta ATM telah sampai pada tahap yang mencemaskan, kemajuan teknologi informasi selain membawa ke dunia bisnis yang revolusioner (***digital revolution area***) yang serba praktis ternyata mempunyai sisi gelap yang mengerikan, seperti pornografi, kejahatan computer (pencurian, penipuan, pemalsuan data, dan atau perbuatan pidana lainnya bahkan terorisme digital, perang informasi, masalah lingkungan, sampah, dan hacker). Karena seringkali sebuah sistem jaringan berbasis internet memiliki kelemahan (lubang keamanan = *hole)*. Ketika terdapat celah/lubang tidak ditutup, pencuri bisa masuk dari celah/lubang itu.

Pemahaman mengenai cybercrime terdapat beragam pandangan. Namun bila dilihat dari asal katanya, cybercrime terdiri dari dua kata, yakni 'cyber' dan 'crime'. Kata 'cyber' merupakan singkatan dari 'cyberspace', yang berasal dari kata 'cybernetics' dan 'space' Istilah cyberspace muncul pertama kali pada tahun 1984 dalam novel William Gibson yang berjudul Neuromancer. Cyberspace oleh Gibson didefenisikan sebagai :

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation ….. A graphic representation of data abstracted from banks of every computer in

the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding

Dari defenisi di atas dapat dilihat bahwa pada mulanya istilah cyberspace tidak ditujukan untuk menggambarkan interaksi yang terjadi melalui jaringan komputer. Pada tahun 1990 oleh John Perry Barlow istilah cyberspace diaplikasikan untuk dunia yang terhubung atau online ke internet.

Bruce Sterling kemudian memperjelas pengertian cyberspace, yakni: *Cyberspace is the 'place' where a telephone conversation appears to occur. Not your desk. Not inside the other person's phone in some other city. The place between the phone. The indefinite place out there, where the two of you, two human beings, actually meet and communication.*

Berdasarkan defenisi yang telah diuraikan sebelumnya, dapat diketahui bahwa cyberspace merupakan sebuah ruang yang tidak dapat terlihat. Ruang ini tercipta ketika terjadi hubungan komunikasi yang dilakukan untuk menyebarkan suatu informasi, dimana jarak secara fisik tidak lagi menjadi halangan.

Crime berarti 'kejahatan'. Seperti halnya internet dan cyberspace, terdapat berbagai pendapat mengenai kejahatan. Menurut B. Simandjuntak kejahatan merupakan "suatu tindakan anti sosial yang merugikan, tidak pantas, tidak dapat dibiarkan, yang dapat menimbulkan kegoncangan dalam masyarakat."

Sedangkan Van Bammelen merumuskan:

Kejahatan adalah tiap kelakuan yang bersifat tidak susila dan merugikan, dan menimbulkan begitu banyak ketidaktenangan dalam suatu masyarakat tertentu, sehingga masyarakat itu berhak untuk mencelanya dan menyatakan penolakannya atas kelakuan itu dalam bentuk nestapa dengan sengaja diberikan karena kelakuan tersebut[1].

Menurut kepolisian Inggris *Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital[2].

Pemakalah memberikan pengertian *Cyber Crime* "kegiatan menggunakan sarana teknologi informasi dengan cara tidak beretika, melanggar moral dan tindakan yang dilakukan oleh pelaku secara illegal, dengan sengaja dan/atau secara melawan hukum"[3].

Kejahatan Siber komunikasi sangat tinggi, bahkan aparat penegak hukum tidak bisa berbuat banyak, karena KUHP peninggalan Belanda yang digunakan Negara kita belum mengatur ***cyber crime*** atau belum ada norma (***vacuum norm/leemten van normen***). oleh karena itu memperhatikan secara bebas gambar Pornografi di Internet sulit dilacak, RUU KUHP (Kitab Undang-Undang Hukum Pidana) Nasional yang saat ini sedang dirancang di DPR-RI, belum menyebutkan sanksi kejahatan cyber, baik dilakukan oleh perorangan maupun korporasi. Misalnya "dalam hukum, aksi-aksi porno yang dipertontonkan melalui dunia virtual/maya ketika ada seseorang (tua, muda maupun anak-anak) yang mengakses internet gambar porno dapat di hukum ?. "sebab situs gambar porno dapat diambil bebas dari internet"[4].

Sejarah Cyber Crime

Aspek sejarah dalam penalaran hukum biasanya diperlukan untuk memberikan konteks kepada suatu rumusan peraturan. Setiap ketentuan hukum apapun bentuknya, adalah karya manusia yang terikat pada ruang dan waktu. Konteks "ruang dan waktu" ini pada model penalaran aliran hukum kodrat ingin diabaikan. Sehingga hukum adalah asas-asas keadilan dan kebenaran yang berlaku universal. Asas-asas itu tidak pernah berubah, menembus sekat-sekat ruang dan waktu. Dalam prakteknya pengabaian konteks ini tidak banyak berhasil. Asas-asas hukum itu terlalu abstrak, sehingga simbol-simbol yang merangkai rumusan-rumusan asas-asas itu kerapkali harus diberikan pemaknaan baru agar mampu menjawab kebutuhan riil masyarakat.

