Projustisia
Prosiding Penelitian dan Pengabdian Masyarakat
Fakultas Hukum Universitas Pamulang
Vol x, No. x Bulan| Tahun
P-ISSN x – x, E-ISSN x – x

PROBLEMATIKA NORMATIF YURISDIKSI TERHADAP TINDAK PIDANA SIBER DALAM PERUNDANG- UNDANGAN INDONESIA DENGAN KONVENSI DEWAN EROPA 2001

Yusri Safira Permata, Yuliana Sari, Aulia Elmira Zayani
Fakultas Hukum, Universitas Pamulang
Shafiraprmt12@gmail.com

ABSTRACT : This research reveals in more detail about state jurisdiction in dealing with cybercrime. The development of crimes or mayantara crimes without being followed by legal developments will make law enforcement unbalanced. Therefore, in addition to examining the criminal jurisdiction contained in Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions, also discusses the 2001 European Council Convention which provides an explanation of major crimes and jurisdiction in accordance with International Law. The basis for regulation of criminal jurisdiction is contained in the Criminal Code (KUHP) Book I Article 2 to Article 9 and Article 2 of Law Number 11 of 2008 concerning Information and Electronic Transactions which adhere to the territorial principle, the principle of the state flag of the ship and the principle of the state aircraft. registered, national principles, protection principles, universal principles, and dual criminality principles. Meanwhile, the regulation of criminal jurisdiction over cyber crimes in South Africa is contained in Act no. 25 of 2002 concerning the Electronic Communication and Transaction Act, 2002 which adheres to the principles of the 2001 European Council Convention, namely subjective territorial principles, objective territorial principles, extra territorial principles, and national principles. the principle of the state flag of the ship, and the principle of the registered state aircraft. The regulation of criminal jurisdiction in Article 2 of Law Number 11 of 2008 concerning Information and Electronic Transactions is relatively short and concise so that in its implementation it requires interpretations and deviations from the principles of jurisdiction in public international law and the theory of locus delicti in criminal law. Law enforcement on cyber criminal act is not apart from jurisdiction, particularly space of validity of criminal law in a place (territorial jurisdiction). Widespread locus delicti potential in cyber criminal act will be give rising to problems in relation to principles of jurisdiction or the incidence of jurisdictional conflicts. The validity of universal jurisdiction requires states cooperation starting by any ratification of cyber criminal act. Given similarity of law enforcement, then minimize the use of legal loopholes due the state jurisdiction. This research was conducted in several places, such as the Pamulang University library and the city library. These places can provide primary data for writing this research. In this study also traced secondary data obtained from the library. Interviews were conducted with various informants to fill the lack of author data, especially international legal experts, police investigators, and other legal practitioners who control this cybercrime case. This study uses a qualitative normative juridical method. This normative juridical research refers to existing legal norms. Qualitative research was used to analyze the data obtained, both from the results of literature reviews and the results of interviews. The results of the study concluded that: (1) cybercrime regulation in the Budapest Convention consists of 9 (nine) categories of crimes committed intentionally and without rights); (2) according to the ITE Law, Indonesian jurisdiction has territorial principles and principles of protection: (3) both the ITE Law and the Budapest Convention use territorial principles in their jurisdiction, and the Budapest Convention has national principles, ship flag principles, registered aircraft principles, which are not owned by the ITE Law. ITE, apart from that the ITE Law has a principle of protection, which the Budapest Convention does not have.[1]
Keywords : UU ITE, Cybercrime, European Council Convention

[1] Kegiatan Penelitian Mahasiswa Fakultas Hukum Universitas Pamulang Tahun Akademik 2022 / 2023 berdasarkan No Kontrak : 2828-343/C.11/LL.SKP/UNPAM/XI/2022

PENDAHULUAN

Era globalisasi terbentuk karena adanya pengglobalan negara-negara dunia. Arus informasi menyebabkan tidak adanya batas ruang dan waktu untuk mengetahui segala sesuatu yang berada di luar negaranya. Batasan negara sudah tidak ada lagi karena adanya teknologi informasi yang semakin canggih. Perlu diketahui dengan adanya era globalisasi ini menyebabkan perlu adanya pengaturan yang sifatnya universal terhadap tindak pidana yang ada di bidang siber.

