NASKAH AKADEMIS KEJAHATAN INTERNET *(Cyber Crimes)*

PUSLITBANG HUKUM DAN PERADILAN
MAHKAMAH AGUNG RI
2004

KATA PENGANTAR

Pengambilan thema mengenai kejahatan komputer dalam penelitian tahun ini diawali dengan adanya perkara-perkara yang dapat dikategorikan sebagai kejahatan komputer, yang dimohonkan informasi dan petunjuk dari Puslitbang MA-RI. Dari pertanyaan-pertanyaan yang diajukan tersebut dapat disimpulkan bahwa disamping banyak permasalahan hukum yang ditimbulkan oleh kejahatan jenis baru ini, yang cukup komplek. yang tampaknya belum dapat ditanggulangi oleh Undang-undang Hukum Pidana yang berlaku, juga karena kurangnya wawasan / penguasaan para hakim atas jenis kejahatan ini.

Berbagai jenis kejahatan komputer dari mulai yang sederhana sampai yang kompleks yang memerlukan penguasaan tehnologi yang tinggi, menunjukan bahwa cyber-crime ini dari tahun ke tahun selalu meningkat, dan menimbulkan kerugian yang besar bagi masyarakat, negara dan perusahaan maupun pengguna komputer lainnya.

Jenis kejahatan yang tradisionil yang memerlukan banyak tenaga dan hasil yang terbatas, mulai ditinggalkan dan bergeser pada jenis kejahatan yang mengunakan sarana dan fasilitas internet dengan hasil yang sangat besar. Manipulasi data per-bankan yang tersimpan dalam komputer; pembobolan ATM; pemalsuan kartu kredit; money laundering; merusak system dan data yang terkandung dalam komputer; menyebarkan virus-virus yang berbahaya merupakan jenis kejahatan baru yang berskala nasional dan internasional

Penelitian ini merupakan penelitian awal untuk mengetahui berapa banyak, jenis kejahatan yang mengunakan sarana komputer yang terjadi didaerah-daerah di Indonesia, dan sampai dimana kemampuan hakim dalam menerapkan peraturan-peraturan yang ada. Hasil penelitian ini akan dirangkum dalam suatu laporan yang berbentuk naskah akademis yang menggambarkan permasalahan-permasalahan hukum yang ditimbulkan akibat perkembangan tehnologi komputer; internet dan telekomunasi lainnya, disamping laporan dan analisa questioner yang diedarkan di sebelas wilayah di Indonesia.

Meskipun tidak lasim, pengabungan masalah pidana dan perdata dalam suatu tulisan, namun sebagai tambahan wawasan bagi para hakim, maka dalam tulisan ini disamping uraian permasalahan yang menyangkut perkara pidana, yaitu tentang istilah, jenis kejahatan, permasalahannya dan peraturan yang diterapkan diluar negeri, juga ada penambahan 1 Bab tentang pandangan dari sudut peraturan-peraturan perdata yang secara singkat menguraikan dasar-dasar dari electronic commerce, bagaimana internet memberikan pengaruh yang sangat besar bagi perkembangan ekonomi, baik secara mikro maupun secara makro.

Semoga hasil penelitian ini dapat bermanfaat bagi para hakim dan mereka yang berminat untuk mempelajari berbagai aspek kejahatan komputer

Kepada segenap pihak yang telah membantu penyelesaian tulisan ini, saya sebagai Kordinator Penelitian ini mengucapkan terima kasih, dan demi kesempurnaan naskah ini kami mengharapkan kritik yang konstruktif

Jakarta, 20 Desember 2003

Kapus Litbang Hukum dan Peradilan MA-RI
Selaku Kordinator Penelitian

Susanti Adi Nugroho SH,MH

DAFTAR ISI

BAB I
PENDAHULUAN

A. PERMASALAHAN

Tehnologi Informasi (*information technology)* memegang peran yang penting baik dimasa kini maupun dimasa yang akan datang. Dunia sekarang mengalami revolusi yang dikenal dengan nama 'revolusi informatika' Revolusi ini lebih canggih dan lebih cepat daripada 'revolusi industri' yang terjadi pada abad ke XIX, dimana tenaga manusia diganti dengan tenaga mesin. Dengan makin berkembangnya dan meluasnya teknologi maka semakin besar kemampuan komputer untuk menyimpan dan memproses informasi yang dapat digunakan untuk berbagai keperluan.