1. http://www.miftakh.com/2010/03/cybercrime-diindonesia.blogspot.com/2012/05/pengertian-dan-sejarah-cyber-crime-thml di-acess pada hari Selasa, 17 Februari 2015
2. ITAC, *IIIC Convention Views Paper On: Cyber Crime,* IIIC 2000, Millenium Congress, Quebec, September 19th, hlm. 2
3. Simon Nahak, *Hukum Tindak Pidana Cyber Crime (Mayantara) Dalam Perspektif Akademik,* Makalah sebagai narasumber Talkshow Penegakan Hukum Cyber Crime, diadakan oleh Perhimpunan Mahasiswa Hukum Indonesia Cabang Bali (DPC. PEMAHI, Bali), Sabtu, 21 Februari 2015, hlm. 6
4. Bugin Burhan, *dalam Harian Bali Post,* 15 -8- 2002, hal. 5 kol. 6.
5. Shidarta, *Hukum Penalaran dan Penalaran Hukum Buku I Akar Filosofis* (Yogyakarta: Genta Publshing, 2013), hlm. 258

Shidarta menulis bahwa " model penalaran mazhab sejarah sebaliknya agar memperhatikan konteks ruang dan waktu dalam pertumbuhan hukum. Bagi penganut model penalaran ini, hukum tidaklah dibuat melainkan tumbuh mengikuti perkembangan masyarakat (*Das Recht wird nicht gemacht, est ist und wrid mit den volke*)"[5].

Berdasarkan uraian tersebut maka dalam aspek sejarah dalam dunia akademik das sain dan dassolen dibutuhkan untuk mengetahui terjadinya suatu fakta hukum (*legal fact*) yang di dalamnya terdapat unsur-unsur untuk menganalisa perbuatan hukum, peristiwa hukum dan keadaan hukum.

Cybercrime terjadi bermula dari kegiatan hacking yang telah ada lebih dari satu abad. Pada tahun 1870-an, beberapa remaja telah merusak sistem telepon baru negara dengan merubah otoritas. Berikut akan ditunjukan seberapa sibuknya para hacker telah ada selama 35 tahun terakhir.

Awal 1960 Fasilitas universitas dengan kerangka utama komputer yang besar, seperti laboratorium kepintaran buatan (*artificial intelligence)* MIT, menjadi tahap percobaan bagi para hacker. Pada awalnya, kata "hacker" berarti positif untuk seorang yang menguasai komputer yang dapat membuat sebuah program melebihi apa yang dirancang untuk melakukan tugasnya.

Awal 1970 John Draper membuat sebuah panggilan telepon jarak jauh secara gratis dengan meniupkan nada yang tepat ke dalam telepon yang memberitahukan kepada sistem telepon agar membuka saluran. Draper menemukan siulan sebagai hadiah gratis dalam sebuah kotak sereal anak-anak. Draper, yang kemudian memperoleh julukan "Captain Crunch" ditangkap berulangkali untuk pengrusakan telepon pada tahun 1970-an. Pergerakan sosial Yippie memulai majalah YIPL/TAP (*Youth International Party Line/Technical Assistance Program*) untuk menolong para hacker telepon (disebut "phreaks") membuat panggilan jarak jauh secara gratis.

Dua anggota dari California's Homebrew Computer Club memulai membuat "blue boxes" alat yang digunakan untuk meng-hack ke dalam sistem telepon. Para anggotanya, yang mengadopsi pegangan "Berkeley Blue" (Steve Jobs) dan "Oak Toebark" (Steve Wozniak), yang selanjutnya mendirikan Apple Computer.

Awal 1980 Pengarang William Gibson memasukkan istilah "cyberspace" dalam sebuah novel fiksi ilmiah yang disebut Neuromancer. Dalam satu penangkapan pertama dari para hacker, FBI menggerebek markas 414 di Milwaukee (dinamakan sesuai kode area lokal) setelah para anggotanya meyebabkan pembobolan 60 komputer berjarak dari Memorial Sloan-Kettering Cancer Center ke Los Alamos National Laboratory. Comprehensive Crime Contmrol Act memberikan yuridiksi Secret Service lewat kartu kredit dan penipuan komputer. Dua bentuk kelompok hacker, the Legion of Doom di Amerika Serikat dan the Chaos Computer Club di Jerman.

Akhir 1980 Penipuan komputer dan tindakan penyalahgunaan memberi kekuatan lebih bagi otoritas federal. Computer Emergency Response Team dibentuk oleh agen pertahanan Amerika Serikat bermarkas pada Carnegie Mellon University di Pittsburgh, misinya untuk menginvestigasi perkembangan volume dari penyerangan pada jaringan komputer.

Pada usianya yang ke-25, seorang hacker veteran bernama Kevin Mitnick secara rahasia memonitor e-mail dari MCI dan pegawai keamanan Digital Equipment. Dia dihukum karena merusak komputer dan mencuri software dan hal itu dinyatakan hukuman selama satu tahun penjara.

Pada Oktober 2008 muncul suatu virus baru yang bernama Conficker (juga disebut Downup, Downandup dan Kido) yang terkategori sebagai virus jenis worm. Conficker menyerang Windows dan paling banyak ditemui dalam Windows XP. Microsoft merilis patch untuk menghentikan worm ini pada tanggal 15 Oktober 2008. Heinz Heise memperkirakan Conficker telah menginfeksi 2.5 juta PC pada 15 Januari 2009, sementara The Guardian memperkirakan 3.5 juta PC terinfeksi. Pada 16 Januari 2009, worm ini telah menginfeksi hampir 9 juta PC, menjadikannya salah satu infeksi yang paling cepat menyebar dalam waktu singkat[6].