Dunia yang sedang berada dalam abad informasi, keberadaan informasi mempunyai peranan penting di dalam kehidupan manusia. Melalui kemajuan informasi, komunikasi, dan teknologi (Information Communication Technology/ICT) dapat mendorong perkembangan dan pertumbuhan ekonomi dunia. Teknologi informasi dan komunikasi (TIK) telah mengubah prilaku masyarakat dan peradaban manusia secara global. Perkembangan teknologi informasi telah meyebabkan perubahan sosial yang secara signifikan berlangsung dengan cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Ketidakmampuan suatu negara untuk melacak dan mengungkap cybercrime pada akhirnya akan mempengaruhi penegakan hukum di negara lain, termasuk negara-negara maju yang memiliki kemampuan relatif tinggi baik sumber daya manusia maupun sarana prasarananya. Hal ini berkaitan dengan adanya prinsip double criminality untuk penegakan hukum terhadap tindak pidana transnasional.

Dalam penegakan hukum tindak pidana siber tidak akan terlepas dengan yurisdiksi, terutama mengenai ruang berlakunya hukum pidana menurut tempat (yurisdiksi teritorial).

Luas dan tersebarnya potensi locus delicti dalam tindak pidana siber akan menimbulkan masalah berkaitan dengan prinsip yurisdiksi atau terjadi konflik yurisdiksi.

Menurut Debra L. Shinder; kasus kejahatan dunia maya, lebih dari kebanyakan kasus lainnya, seringkali melibatkan masalah yurisdiksi kompleks yang dapat menghadirkan hambatan hukum dan praktis untuk penuntutan.

Oleh karena itu upaya penegakan hukum terhadap pelaku cybercrime tidak hanya menjadi perhatian nasional saja tetapi juga regional dan internasional. Lahirnya pemikiran untuk membentuk suatu aturan hukum yang dapat merespon persoalan-persoalan hukum yang muncul akibat dari pemanfaatan TIK terutama disebabkan oleh sistem hukum konvensional yang tidak dapat merespon persoalan-persoalan tersebut dengan memuaskan. Hal ini pada gilirannya akan melemahkan atau bahkan mengusangkan konsep-konsep hukum yang sudah mapan seperti konsep-konsep kedaulatan dan yurisdiksi.

Kedua konsep ini berada pada posisi yang dilematis ketika harus berhadapan dengan kenyataan bahwa dalam pemanfaatan internet tidak lagi menghiraukan batas-batas yurisdiksi negara. Dilema yang dihadapi oleh konsep- konsep hukum konvensional dalam menghadapi fenomena di cyberspace merupakan alasan utama perlunya membentuk regulasi yang akomodatif terhadap fenomena-fenomena yang muncul akibat pemanfaatan TIK, khususnya menyangkut yurisdiksi.

Prinsip-prinsip yurisdiksi dalam hukum internasional memiliki dasar yang sama, yaitu adanya penentuan wilayah yang jelas, apakah suatu peristiwa terjadi di wilayah suatu negara, ataukah di wilayah negara asing yang berdampak pada wilayahnya sendiri. Namun demikian yang menjadi kendala dalam penerapan yurisdiksi dalam hukum internasional adalah adanya suatu kondisi dalam teknologi informasi dan komunikasi yang tanpa batas.

Internet telah membentuk masyarakat dengan kebudayaan baru, dimana saat ini hubungan antara masyarakat dalam dimensi global tidak lagi dibatasi oleh batas- batas teritorial negara (borderless).

Hadirnya internet dengan segala fasilitas dan program yang menyertainya, telah memungkinkan dilakukannya komunikasi global tanpa mengenal batas negara. Fenomena ini merupakan salah satu bagian dari globalisasi yang melanda dunia saat ini. Derasnya penggunaan teknologi informasi dalam kegiatan yang berbasis transaksi elektronik, seperti layanan anjungan tunai mandiri (ATM), transaksi internet banking, mobile banking, transaksi perdagangan dunia maya (e- commerce), dan lain-lain; sayangnya belum diikuti dengan perkembangan perangkat hukum.