Kemajuan di bidang system jaringan Internet dan telekomunikasi menyebabkan komunikasi secara elektronis dari satu negara ke negara lain makin bertambah cepat dan mudah. Peristiwa-peristiwa yang terjadi di belahan dunia yang jauh dapat diketahui hanya dalam hitungan menit melalui jaringan internet. Transfer uang antar bank yang dikenal pula dengan *"E-cash"* di dalam negeri maupun ke luar ngeri dapat dilakukan dengan lebih cepat lagi. Perdagangan melalui Internet di "cyberspace" yang dikenal dengan "electronic commerce" *(E-Commerce)* semakin meningkat. Iklan-iklan untuk segala macam barang dan piranti lunak/software yang dilaksanakan di "cyberspace" sudah merupakan hal lazim yang dengan mudah dapat diamati. Pembayaran untuk pemesanan barang atau program komputer dapat dilakukan dengan menggunakan *"credit card"* dalam formulir yang telah disediakan oleh penjual yang secara cepat muncul dalam komputer para pembeli.

Transfer uang secara elektronis yang disebut dengan "wire transfer" merupakan cara umum untuk untuk mentransfer uang dengan pesan elektronis (electronic messages) antara bank.[1]

Betapa besar uang yang ditransfer setiap harinya melalui jaringan internet dapat dilihat dari fakta kegiatan lembaga-lembaga yang memberikan jasa dibidang ini, misalnya transfer uang antar bank yang dilakukan melalui jaringan komputer melalui sistim *Electronic Funds Transfer System (EFTS)* atau melalui jaringan *Society for Worldwide International Finnancial Telecommunications Transfer (SWIFT).*

Demikian pula halnya, betapa besarnya asset yang perlu dilindungi dapat dilihat dari sarana komputer yang dimiliki oleh suatu Negara dan dari jumlah

[1] U.C.C. Article 4A Prefatory Note (1991) mendefinisikan "wire transfer" sebagai serangkaian transaksi yang dimulai dengan perintah pembayaran dari yang memerintahkan pembayaran ("originator") untuk disampaikan kepada sipenerima perintah itu. (...as "a series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order.")

uang yang ditransfer oleh system elektronis seperti yang dimiliki oleh lembaga EFTS dan SWIFT tersebut ke berbagai penjuru dunia. Berdasarkan penelitian diperkirakan bahwa uang yang ditransfer secara elektronis setiap hari oleh kedua lembaga tersebut lebih banyak dari anggaran Negara Amerika Serikat dan Inggris untuk satu tahun.

Sarana komputer dan biaya pemeliharaanya yang disediakan negara-negara majupun cukup besar mengingat pentingnya komputer untuk pelaksanaan tugas-tugas negara. Misalnya, di Inggris beberapa tahun yang lalu perbelanjaan untuk komputer dan perbaikannya diperkirakan sebesar 3% dari pengeluaran nasional negara Eropa. Nilai peralatan komputer yang dimiliki pemerintah Inggris adalah lebih dari 5 miliar poundsterling dan pengeluaran belanja untuk sistim komputer sekitar 5 miliar poundsterling, sedangkan biaya pemasangan sistim komputer di Inggris setiap tahun meningkat 25%.

Seperempat penghasilan Inggris diperoleh dari aktivitas usaha keuangan dan asuransi yang tergantung kepada sistim komputer. Selain daripada itu setiap harinya sekitar 250 miliar poundsterling melewati kota London melalui peralatan computer.

Laporan keuangan di Amerika Serikat tahun 1989 menunjukkan bahwa setiap tiga jam, empat jaringan komputer utama di Amerika Serikat mentransfer uang yang jumlahnya sama dengan seluruh anggaran pemerintah federal setiap tahun. Disamping itu lembaga-lembaga pertahanan, penerbangan, perbankan, perguruan tinggi, pelayaran, keuangan, ekonomi, pendidikan, kesehatan, ilmu pengetahuan, perindustrian dan lainnya makin banyak menggunakan komputer dan telah meninggalkan cara-cara tradisionil, yang pada akhirnya menimbulkan ketergantungan kepada komputer dalam pelaksanaan tugas mereka. Dengan penemuan Internet dan kemajuan teknologi telekomunikasi data dapat dikirimkan keberbagai penjuru dunia dengan lebih cepat lagi.