Sejarah Cyber Crime juga berawal mula dari penyerangan didunia Cyber pada tahun 1988 yang lebih dikenal dengan istilah *CyberAttack* Pada saat itu ada seorang mahasiswa yang berhasil menciptakan sebuah worm atau virus yang menyerang program computer dan mematikan sekitar 10% dari seluruh jumlah komputer di dunia yang terhubung ke internet Pada tahun 1994

6. https://pritamaardi.wordpress.com/2011/11/21/sejarah-cyber-crime-thml diacess pada hari Selasa, 17 Februari 2015

seorang anak sekolah musik yang berusia 16 tahun yang bernama RichardPryce, atau yang lebih dikenal sebagai “the hacker” alias “Datastream Cowboy”, ditahan lantaran masuk secara ilegal ke dalam ratusan sistem komputer rahasia termasuk pusat data dari Griffits AirForce, NASA dan Korean Atomic Research Institute atau badan penelitian atom Korea Dalam interogasinya dengan FBI, ia mengaku belajar hacking dan cracking dari seseorang yang dikenalnya lewat internet dan menjadikannya seorang mentor, yang memiliki julukan “Kuji”. Hebatnya, hingga saat ini sang mentor pun tidak pernah diketahui keberadaannya.Hingga akhirnya, pada bulan Februari 1995, giliran Kevin Mitnick diganjar hukuman penjara untukyang kedua kalinya. Dia dituntut dengan tuduhan telah mencuri sekitar 20.000 nomor kartu kredit!Bahkan, ketika ia bebas, ia menceritakan kondisinya di penjara yang tidak boleh menyentuh komputer atau telepon[7].

Beberapa waktu lalu di Indonesia dihebohkan dengan kasus pembobolan ATM di dunia perbankan, itu termasuk salah satu perbuatan dari salah satu hacker yang ingin mendapatkan suatu

Bagan 1.1

Masalahnya adalah minimnya upaya pengawasan bank terhadap dua sistem tersebut. Sehingga nasabah dituntut untuk lebih berhati-hati/waspada saat bertransaksi di ATM.

Selain pembobolan bank, bank juga memiliki suatu layanan yaitu layanan internet banking. Internet banking adalah layanan perbankan yang dilakukan dengan menggunakan internet. Transaksi yang dapat dilakukan diantaranya adalah pengecekan saldo, transfer uang, pembayaran tagihan. Penyelenggaraan Internet Banking yang sangat dipengaruhi oleh perkembangan teknologi informasi, dalam kenyataannya pada satu sisi membuat jalannya transaksi perbankan semakin mudah, akan tetapi di sisi yang lain membuatnya juga semakin berisiko. Dengan kenyataan seperti ini, faktor keamanan harus menjadi faktor yang paling perlu diperhatikan.

Seiring dengan meningkatnya pemanfaatan Internet Banking, akan semakin banyak pihak-pihak yang mencari kelemahan sistem Internet Banking yang ada. Serangan-serangan tersebut akan semakin beragam jenisnya dan tingkat kecanggihannya. Bila dahulu serangan tersebut umumnya bersifat pasif, misalnya *Eavesdropping* dan *Offline Password Guessing*, kini serangan tersebut menjadi bersifat aktif, dalam arti penyerang tidak lagi sekedar menunggu hingga user beraksi, akan tetapi mereka beraksi sendiri tanpa perlu menunggu user. Beberapa jenis serangan yang dapat dikategorikan ke dalam serangan aktif adalah *man in the middle attack dan trojan horses*.

Gambaran umum dari aktifitas yang sering disebut *man in the middle attack* adalah sebagai berikut: penyerang membuat sebuah website dan membuat user masuk ke website tersebut. Agar berhasil mengelabui user, website tersebut harus dibuat semirip mungkin dengan website bank yang sebenarnya. Kemudian user memasukkan passwordnya, dan penyerang kemudian menggunakan informasi ini untuk mengakses website bank yang sebenarnya.

Sedangkan, trojan horses adalah program palsu dengan tujuan jahat, yang disusupkan kepada sebuah program yang umum dipakai. Di sini para penyerang meng-install trojan kepada komputer user. Ketika user login ke website banknya, penyerang menumpangi sesi tersebut melalui trojan untuk melakukan transaksi yang diinginkannya.

Dalam rangka melakukan pengawasan terhadap perbankan, Bank Indonesia perlu melakukan audit terhadap Sistem Teknologi Informasi dan Komunikasi yang digunakan oleh perbankan untuk setiap kurun waktu tertentu. Memperketat / mengendalikan dengan cermat akses nasabah maupun pegawai kejaringan sistem ICT perbankan, agar seluruh pegawai perbankan mengetahui bahwa merekapun juga dipantau. Perlu ketentuan (Peraturan atau UU) agar perbankan bertanggung jawab dengan mengganti uang nasabah yang hilang akibat kelemahan sistem pengamanan ICT perbankan, misalnya perbankan lalai meningkatkan sistem pengamanan ICT-nya, seperti halnya Regulation E di Amerika. Perlu digunakan Perangkat Lunak Komputer Deteksi untuk aktifitas rekening nasabah, agar apabila terjadi kejanggalan transaksi, seperti pengambilan uang nasabah yang melampaui jumlah tertentu, dapat ditangani dengan cepat. Perlunya sosialisasi aktif dari perbankan kepada masyarakat/nasabah dan pegawai perbankan mengenai bentuk-bentuk kejahatan yang dapat terjadi dengan produk/layanan yang disediakannya. Menambah per-