Oleh karena itu, diperlukan kehadiran perangkat hukum yang dapat menyelesaikan permasalahan/sengketa yang terjadi di dunia maya, karena hukum positif yang ada belum cukup dapat menjangkaunya (Efa Laela Fakhriah, 2017: 4). Dalam perkembangan dunia digital internet selanjutnya, muncullah e- commerce. Secara umum e-commerce itu merupakan mekanisme transaksi dalam berbisnis yang tidak menggunakan kertas sebagai sarana mekanismenya, tapi menggunakan teknologi dalam pengertian luas dalam proses dan praktik transaksinya, seperti penggunaan e-mail atau bisa melalui worldwibeweb (www) (Onno W Purbo dan Aang Arief Wahyudi, 2001: 1-2).

Secara singkat dapat diartikan bahwa e-commerce merupakan suatu transaksi komersial yang dilakukan antar penjual dan pembeli atau dengan pihak lain dalam hubungan perjanjian yang sama untuk mengirimkan sejumlah barang, pelayanan atau peralihan hak.transaksi komersial ini terdapat di dalam media elektronik (media digital) yang secara fisik tidak memerlukan pertemuan para pihak yang bertransaksi dan keberadaan media ini di dalam jaringan umum (public network) atau sistem yang berlawanan dengan jaringan pribadi (private network).Pemanfaatan internet yang begitu luas jangkauannya, sehingga membuat perkembangan bisnis di dunia maya (electronic commerce atau e-commerce) meningkat secara signifikan. Perkembangan e-commerce yang begitu pesat membuat tawaran barang dan jasa jadi berkembang lintas benua. Alhasil, perdagangan di dunia maya (e-commerce) ini jauh melebihi perkembangan perdagangan di dunia nyata. Pergeseran penjualan barang dan jasa ke dunia maya (e-commerce) didukung dengan berbagai kemudahan, antara lain: hampir semua jenis barang yang dibutuhkan ada di dunia maya, hampir segala jenis jasa tersedia, tidak perlu mengeluarkan uang tunai – cukup hanya menggunakan kartu debit atau kredit – dengan berbagai cara pembayaran.

Secara umum, dampak positif dari penggunaan internet adalah kemudahan komunikasi dengan siapapun di seluruh dunia, sebagai media pertukaran data dengan menggunakan fasilitas mesin pencarian (search engine), yang memudahkan pengguna di seluruh dunia dapat bertukar informasi dengan cepat, mudah, penting dan akurat sehingga manusia dapat mengetahui apa saja yang terjadi di belahan bumi lain; digunakan sebagai lahan informasi untuk bidang pendidikan, kebudayaan dan lain- lain; dan kemudahan bertransaksi dan berbisnis di tempat dalam bidang perdagangan. Sungguhpun demikian, di setiap peluang kemajuan terdapat potensi kecurangan atau tindakan kejahatan. Kejahatan sangat erat kaitannya dengan perkembangan masyarakat. Semakin maju kehidupan masyarakat, maka kejahatan juga mengiringi kemajuan tersebut. Peluang besar dapat terjadi di dunia internet yang tanpa batas-batas negara (borderless) ini sering disebut sebagai kejahatan dunia maya (cybercrime).

Dan dalam perkembangannya, cybercrime ini juga telah melampaui batas- batas negara. Pelaku kejahatan atau tindak pidana dunia maya ini, bisa dilakukan di mana saja dan menimbulkan korban di mana saja, tanpa mengenal batas negara. Teknologi internet yang berkembang ini kemudian dijadikan sarana untuk melakukan tindak pidana (cybercrime). Tindak pidana yang berbasiskan internet, baik berupa tindak pidana berupa membocorkan kerahasiaan (confidentiality), tentang integritas (integrity), dan keberadaan data (avaiability); atau penyerangan terhadap sistem komputer seperti hacking, cracking, phreaking, virusses dan lain- lain, maupun tindak pidana yang

digunakan melalui media teknologi informasi dan komunikasi sebagai alat, seperti cyberfraud, credit card fraud, cyberpornography, cyberterrorism dan lain-lain.