Pada gilirannya perkembangan yang cepat dalam bidang komputer menimbulkan titik rawan dalam penyusunan alat pengaman *(security device)* pada sistim komputer, baik untuk keperluan pemerintahan maupun untuk dunia usaha lainnya. Padahal kelemahan dari system yang dipergunakan oleh suatu lembaga seringkali disalahgunakan oleh pihak ketiga untuk kepentingannya sendiri.

Berdasarkan data kepolisian ternyata bahwa organisasi penjahat internasional seperti *Mafia, Yakutza, Yungs* telah mengarahkan sasarannya ke system perbankan dan keuangan lainnya, bahkan yang sudah menggunakan fasilitas Internet. Moto mereka ialah: Apabila dengan memiliki ilmu komputer yang sederhana dan personalia yang terbatas dapat memperoleh hasil yang banyak, mengapa harus bersusah payah melakukan kejahatan tradisionil yang memerlukan tenaga banyak sedangkan hasilnya lebih terbatas. Data menunjukkan bahwa manipulasi data perbankan yang tersimpan dalam komputer, pembobolan ATM dan pemalsuan kartu kredit dengan skala besar

selain seringkali didalangi oleh orang dalam (insiders) juga oleh organisasi internasional tersebut.

Ulah para *"hackers"* untuk menerobos system komputer menimbulkan kerugian yang sangat meresahkan para pengguna komputer. Selain data mereka dapat diintip, perbuatan hackers seringkali menyebabkan rusaknya system dan data yang terkandung dalam komputer. Terlebih lagi apabila perbuatan hacking menyebabkan tersebarnya virus-virus yang berbahaya. Seringkali perbuatan mereka diikuti dengan ancaman pemerasan untuk merusak data komputer yang telah diterobos.

Selain dapat menimbulkan kerugian materi dan keuangan yang besar, dan bahkan mengancam keselamatan jiwa manusia apabila kerusakan terjadi pada system komputer lalu-lintas atau transportasi darat dan udara, kejahatan komputer menimbulkan permasalahan hukum yang serius bagi peradilan pidana di sebagian besar negara-negara di dunia. Oleh karena itu penanggulangan kejahatan komputer tidak cukup dilakukan secara tambal sulam, namun harus dilakukan secara komprehensif oleh karena kejahatan komputer berdimensi luas, bisa dilihat dari aspek pidana maupun aspek perdata, yang berskala nasional maupun internasional.

Dengan munculnya E-Commerce, yaitu tata niaga secara electronis di alam cyber *("cyber space")* memunculkan generasi konsumen baru yang disebut *"cybershoppers"* yang biasa melakukan *"cybershopping"*, dengan melakukan secara E-cash ataupun melalui electronic transfer.[2]

Mengetahui bahwa apa-apa yang dikirim melalui transfer elektronis itu sangat berharga, maka berbagai organisasi penjahat berusaha untuk mengintersepsi dan mengalihkan uang itu ke bank mereka. Hal mana pada akhirnya melahirkan pula berbagai jenis kejahatan yang disebut *"cyber crime"*. Apabila kejahatan terhadap "data" komputer atau *"digital goods"* yang juga mempunyai nilai tinggi yang disebut "digital crimes" sasarannya masih dalam jumlah yang terbatas, kini para pelaku kejahatan telah mengembangkan operasinya dengan kejahatan yang disebut *"cyber crimes"*, yang tentunya dengan dimensi dan sasaran yang yang lebih luas lagi. Swalayan besar di *"cyber space"* (disebut pula *"cybernation"*) kini menjadi sasaran empuk para penjahat internasional yang dengan menggunakan teknologi komputer yang canggih dengan lihai melakukan kejahatan "cyber". Demikian pula halnya, para konsumen yang ceroboh akan menjadi sasaran empuk penipuan melalui Internet *(Internet fraud)*.

---

[2] Ada 3 sistem pengiriman uang secara electronis utama yang dikenal di dunia ini, yaitu:

(1) SWIFT: the Society for Worldwide Interbank Financial Telecommunication, merupakan asosiasi bank yang berbasis di Belgia yang menyediakan jaringan komunikasi untuk transfer uang dalam jumlah besar secara internasional, dan juga di Amerika Serikat sendiri.