7. *Ibid.*,

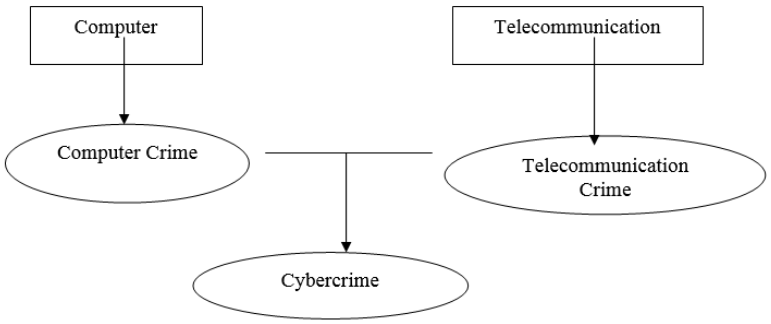
syaratan formulir identitas pada waktu pembukaan rekening baru untuk pemeriksaan pada data base yang menghimpun daftar orang bermasalah dengan institusi keuangan. Meskipun hingga saat ini belum terdapat teknologi yang dapat membuat Internet Banking menjadi aman[8], akan tetapi pihak perbankan dan pemerintah perlu mengupayakan agar penyelenggaraan Internet Banking yang telah ada agar lebih aman. Perkembangan Cyber Crime di Indonesia walau di dunia nyata Indonesia dianggap sebagai salah satu negara terbelakang, namun prestasi yang sangat gemilang telah berhasilditorehkan oleh para hacker, cracker dan carder lokal.Hasil "kerja keras" mereka selama ini telah menempatkan Indonesia sebagainegara No. 2 dalam kasus pencurian kartu kredit terbesar di dunia. Bukan hanya itu, berbagai tindak kejahatan typosite alias pencatutan alamat website suatu perusahaan untuk digunakan demi kepentingan pribadi juga tidak kalah maraknya. Misalnya kasus pencurian domain perusahaan kosmetik Martha Tilaarbeberapa waktu lalu yang disusul dengan perusahaan lain seperti www.RedHat.or.id, Satelindo.co.id, BCA, www.2800.com dan yang terbaru adalah pengrusakan situs KPU.go.id yang dilakukan oleh DenyFirmansyah, mahasiswa Universitas Muhammaddiyah Yogyakarta[9].

Di Indonesia sendiri juga sebenarnya prestasi dalam bidang cyber crime ini patut diacungi dua jempol. Walau di dunia nyata kita dianggap sebagai salah satu negara terbelakang, namun prestasi yang sangat gemilang telah berhasil ditorehkan oleh para hacker, cracker dan carder lokal. Virus komputer yang dulunya banyak diproduksi di US dan Eropa sepertinya juga mengalami “outsourcing” dan globalisasi. Di tahun 1986 – 2003, epicenter virus computer dideteksi kebanyakan berasal dari Eropa dan Amerika dan beberapa negara lainnya seperti Jepang, Australia, dan India. Namun hasil penelitian mengatakan di beberapa tahun mendatang Mexico, India dan Africa yang akan menjadi epicenter virus terbesar di dunia, dan juga bayangkan, Indonesia juga termasuk dalam 10 besar. Seterusnya 5 tahun belakangan ini China , Eropa, dan Brazil yang meneruskan perkembangan virus-virus yang saat ini mengancam komputer kita semua dan gak akan lama lagi Indonesia akan terkenal namun dengan nama yang kurang bagus alasannya, mungkin pemerintah kurang ketat dalam pengontrolan dalam dunia cyber, terus terang para hacker di Amerika gak akan berani untuk bergerak karena pengaturan yang ketat dan system kontrol yang lebih high-tech lagi yang dipunyai pemerintah Amerika Serikat[10].

Widodo menulis bahwa “dalam dimensi internasional satu-satunya instrument internasional yang mengatur tentang *Cyber Crime* adalah *Convention on Cybercrime* yang ditandatangani di Budapest (Hungaria) tahun 2001. Dewan Eropa (*The Council of Europe*) sejak tahun 1997 merancang *Proposal for a Convention on Cyber Crime* naskah konvensi tersebut disetujui dan ditandatangani oleh 38 negara (34 negara anggota Dewan Eropa, dan 4 negara bukan Dewan Eropa). Setelah ditandatangani dan diratifikasi atau diaksesi oleh 8 negara anggota Dewan Eropa, yaitu Albania, Croasia, Estonia, Hungaria, Lithuania, Macedonia, Rumania and Slovenia”[11]. Berdasarkan Konvensi tersebut kemudian masing-maisng negara yang menandatangani dan meratifikasi sepakat untuk mengimplementasikan konvensi tersebut pada hukum pidana di masing-masing negara melalui harmonisasi hukum. Konvensi tersebut juga dijadikan standar minimum (*Standart Minimum Rules*) dalam penyusunan hukum pidana yang mengatur kejahatan yang berhubungan dengan Komputer.