Berdasarkan latar belakang tersebut, maka penulis telah melakukan penelitian dengan judul **"Problematika Normatif Yurisdiksi Terhadap Tindak Pidana Siber Dalam Perundang- Undangan Indonesia Dengan Konvensi Dewan Eropa 2001"**

PERMASALAHAN

Penelitian ini mengkaji tentang peraturan dan pengaturan perundang-undangan yang memuat cybercrime belum menjamin perlindungan hukum bagi masyarakat dalam hukum di indonesia, supaya penelitian ini tidak melebar terlalu jauh dari substansi, maka penelitian ini penulis batasi hanya yang berkaitan dengan masalah-masalah sebagai yaitu, **Pertama** Bagaimana penerapan ketentuan UU ITE yang berkaitan dengan KUHP atau Perundang – undangan lainnya? **Kedua** Bagaimana tindak pidana siber dalam Konvensi Dewan Eropa 2001 dalam UU ITE? serta **Ketiga** Bagaimana penegakan hukum terhadap tindak pidana siber sebelum Berlakunya Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

METODELOGI PENELITIAN

Penelitian hukum merupakan suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum atau doktrin-doktrin hukum untuk menjawab isu-isu hukum yang dihadapi. Jenis penelitian yang digunakan di dalam melakukan penelitian adalah tipe penelitian normatif yakni tipe penelitian yang mengkaji tentang asas-asas, norma, kaidah dari peraturan perundang - undangan dan putusan pengadilan. sehingga penelitian ini sangat erat hubungannya dengan perpustakaan dikarenakan akan membutuhkan data yang bersifat sekunder pada perpustakaan. Di dalam penelitian hukum normatif hukum yang tertulis dikaji dari berbagai macam aspek seperti aspek teoritis, filosofi, perbandingan, struktur/komposisi, konsistensi, penjelasan umum dan penjelasan pada tiap pasal, formalitas dan kekuatan mengikat suatu undang-undang seta bahasa yang digunakan adalah bahasa hukum. Sehingga dapat disimpulkan, bahwa penelitian hukum normatif itu mempunyai cakupan yang luas. Penelitian hukum normatif dapat juga mengumpulkan data primer, tetapi peruntukan data primer tersebut hanyalah untuk memperkuat data sekunder. Metode penelitian hukum normatif biasanya dikenal dengan metode yang preskriptif, oleh karenanya dalam metode ini harus selalu disertai dengan rekomendasi dan saran mencari norma baru atau melengkapi norma yang diteliti agar lebih baik. Selain itu, metode normatif juga merupakan metode yang murni karena menguji obyek yang diteliti, yaitu norma. Adapun di dalam penelitian penulis yaitu tentang *"Problematika Normatif Yurisdiksi Terhadap Tindak Pidana Siber Dalam Perundang- Undangan Indonesia Dengan Konvensi Dewan Eropa 2001"* ini adalah merupakan suatu penelitian hukum yuridis normatif yaitu penelitian terhadap bahan hukum berupa perundang-undangan atau hukum tertulis yang dalam hal ini adalah Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik *"Dalam* penelitian hukum diperlukan metode pendekatan yang dimaksudkan untuk mendapatkan informasi dari berbagai aspek mengenai isu-*isu hukum yang sedang dicoba untuk dicari jawabannya". Maka di dalam kaitannya dengan penelitian hukum* normatif ini, penulis menggunakan pendekatan perundang-undangan atau Statute Approach, yang

dilakukan dengan menelaah segala peraturan undang-undang yang berhubungan dengan masalah hukum yang sedang dibahas, yaitu peraturan hukum yang berkaitan dengan Dunia Siber.

PEMBAHASAN

Penerapan Ketentuan UU ITE yang Berkaitan dengan KUHP atau Perundang – undangan lainnya

Hasil penelitian dari penerapan kententuan UU ITE yang berkaitan KUHP atau Perundang – undangan, bersumber dari 2 (dua) sumber primer, yaitu Buku Andi Hamzah di terbitkan oleh Sinar Grafika pada tahun 2002 dengan judul " Hukum Acara Pidana dan buku Orin S. Kerr, di terbitkan New York University Press pada tahun 2006 dengan judul "Digital Evidence and the New Criminal Procedure" dalam Jack M.Balkim, et.al. (ed.), Cybercrime Digital Caps in Networked Environment.