(2) CHIPS: the Clearing House Interbank Payments System, system penyelesaian keuangan (funds settlement system) yang dilakukan oleh New York Clearing House;

(3) Fedwire: system transfer keuangan yang secara khusus dipergunakan dan dilakukan oleh (US) Federal Reserve System.

Maka untuk menjamin keamanan dan kelancaran tersebut diperlukan upaya-upaya pengamanan yang optimal, baik secara preventif maupun represif, dan setiap usaha gangguan sebagaimana kecilnyapun harus dicegah sebelum berkembang dan menyebar, antara lain dengan meningkatkan teknologi pengamanan, meningkatkan ketrampilan dan kejujuran/integritas petugas komputer, dan menyempurnakan peraturan perundang-undangan hukum pidana, khususnya yang berkaitan dengan perbuatan penyalahgunaan komputer seperti kejahatan di ruang *"cyber " atau "cyber space"*.

Sistem komputer yang dimiliki berbagai perguruan tinggi seringkali dijadikan tempat percobaan para mahasiswa untuk menerobos -hacking- system komputer orang atau lembaga lain. Dan usaha mereka seringkali berhasil dan seringkali merugikan orang lain. Oleh karena itu berbagai peraturan baru dalam Penal Code telah dikeluarkan agar perbuatan yang tidak terpuji itu tidak dilakukan lagi

B. TUJUAN PENELITIAN DAN HASIL YANG HENDAK DICAPAI

Bagi Indonesia kejahatan yang berkaitan dengan tehnologi tinggi, ataupun kejahatan cyber dengan sarana pengunaan komputer (kejahatan komputer) maupun perdagangan melalui e-commerce masih merupakan hal yang baru, dan belum ada perundang-undangan yang khusus mengaturnya. Kejahatan Komputer ini disamping merupakan kejahatan jenis baru, juga menimbulkan kerugian yang sangat besar bagi masyarakat, negara, dan perusahaan pengguna komputer. Permasalahan hukum yang ditimbulkan oleh kejahatan jenis baru ini cukup kompleks. Beberapa jenis kejahatan komputer tampaknya belum dapat ditanggulangi oleh Undang-undang Hukum Pidana yang berlaku, sehingga perlu dilakukan penafsiran-penafsiran baru untuk memperluas berlakunya undang-undang tersebut.

Penelitian ini dimaksudkan:

1. Untuk mengetahui sampai dimana pengetahuan para hakim mengenai kejahatan komputer ini, dan perkara apa saja (baik pidana atau perkara perdata) yang pernah ada di wilayah Pengadilan Negeri maupun ditingkat banding, baik yang disidangkan oleh responden sendiri maupun oleh hakim lain,
2. Untuk menghimpun pandangan-pandangan dan memberikan gambaran tentang apa dan bagaimana kejahatan komputer ini, kendala-kendala yang diakibatkan perkembangan teknologi komputer, Internet, dan telekomunikasi, beserta permasalahan hukum apa yang ditimbulkan, dan bagaimana usul penyelesaiannya.
3. Penelitian ini juga untuk memberikan gambaran pengalaman dari negara-negara lain sebagai studi perbandingan, sehingga dapat menjadi tolak ukur

formulasi yang bagaimana yang cocok dengan keadaan di Indonesia.

4. Hasil penelitian ini akan dievaluasi dan diterbitkan suatu naskah akademis yang lengkap, yang disamping mengulas laporan hasil questioner, juga ulasan umum tentang apa dan bagaimana kejahatan komputer, dan kasus-kasus yang pernah terjadi. Diharapkan hasil naskah akademis ini dapat dibagikan kepada para hakim sebagai tambahan wawasan.
5. Penelitian dan diskusi ini hanya melibatkan peserta dari para hakim dan panitera dari 4 lingkungan peradilan yaitu Peradilan Umum, Peradilan Tata Usaha Negara, Peradilan Agama dan Peradilan Militer sebagai responden. Dengan adanya pendapat dan argumentasi dari berbagai pihak tersebut, diharapkan hasil penelitian ini dapat sebagai rekomendasi bagi Pimpinan Mahkamah Agung dan dalam jangka panjang sebagai informasi bagi penyempurnaan Hukum Acara yang akan diberlakukan dikemudian hari.