Barda Nawawi Arief menulis bahwa “masalah *Cyber Crime* dalam *International Information Industry Congres* (IIIC) 2000 Millenium Congres diselenggarakan di Quebec pada 19 September 2000, Assosiasi

Bagan 1.2



Sumber: Agus Rahardjo, 2002, hal. 288

8. sejarah cybercrime-Google, kelompok2kleas6f.blogspot.com/2013/03/sejarah-perkembangan-cyber-crime-di-thml diacess pada hari Selasa, 17 Februari 2015
9. artikel cybercrime.blogspot.com/2011/11/sejarah-cyber-crime-thml diacess pada hari Selasa, 17 Februari 2015
10. http://artikelcybercrime.blogspot.com/2011/11/sejarah-cyber-crime-dan-perkembangan.html, diaces pada hari Selasa, 17 Februari 2015
11. http:www/conventions.Coe.Int/commun/chercheSig, dalam Widodo, Sistem Pemidanaan Dalam Cyber Crime, Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime (Yogyakarta : Penerbit Laksbang Mediatama, 2009), hlm. 83
12. Barda Nawawi Arief, Kapita Selekta Hukum Pidana, (Bandung: Penerbit PT. Citra Aditya Bakti, 2010), hlm. 254
13. Data Protection Working Party, dalam Barda Nawawi Arief, Ibid

Sistem Pemidanaan Cyber Crime

NCIS telah mendeteksi bahwa internet telah dijadikan sebagai alat yang handal dan modern untuk melakukan komunikasi antargangster, anggota sindikan obat bius, dan komunikasi antar hooligan di dunia sepak bola. Bahwa dengan mengacu pada *Convention On Cyber Crime* yang diadakan Budapest, 23.XI. 2001 maka bentuk Tindak Pidana mayantara *(Cyber Crime)* antara lain; Pasal 7 tentang Pemalsuan lewat Komputer, Pasal 8 tentang Penipuan lewat Komputer, Pasal 9 tentang Pelanggaran yang berhubungan dengan pornografi anak-anak[14].

Dasar Hukum Cyber Crime

Dasar hukum kejahatan Duma, meskipun secara khusus belum terdapat aturan yang mengatur "khusus tentang Tindak Pidana Mayantara (***Cyber Crime***), namun secara nasional terdapat hukum positif yang dipergunakan sebagai dasar hukum penanggulangan Tindak Pidana Mayantara antara lain : Kitab Undang-Undang Hukum Pidana, Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang RI No. 14 tahun 2008 tentang Keterbukaan Informasi Publik, Undang-Undang RI No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang RI No. 36 tahun 1999 tentang Telekomunikasi, Undang-Undang RI No. 32 tahun 2002 tentang Penyiaran, Undang-Undang RI No. 40 tahun 1999 tentang Pers, Undang-Undang RI No. 23 tahun 2002 tentang Perlindungan anak, Undang-Undang RI No. 44 tahun 2008 tentang Pornografi, Undang-Undang RI No. 31 Tahun 1999 diperbaharui dengan UU RI No. 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi, Konvensi Internasional, Convention On Cyber Crime yang diadakan di Budapest, 23.XI. 2001

Sesungguhnya telah kita ketahui bersama dampak *Cyber Crime* secara tegas berdampak/ berpengaruh negatif. Dikatakan berpengaruh negatif karena akibat penyalahgunaan dunia mayantara tersebut dapat mengakibatkan kerugian baik secara ekonomi, sosial, budaya, mapun mental anak. Sebagai contoh kasus yang sedang menghebohkan dunia informasi kita yakni : kasus Vidio Porno Ariel Peterpen, Luna Maya dan Cut Tari yang diduga melanggar tindakan asusila sehingga dapat dikenakan ketentuan Undang-Undang RI. No. 44 tahun 2008 tentang Pornografi jo UU RI No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Dengan ancaman penjara 12 tahun. Kasus Prita Mulia Sari, dan lain-lain.

Uraian tersebut menegaskan agar setiap anak dan mahasiswa/i kelak mampu memikul tanggungjawab sebagai generasi penerus cita-cita bangsa, maka ia perlu mendapat kesempatan yang seluas-luasnya untuk tumbuh dan berkembang secara optimal, baik fisik, mental maupun sosial, dan berakhlak mulia, perlu dilakukan upaya perlindungan serta untuk mewujudkan kesejahteraan anak dengan memberikan jaminan terhadap pemenuhan hak-haknya serta adanya perlakuan tanpa diskriminasi. Bahwa untuk mewujudkan perlindungan dan kesejahteraan anak diperlukan dukungan kelembagaan dan peraturan perundang-undangan yang dapat menjamin pelaksanaannya. (dasar pertimbangan lahirnya UU RI No. 23 tahun 2002 tentang Perlindungan anak)

Bahwa oleh karena dampak Tindak Pidana *Cyber Crime* terhadap perkembangan anak adalah berdampak negatif, maka hendaknya peranan keluarga dan pendidikan serta pembinaan iman anak selalu ditingkatkan untuk penggunaan informasi teknologi secara postif[15]. dalam bahasa pendidikan/akademis gunakan internet positif.

Pasal 10 KUHP menentukan "macam-macam hukuman ada 2 yaitu, hukuman pokok : Mati, Penjara, kurungan, dan denda

Hukuman tambahan : Pencabutan beberapa hak tertentu, perampasan barang yang tertentu, pengumuman putusan hakim. Ke depan sistem pemidanaan pekerja kerja sosial, pidana pengawasan juga patut diterapkan terhadap pelaku tindak pidana cyber crime.