Pengaturan tindak pidana pengaturan tindak pidana siber dalam hukum nasional tersebut merupakan implementasi dari yurisdiksi megara dalam rangka memberikan perlindungan kepada masyarakat. Pemgaturan suata perbuatan menjadi tindak pidana tersebut didasarkan pada asas dalam hukum pidana yang menjadi "tiang" (cornerstone) tegaknya hukum pidana yang berlaku universal yaitu asas lepalitas. Keberadaan hukum (Undang-Undang pidana) yang mengatur suatu tindak pidana merupakan syarat dan dasar agar suatu perbuatan yang merupikan/membahayakan masyarakat dapat dituntut, diadili, dan dipidana. Ketiadaan hukum yang secara tegas dan jelas mengatur suatu perbuatan sebagai tindak pidana sesuai dengan prinsip-prinsip lex certa, lex scripta, dan lex stricta sebagai implementasi dari asas legalitas maka upaya pemberantasan terhadap perbuatan yang merugikan/membahayakan masyarakat tersebut tidak mungkin dilakukan.

Berdasarkan karakteristik dan kategorisasi tindak pidana siber serta sistem hukum pidana substantif Indonesia kebijakan pengaturan tindak pidana siber yang dapat ditempuh saat ini adalah dengan membentuk UU Khusus. Dalam UU Khusus tersebut diatur aturan umum yang akan berlaku terhadap tindak pidana siber, perbuatan-perbuatan yang dikriminalisasi sebagai tindak pidana siber, pedoman pemidanaan khusus dan hukum acara pidana khusus sesuai dengan karakteristik tindak pidana di bidang teknologi informasi dan komunikasi.

Tindak pidana siber yang diatur dalam UU Khusus ini minimal mencakup :

1) Tindak pidana terhadap kerahasiaan, keutuhan, dan ketersediaan data komputer atau sistem komputer, antara lain : illegal acces, illegal interception, data interference, system interference, dan misuse of device.

2) Computer, related crime, antra lain : tindak pidana pemalsuan, pencurian, penipuan, pemerasan, pengancaman, penghinaan, perjudian, dan beberapa tindak pidana tradisional lainnya.

3) Content, related offences, yaitu: pornografi baik pornografi anak maupun pornografi pada umumnya.

Pengaturan tindak pidana siber dalam perundang-undangan Indonesia termasuk UU ITE, memiliki implikasi terhadap pengaturan hukum acara pidananya terutama pengaturan mengenai : alat bukti, kewenangan penyidik untuk melakukan penggeledahan, penyitaan dan kerjasama internasional, peran ahli teknologi informasi dan komunikasi, serta peran industri atau lembaga yang bergerak di bidang teknologi informasi dan komunikasi.

Menurut Orin S Kerr dalam pemberantasan tindak pidana siber damping perlu adanya pengaturan hukum pidana materiil juga diperlukan ketentuan-ketentuan baru dalam hukum acara pidana, karena dalam tindak pidana siber menunjukkan adanya fakta baru yang akan membutuhkan hukuman acara pidana yang baru.

Tindak Pidana Siber dalam Konvensi Dewan Eropa 2001 dalam UU ITE

Tindak pidana siber dalam Konvensi Dewan Eropa 2001 dalam UU ITE berdasarkan sumber dari Naskah Akademik RUU tentang 'Tindak Pidana Teknologi Informasi', pada tahun 2008 Saat ini Pemerintah melalui Kementrian dan Informasi telah Menyusun Draft RUU Ratifikasi Council Of Europe Convention on Cybercrime, 2001. Draft RUU Tindak Pidana Teknologi Informasi Tanggal 11 Maret 2011.

Naskah Akademik RUU Tindak Pidana Teknologi Informasi. 2008. dan Naskah Akademik RUU Tentang Informasi dan Transaksi Elektronik.