C. METODE PENELITIAN

Berdasarkan permasalahan tersebut diatas, dilakukan penelitian yang bersifat diskriptif dan problem identifikasi. Penelitian ini menggunakan data primer yaitu data yang diperoleh dari lapangan melalui wawancara, pengisian kuesioner dari responden yang hadir. Kegiatan wawancara dilakukan kepada responden yang dianggap dapat sebagai nara sumber yang mempunyai kemampuan memberikan informasi tentang proses penyelesaian perkara. Sedangkan data sekunder diperoleh melalui studi perpustakaan berupa buku-buku baik dari karangan dalam maupun luar negeri, disamping mengolah data dari penelitian-penelitian lain yang pernah dilakukan oleh Mahkamah Agung yang berasal dari empat lingkungan peradilan yaitu Peradilan Umum, Peradilan Agama, Peradilan Tata Usaha Negara dan Militer, yang dianggap dapat mewakili pengadilan-pengadilan lain di seluruh Indonesia.

D. RUANG LINGKUP DAN WILAYAH PENELITIAN

Penelitian ini lebih ditujukan pada wawasan segi pidananya dari kejahatan komputer *(cyber-crime)*, namun untuk menambah dan memperluas wawasan para hakim, seperti yang dikemukakan diatas, penelitian ini juga akan sedikit dikembangkan dengan menambah 1 bab yang secara sepintas akan menguraikan dasar-dasar dari perdagangan melalui elektronik (*Electronic Commerce).* Karena perkembangan teknologi telah menimbulkan berbagai perubahan dan mempengaruhi pula pada kegiatan perdagangan yang semula dilakukan melalui kontak secara fisik, kini dengan teknologi Internet kegiatan perdagangan juga dilakukan secara elektronik atau dikenal dengan nama *E-Commerce.*

Secara sepintas akan menguraikan hal-hal sebagai berikut:

Dari segi pidana yang mengenai kejahatan komputer dan permasalahan akan dicoba untuk memberi pembahasan dan dicarikan pemecahannya di dalam penelitian ini yang mencakup hal-hal sebagai berikut:

1. Arti umum tentang kejahatan komputer, dan komputer sebagai alat untuk melakukan kejahatan tradisional
2. Penipuan dengan memanipulasi komputer
3. Spinase komputer dan pembajakan perangkat lunak

Responden terdiri dari hakim-hakim, panitera dari 4 badan peradilan yang meliputi Wilayah Pengadilan Tinggi Tanjung Karang, Bengkulu, Medan, Pekanbaru, Ujung pandang/Makassar, Denpasar, Mataram, Palu, Banjarmasin, Pontianak dan Bandung. Dari jumlah kuesioner yang diedarkan setiap daerah 50 responden, dapat diasumsikan bahwa kuesioner tersebut merupakan data valid. Disamping jawaban-jawaban melalui kuesioner, juga dilakukan wawancara terhadap beberapa responden hakim tinggi yang dianggap sebagai representatif yang mewakili masing-masing daerah. Untuk lebih jelasnya dapat diuraikan sebagai berikut:

Lokasi atau wilayah penelitian meliputi Pengadilan Negeri dan Pengadilan Tinggi sebagai berikut :

REKAPITULASI JUMLAH KUESIONER

NOMOR	LOKASI	JENIS PERADILAN							JUMLAH
		PT	PN	PTTUN	PTUN	PTA	PA	MAHMIL	
1	BANDUNG	13	10	0	4	6	4	5	42
2	BANJARMASIN	11	14	0	7	7	5	2	46
3	BENGKULU	14	13	0	5	9	11	0	52
4	DENPASAR	15	4	0	5	0	20	5	49
5	LAMPUNG	11	19	0	0	6	9	0	45
6	MAKASSAR	11	9	5	5	10	6	2	48
7	MATARAM	17	10	0	5	8	11	0	51
8	MEDAN	12	9	5	5	1	14	4	50
9	PEKANBARU	14	11	0	5	9	11	0	50
10	PALU	8	16	0	7	7	9	0	47
11	PONTIANAK	18	9	0	5	6	5	5	48
JUMLAH		144	124	10	53	69	105	23	528

BAB II
PENGERTIAN KEJAHATAN KOMPUTER SERTA BEBERAPA ISTILAH TEHNIS KOMPUTER

I. ISTILAH KEJAHATAN KOMPUTER YANG LAZIM DIPER-GUNAKAN

Sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana kejahatan komputer dalam bahasa Inggrispun masih belum seragam. Beberapa sarjana menggunakan istilah *"computer misuse", "computer abuse", "computer fraud", "computer-related crime", "computer-assisted crime"*, atau *"computer crime"*. Namun para sarjana pada umumnya lebih menerima pemakaian istilah "computer crime" oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan internasional.