Sebelum menguraikan sistem pemidanaan yang mengacu pada Pasal 10 KUHP, tersebut

14. NCIS Inggris, *Cyber Crime, Awas Bandit dan Vandalisme Digital*, Republika, 27 Mei 2001, hal. 7
15. Simon Nahak, *Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime) Melalui Kebijakan Hukum Pidana di Indonesia*, Thesis Program Magister (S2) Ilmu Hukum Program Pascasarjana Universitas Udayana Denpasar, 2004, hlm. 1
16. Sauer *menyebutnya sebagai "trias hukum pidana" (berupa "sifat melawan hukum" kesalahan" dan "Pidana")* dan H.L. Packer (1968:17*) menyebutnya sebagai "the tree concept" atau "the tee basic problems" (berupa "offence", "guilt", dan "punishment*"). Dalam Barda Nawawi Arief, *Op. Cit.*, hlm. 328-329

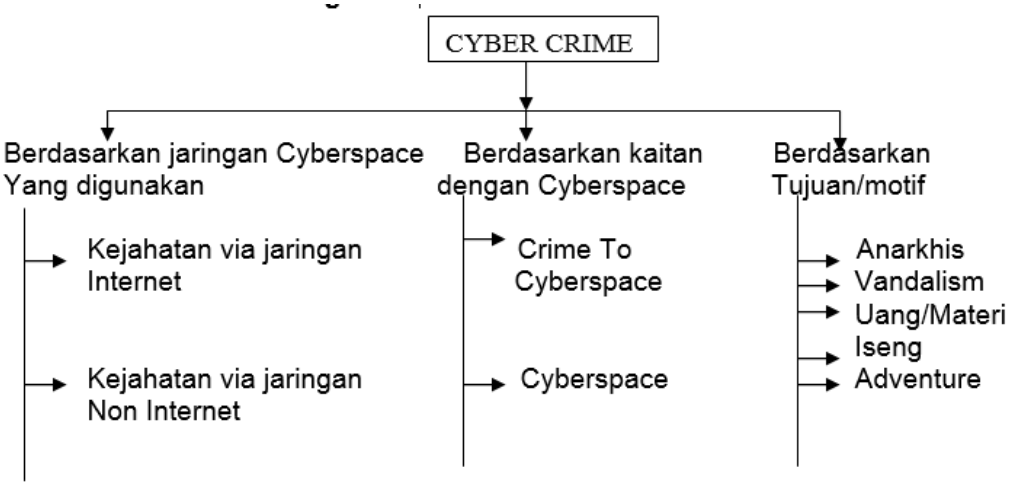
maka sangat penting perlu diperhatikan 3 (tiga) konsep mempelajari hukum Pidana antara lain : **Perbuatan Pidana (*strafbaarfeit/criminal act/actus reus*), Tanggung Jawab Pidana/ Kesalahan (*schuld/guilt/mens rea*) dan Pidana *(straf/punishment/poena*)**[16]. Yang termasuk dalam perbuatan pidana yang dilarang dalam kaitannya dengan adalah perbuatan yang dengan sengaja dan tanpa hak dengan cara melawan hukum sebagai contoh dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, antara lain sebagaimana diatur dalam Pasal 27 – 37. Selanjutnya Tanggung Jawab atas kesalahan dikenakan sanksi Bab XI Ketentuan Pidana Pasal 45 – 52.

Adapun perbuatan yang dilarang menurut ketentuan tersebut antara lain: setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau Dukomen elektronik yang memiliki muatan yang melanggara kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan/pengancaman, (Pasal 27), merugikan konsumen dan transaksi elektronik, kebencian, pemusuhan individu, kelompok dan SARA, (Pasal 28), ancaman kekerasan untuk menakut-nakuti yang ditujukan secara pribadi, (Pasal 29), setiap orang dengan sangaja dan melawan hukum mengakses computer dan/atau sistem elektronik milik orang lain dengan cara apapun, dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, mengakses computer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, (Pasal 30), melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu computer dan/atau sistem elektronik tertentu milik orang lain, dstnya hingga Pasal 31,32,33,34,35,36 dan 37. Kajian aspek perbuatan pidana, tanggung jawab atas kesalahan pelaku tindak pidana Cyber Crime dan sistem pemidanaan terhadap pelaku Tindak Pidana Cyber Crime. Maka berikut ini dipresentasikan bagan tentang jaringan cyberspace, kaitan dengan cyberspace serta tujuan dan motif.

Manifestasi dari tindak kejahatan Cyber Crime muncul dalam berbagai bentuk atau variasi seperti berikut ini: **Recreational Hackers, Crakers atau Criminal Minded Hackers, Political Hackers, Denial of Service attack, Insiders atau Internal Hackers, Viruces, Piracy, Fraud, Gambling, Pornography and Paeddophilia.** Dunia Siber selain mendatangkan kemudahan dengan mengatasi kendala ruang dan waktu, juga telah melahirkan dunia pornografi yang mengkahwatirkan berbagai kalangan. Melalui *news group*, *chat rooms* mengeksploitasi pornografi anak-anak di bawah umur **Cyber-Stalking, Hate Situs, .Criminal Communication.**

Penulis mengkaji dalam sistem pemidanaan melalui mekasnisme praktik sistem peradilan pi-

Bagan 1.3



Sumber: Widyopramono; 1994, Kejahatan Bidang Komputer

dana ada 5 (lima) konsep dalam menghadapi perkara pidana yakni; pelaku, bukti surat/saksi, mediasi penal berupa perdamaian antara pelaku dengan korban baik pada tingkat Kepolisian, Kejaksaan maupun Pengadilan untuk dijadikan dasar pertimbangan tuntutan Jaksa Penuntut Umum, pledoi Advokat Pelaku dan Vonis Majelis Hakim untuk meringankan bahkan membebas-