Ketentuan hukum pidana materil yang mengatur tindak pidana siber hanya dapat dilaksanakan berdasarkan hukum pidana formil atau hukum acara pidana. Dalam konteks penegakan hukum, kriminalisasi tindak pidana mempunyai kaitan langsung dengan hukum acara pidana. Demikian pula hal nya dengan pengaturan tindak pidana siber dalam perundang-undangan Indonesia, khususnya UU ITE dapat di jalankan dengan berdasarkan ketentuan mengenai hukum acara pidana nya, sebagaimana diatur dalam UU No. 8 Tahun 1981

Penegakan Hukum terhadap Tindak Pidana Siber sebelum berlakunya Undang –Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

a. bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat

b. bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa

c. bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru

d. bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan Peraturan Perundang- undangan demi kepentingan nasional

e. bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdaganga da pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat

f. bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia

g. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f, perlu membentuk Undang-Undang tentang Informasi dan Transaksi

Elektronik

Pasal 1
Dalam Undang-Undang ini yang dimaksud dengan:

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan suara, gambar, peta, rancangan, foto, electronic dat interchange (EDI), surat elektronik (electronic mail) telegram, teleks, telecopy atau sejenisnya, huruf, tanda angka, Kode Akses, simbol, atau perforasi yang telah diola yang memiliki arti atau dapat dipahami oleh orang yan mampu memahaminya

2. Transaksi Elektronik adalah perbuatan hukum yan dilakukan dengan menggunakan Komputer, jaringa Komputer, dan/atau media elektronik lainnya.

3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

6. Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.

7. Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.

8. Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.

9. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.

10. Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.

11. Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.

12. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informas Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

13. Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.

14. Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.

15. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.

16. Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.

17. Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.

18. Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.

19. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.

20. Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.

21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.

22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.

23. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

Pasal 2

Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan huku sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hokum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Pasal 3

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Pasal 4

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia

b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat

c. meningkatkan efektivitas dan efisiensi pelayanan publik

d. membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab dan

e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi

Pasal 5

(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 UndangUndang ini.

(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk :

a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis dan

b. surat beserta dokumennya yang menurut UndangUndang harus dibuat dala bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Pasal 6

Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Pasal 7

Setiap Orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundangundangan.

Pasal 8

(1) Kecuali diperjanjikan lain, waktu pengiriman suatu Informasi

Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim.

(2) Kecuali diperjanjikan lain, waktu penerimaan suatu Informasi

Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.

(3) Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan terjadi pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk.

(4) Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka :

a. waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki system informasi pertama yang berada di luar kendali Pengirim

b. waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki system informasi terakhir yang berada di bawah kendali Penerima.

Pasal 9

Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Pasal 10

(1) Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.

(2) Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah. Pasal 11

(1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan
b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan
c. segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui
d. segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui
e. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa

Penandatangannya dan

f. terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

(2) Ketentuan lebih lanjut tentang Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 12

(1) Setiap Orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya.

(2) Pengamanan Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1 sekurang-kurangnya meliputi :

a. sistem tidak dapat diakses oleh Orang lain yang tidak berhak

b. Penanda Tangan harus menerapkan prinsip kehatihatian untuk menghindar penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik

c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika :

1. Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol atau

2. keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik dan

d. dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

(3) Setiap Orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat (1), bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

Pasal 13

(1) Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.

(2) Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.

(3) Penyelenggara Sertifikasi Elektronik terdiri atas

a. Penyelenggara Sertifikasi Elektronik Indonesiadan

b. Penyelenggara Sertifikasi Elektronik asing.

(4) Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.

(5) Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.

(6) Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 14

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi :

a. metode yang digunakan untuk mengidentifikasi Penanda Tangan

b. hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda

Tangan Elektronik dan

c. hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Pasal 15

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 16

(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut :

a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan

b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut

c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut

d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut dan

e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

(2) Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 17

(1) Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik ataupun privat.

(2) Para pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beriktikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.

(3) Ketentuan lebih lanjut mengenai penyelenggaraan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 18

(1) Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.

(2) Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya.

(3) Jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional.

(4) Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari Transaksi Elektronik internasional yang dibuatnya.

(5) Jika para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (4), penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata Internasional.

Pasal 19

Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati.

Pasal 20

(1) Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.

(2) Persetujuan atas penawaran Transaksi Elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

KESIMPULAN

Berdasarkan pembahasan di atas maka dapat diuraikan kesimpulan sebagai berikut: **Pertama** Yurisdiksi negara terhadap tindak pidana siber berdasarkan perundang-undangan Indonesia berkaitan dengan wewenang negara untuk melakukan regulasi terhadap tindak pidana siber, wewenang negara melalui aparat penegak hukum atau pejabat pemerintah untuk menerapkan hukum, dan wewenang negara untuk menuntut dan mengadili dalam rangka penegakan hukum pidana terhadap tindak pidana siber. Yurisdiksi terhadap tindak pidana siber tersebut meliputi baik dalam hukum pidana materil maupun hukum pidana formil. Yurisdiksi dalam hukum pidana materil dilakukan dalam upaya perlindungan hukum dan keadilan terhadap masyarakat, yaitu dengan adanya kriminalisasi perbuatan tertentu yang merupakan tindak pidana siber dalam UU Khusus tentang Tindak Pidana Siber Yurisdiksi dalam hukum pidana formil dilakukan dengan mengatur hukum acara pidana khusus dalam UU Khusus tentang Tindak Pidana Siber tersebut, khususnya mengenai alat bukti; kewenangan penyelidikan dan penyidikan terutama penggeledahan, penyadapan. dan penyitaan digital evidence, pertukaran informasi elektronik dalam penyelidikan dan penyidikan dengan aparat penegak hukum negara lain peranan computer forensik dan ahli komputer atau ahli teknologi informasi dan komunikasi dalam penyidikan, peranan lembaga pengelola dan industri teknologi informasi dan komunikasi dalam penyidikan; pengembangan kelembagaan penegak hukum peningkatan kemampuan sumber daya aparat penegak

hukum peningkatan sarana prasarana di bidang teknologi informasi dan komunikasi; pengaturan yurisdiksi kriminal berlakunya hukum pidana nasional terhadap tindak pidana siber, dan pentingnya kerjasama internasional dalam pemberantasan tindak pidana siber terutama dalam penyelidikan dan penyidikan. Yurisdiksi tersebut dalam implementasinya didasarkan pada prinsip quasi yurisdiksi dan *teori pro parte locus delicti, pro parte non locus delicti*, sesuai dengan karakteristik tindak pidana siber. **Kedua** Pengaturan yurisdiksi kriminal dalam Buku I KUHP (Pasal 2 s.d. Pasal 9) dan UU ITE (Pasal 2) bersifat terbatas sehingga memungkinkan suatu tindak pidana siber tidak dapat dituntut dan diadili serta akan bertentangan dengan prinsip "no save haven" untuk tindak pidana siber. Pengaturan yurisdiksi kriminal dalam peraturan perundang-undangan Indonesia terhadap tindak pidana siber seharusnya menggunakan prinsip quasi yurisdiksi, yaitu menggunakan yurisdiksi teritorial, yurisdiksi ekstra-teritorial terhadap tindak pidana yang dilakukan di luar wilayah negara tetapi berada dalam yurisdiksi negara lain, dan yurisdiksi ekstra-teritorial terhadap tindak pidana yang dilakukan di luar yurisdiksi negara manapun. Prinsip-prinsip yurisdiksi teritorial yang dapat digunakan antara lain prinsip yurisdiksi teritorial subjektif dan prinsip teritorial objektif dengan perluasan baik sebagian perbuatan atau akibat terjadi dalam wilayah negara dan sebagian lagi berada di luar wilayah negara, prinsip bendera negara kapal dan prinsip pesawat negara terdaftar, dengan perluasan baik bersifat subjektif maupun objektif. Prinsip-prinsip yurisdiksi ekstra-teritorial yang dapat digunakan adalah prinsip nasional aktif, prinsip nasional pasif dan prinsip perlindungan baik tindak pidana dilakukan di dalam yurisdiksi suatu negara maupun di luar yurisdiksi negara manapun, serta prinsip universal untuk tindak pidana siber tertentu. Penerapan prinsip dual criminality dalam pemberantasan tindak pidana siber diterapkan secara terbatas untuk yurisdiksi nasional aktif dan yurisdiksi nasional pasif. Yurisdiksi kriminal berlakunya hukum pidana nasional terhadap tindak pidana siber didasarkan pada teori pro parte locus delicti, pro parte non locus delicti, karena dalam menetapkan yurisdiksi kriminal terhadap tindak pidana siber berdasarkan tenpat terjadinya tindak pidana juga tidak didasarkan pada tempat terjadinya tindak pidana, tetapi didasarkan pada kepentingan-kepentingan hukum yang dilindungi.