17.Simon Nahak, Hukum Tindak Pidana Mayantara (*Cyber Crime*) Dalam Perspektif Akademik,

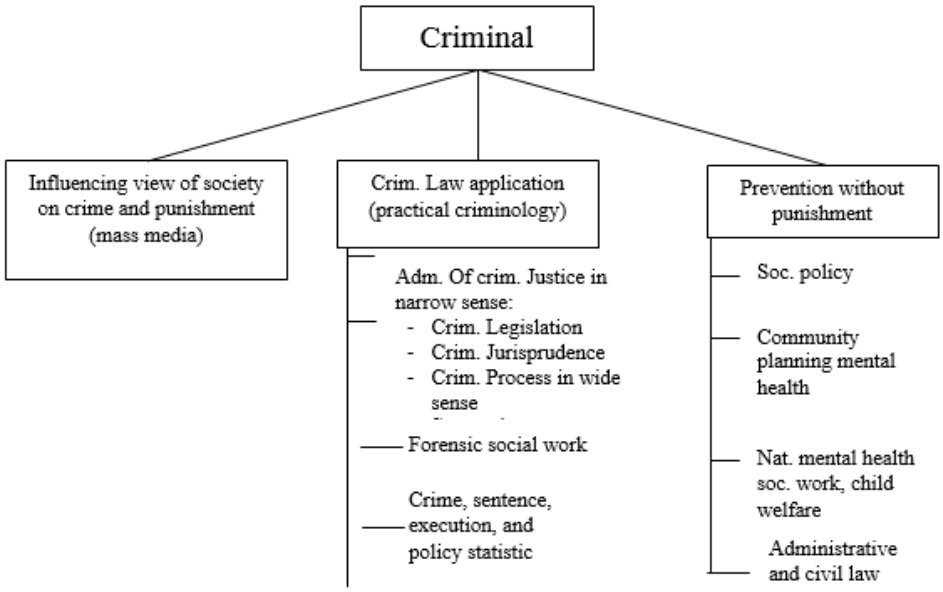
kan pelaku"[17].

Kajian Terhadap Kebijakan Penanggulangan Tindak Pidana Cyber Crime

Kajian Kebijakan Penanggulangan Tindak Pidana Mayantara mengacu pada teori Kebijakan

Ragaan: 1.4

G. Peter Hoefnagels menggambarkan ruang lingkup "*criminal policy*" sebagai berikut:[18]



Berdasarkan ragaan tersebut, maka menurut G.P. Hoefnagels upaya penanggulangan kejahatan dapat ditempuh dengan:

a) Penerapan hukum pidana (criminal law application)
b) Pencegahan tanpa pidana (prevention without punishment)
c) Memengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat mas media (influencing views of society on crime and punishment/mass media).

Pendapat G. Peter Hoefnagels tersebut menggambarkan bahwa, upaya penanggulangan kejahatan secara garis besar dapat dibagi 2 (dua) yaitu lewat jalur "*penal*" (hukum pidana) dan lewat jalur "*non penal*" (bukan/di luar hukum pidana). Dalam pembagian G.P. Hoefnagels di atas, upaya-upaya yang disebut dalam butir (b) dan (c) dapat dimasukan kedalam kelompok upaya "non penal".

Pendapat G.P.Hoefnagels tersebut, menunjukkan bahwa upaya penanggulangan kejahatan pelaku tindak pidana perpajakan secara non penal yakni, Pencegahan tanpa pidana (*prevention without punishment*) dan mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat mass media (*influencing views of society on crime and punishment/mass media*)

Penanggulangan kejahatan terhadap pelaku tindak pidana perpajakan tanpa pidana adalah melalui jalur kebijakan sosial (*social policy*) pada dasarnya adalah kebijakan atau upaya-upaya rasional untuk mencapai kesejahteraan masyarakat. Jadi identik dengan kebijakan atau perencanaan pembangunan nasional yang meliputi berbagai aspek yang cukup luas dari pembangunan. Penanganan atau kebijakan berbagai aspek pembangunan ini sangat penting karena disinyalir dalam berbagai kongres Perserikatan Bangsa Bangsa (PBB) (mengenai *The Prevention of Crime and The Treatment of Offenders*), bahwa pembangunan itu sendiri dapat bersifat "kriminogen" apabila pembangunan itu:

a) Tidak direncanakan secara rasional (it was not rationally planned); atau direncanakan secara timpang, tidak memadai/tidak seimbang (unbalanced/inadequately planned);
b) Mengabaikan nilai-nilai kultur dan moral (disregarded cultural and moral values); dan
c) Tidak mencakup strategi perlindungan masyarakat yang menyeluruh/integral (did not include integrated social defence strategies)[19].