SARAN

Berdasarkan kesimpulan di atas maka dapat diuraikan saran sebagai berikut: **Pertama** Dilihat dari masih biasnya makna dari pasal 27 dan pasal 29 UU ITE, diharapkan masyarakat maupun jurnalis yang melakukan aktivitas di dunia cyber dapat lebih bijaksana lagi dalam penggunaan kata maupun kalimat sehingga tidak dianggap masuk dalam kriteria perbuatan yang memenuhi unsur-unsur pencemaran nama baik ataupun penghinaan. **Kedua** Perlunya aturan lebih konkrit dan spesifik yang secara tegas dan jelas mengatur serta membatasi kejahatan cyberbullying sehingga tidak terjadi kebingungan atau penjatuhan sanksi semena-mena kepada masyarakat yang dapat merampas hak asasi manusia yaitu hak kebebasan berekspresi.

DAFTAR PUSTAKA

Buku :

Buku Andi Hamzah, *Hukum Acara Pidana*, Sinar Grafika, Jakarta, 2002.

Balkin, Jack M. et.al. (ed.), *Cybercrime* Digital Cops in Networked Environment, New York University Press, New York, 2006.

Barda Nawawi Arief. *Tindak Pidana Mayantara*. Perkembangan Kajian Cyber Crime di Indonesia, Raja Grafindo Persada, Jakarta, 2006.

Koops, Bert-Jaap & Brenner, Susan W. *Cybercrime and harisdiction*, TMC Asser Press. The Hague, 2006.

Romli Atmasasmita, *Hukum Pidana Internasional Bagian II*, PT. Hecca Mitra Utama, Jakarta, 2004.

Shaw, Malcolm N., *International Law*, Butterworths, London 1986

Shinder, Debra L. Scene of Cybercrime, Computer Forensic Handbook, Syngress Publishing, Rockland, 2002.

Starke, J.G., *Pengantar Hukum Internasional,* (Terjemahan Bambang Iriana Djajaatmadja). Sinar Grafika, Jakarta, 2004

Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung, 2004.

Cyer et al., *Universal Jurisdiction: International and Municipal Legal*

Cedric J. Magnin, *The 2001 Council of Europe on Cyber – Crime: A Efficient*

Tool to Fight Crime in Cyber – Space, LLM Dissertation on Santa Clara University

Adam Chazawi 2003. Pelajaran Hukum Pidana I. Jakarta : RajawaliGrafindoPersada

Sayad Sanusi. 2010 „ "Efektivitas UU ITE Dalam Pengaturan Perdagangan.

Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi, Refika Aditama, Bandung, 2010. Dedi Feriandi, Tinjauan Hukum dan Erika Periklanan di Internet, Menegakkan Hukum Sistem Informasi.*
Institut Teknologi Bandung, Agustus 2000

Barda Nawawi Arief 2005. Bunga Rampai Kebijakan Hukum Pidana Bandung: Citra Bakti

Peraturan Perundang-Undangan :

UU ITE No. 11 Tahun 2008

RUU TIPITI Bab VII Pasal 20 -25

KUHP Pasal 2, Pasal 3 dan Pasal 4 tentang Ketentuan Mengatur Yuridiksi kriminal

Artikel Jurnal :

Kijzer. Nico, *Criminal Jurisdiction Regarding Cross-Border Crimes,*

Penataran Nasional Hukum Pidana dan Kriminologi, ASPEHUPIKI DAN FH UBAYA, Pasuruan, 2002.

ITAC. 2000. *Cybercrime* is a real and growing threat to economic and social development around the world, dalam ITAC, IC Common Views *Paper on: Cyber Crime, IIIC 2000 Millenium Congress*