Berdasarkan kebijakan kriminal yang diuraikan oleh G.Peter Hoefnagels tersebut, maka upaya penanggulangan terhadap pelaku tindak pidana Cyber Crime yakni melalui cara Non Penal/

18.G.P. Hoefnagels, *The Other Side Of Criminology*, 1973, Page 99
19.*Ibid.*

SIMPULAN

Berdasarkan pendahuluan dan pembahasan dalam uraian makalah ini, maka dapat disimpulkan sebagai berikut:

1) *Cyber Crime* adalah kegiatan menggunakan sarana teknologi informasi dengan cara tidak beretika, melanggar moral dan tindakan yang dilakukan oleh pelaku secara illegal dengan sengaja dan/atau secara melawan hukum. Sejarah Cyber Crime diawali dengan kejahatan teknologi informasi sejak tahun 1870-an, hingga sekarang sampai dengan penandatanganan *Convention On Cyber Crime* yang diadakan Budapest, 23.XI. 2001;
2) Sistem pemidanaan dengan mengacu pada perbuatan yang dilarang, tanggung jawab atas kesalahan dan pidana berdasarkan ketentuan Pasal 10 Kitab Undang-Undang Hukum Pidana serta ketentuan peraturan yang terkait dengan Cyber Crime, khususnya Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, secara teori memperhatikan 3 (tiga) konsep yakni, perbuatan, kesalahan dan pidana. Kajian kebijakan penanggulangannya adalah secara Penal dan Non Penal.

Kajian Upaya penanggulangan tindak pidana mayantara (Cyber Crime) selain penanggulangan melalui cara Penal dengan memperhatikan 3 (tiga) konsep hukum pidana yakni Perbuatan, Kesalahan dan Pidana, dalam perspketif teori/akademik, namun hendaknya dalam perspektif empiric juga perlu memperhatikan 5 (lima) konsep penyelesaian perkara pidana dalam Sistem Pemindanaan melalui proses Sistem Peradilan Pidana yakni; pelaku, bukti surat/saksi, mediasi penal berupa perdamaian antara pelaku dengan korban baik pada tingkat Kepolisian, Kejaksaan maupun Pengadilan untuk dijadikan dasar pertimbangan tuntutan Jaksa Penuntut Umum, pledoi Advokat Pelaku dan Vonis Majelis Hakim untuk meringankan bahkan membebaskan pelaku".

UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih kepadan Mitra Bestari atas masukan-masukan yang diberikan untuk perbaikan substansi artikel saya ini.

DAFTAR PUSTAKA

Agus Rahardjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Penerbit PT. CitraAdity Bakti, 2002

Artikel *cybercrime.blogspot.com/2011/11/sejarah-cyber-crime-thml* diacess pada hari Selasa, 17 Februari 2015

Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, (Bandung: Penerbit PT. Citra Aditya Bakti, 2010

Bugin Burhan, dalam Harian Bali Post, 15 -8- 2002,

Hoefnagels, G.P., *The Oder Side Of Criminology*, 1973

http://artikelcybercrime.blogspot.com/2011/11/sejarah-cyber-crime-dan-perkembangan.html, diaces pada hari Selasa, 17 Februari 2015

https://pritamaardi.wordpress.com/2011/11/21/sejarah-cyber-crime-thml diacess pada hari Selasa, 17 Februari 2015

http://www.miftakh.com/2010/03/cybercrime-diindonesia.blogspot.com/2012/05/pengertian-dan-sejarah-cyber-crime-thml diacess pada hari Selasa, 17 Februari 2015

ITAC, *IIIC Convention Views Paper On: Cyber Crime,* IIIC 2000, Millenium Congress, Quebec, September 19th,

NCIS Inggris, *Cyber Crime, Awas Bandit dan Vandalisme Digital*, Republika, 27 Mei 2001

Sejarah cybercrime-Google, kelompok2kleas6f.blogspot.com/2013/03/sejarah-perkembangan-cyber-crime-di-thml diacess pada hari Selasa, 17 Februari 2011

Shidarta, *Hukum Penalaran dan Penalaran Hukum Buku I Akar Filosofis* (Yogyakarta: Genta Publshing, 2013

Simon Nahak, *Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime) Melalui Kebijakan Hukum Pidana di Indonesia*, Thesis Program Magister (S2) Ilmu Hukum Program Pascasarjana Universitas Udayana Denpasar, 2004

_____, *Hukum Tindak Pidana Cyber Crime (Mayantara) Dalam Perspektif Akademik,* Makalah sebagai narasumber Talkshow Penegakan Hukum Cyber Crime, diadakan oleh Perhimpunan Mahasiswa Hukum Indonesia Cabang Bali (DPC. PEMAHI, Bali), Sabtu, 21 Februari 2015

Widyopramono; Kejahatan Bidang Komputer, Jakarta, 1994

Widodo, *Sistem Pemidanaan Dalam Cyber Crime, Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime* Yogyakarta : Penerbit Laksbang Mediatama, 2009

Undang-Undang Dasar Republik Indonesia Tahun 1945
Kitab Undang-Undang Hukum Pidana
Kitab Undang-Undang Hukum Acara Pidana
Undang-Undang RI No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik
Undang-Undang RI No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Undang-Undang RI No. 36 Tahun 1999 tentang Telekomunikasi
Undang-Undang RI No. 32 Tahun 2002 tentang Penyiaran
Undang-Undang RI No. 40 Tahun 1999 tentang Pers
Undang-Undang RI No. 23 Tahun 2002 tentang Perlindungan anak
Undang-Undang RI No. 11 Tahun 2012 tentang Sistem Peradilan anak
Undang-Undang RI No. 44 Tahun 2008 tentang Pornografi
Undang-Undang RI No. 31 Tahun 1999 diperbaharui dengan UU RI No. 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi
Konvensi Internasional*, Convention On Cyber Crime yang diadakan di Budapest*, 23.XI. 2001