The U.S. Computer Crime Manual menggunakan *"computer-related crime"* disamping *"computer crime"*.[3] Komisi Franken lebih condong menggunakan 'computer misuse' oleh karena 'computer crime' lebih membatasi pada perbuatan yang dilarang oleh undang-undang hukum pidana, padahal perbuatan penyalahgunaan komputer dapat dilarang pula oleh ketentuan lainnya. Dalam bahasa Belanda sering dipergunakan istilah 'computer misbruik' disamping 'computer criminaliteit'. Dengan berkembangnya jariangan Internet dan telekomunikasi kini dikenal istilah *"digital crimes"* dan *"cyber crimes"* seperti yang akan diuraikan dibawah ini.

Di Indonesia istilah yang biasa dipergunakan ialah 'penyalahgunaan komputer' atau 'kejahatan komputer'.[4] Namun tampaknya istilah yang lebih cocok dipergunakan ialah kejahatan komputer oleh karena penyalahgunaan komputer mengandung pengertian bahwa komputer adalah alat untuk melakukan tindak pidana, padahal dalam kenyataannya seringkali komputer dan data komputer menjadi obyek tindak pidana. Kejahatan komputer memuat pengertian yang lebih luas yaitu semua tindak pidana dimana komputer selain merupakan sarana untuk melakukan suatu tindak pidana, juga merupakan objek dari tindak pidana itu sendiri.

Terlebih lagi dengan munculnya teknologi baru Internet maka

---

[3] Lihat Schojlberg, Stein, Computers and Penal Legislation, A Study of the Legal Politics of a New Technology, Complex-Norwegian Research Centre for Computers and Law, Universiteitsforlaget (1983), hal.3- 4.Lihat pula Wasik, Martin, Crime and the Computer, Oxford University Press (1991), hal.1-4; dan Rostoker, MD et.al.,Computer Jurispru (1986), Oceana, hal. 331-334. Kaspersen menggunakan 'computermisbruik' dalam bukunya Strafbaarstelling van Computermisbruik(1990).

[4] Reksodiputro, Mardjono. "Kejahatan Komputer". Suatu Catatan Sementara dalam Rangka KUHP Nasional yang akan Datang. Makalah dalam Lokakarya BPHN, Departemen Kehakiman, tanggal 18 Januari 1988.

penyebaran informasi dari data suatu komputer untuk berbagai keperluan ke tempat tujuan, dapat dilaksanakan dengan lebih cepat lagi. Mengingat sangat berharganya informasi yang terkandung dalam data komputer yang disebarkan melalui internet itu, para pelaku kejahatan mulai memusatkan usahanya untuk menerobos, merusak, melakukan pemerasan (blackmail), atau memanipulasi untuk kepentingannya data-data yang terkandung dalam setiap komputer, misalnya yang berkatian dengan system pertahanan suatu negara, kegiatan perbankan, hak cipta dan penemuan ilmiyah lainnya.

1. **"Komputer"** ialah alat elektronis, magnetis, optik, kimia-elektris (electrochemical), atau alat pemroses data yang cepat yang menghasilkan fungsi logis, aritmatik, atau penyimpanan dengan memanipulasikan denyut elektronis atau magnit dan meliputi semua fasilitas masuk (input), keluar (output), pemrosesan, penyimpanan, atau komunikasi yang dihubungkan atau dikaitkan kepada alat tersebut.

2. **"Jaringan computer"** ialah interkoneksi dari dua atau lebih komputer atau system komputer dengan satelit, microwave, hubungan, atau sarana komunikasi dengan kemampuan untuk mengirimkan informasi diantara komputer tersebut.

3. **"Program komputer"** ialah sejumlah data yang teratur yang mengandung instruksi-instruksi yang berkode atau keterangan yang apabila dioperasikan oleh komputer menyebabkan komputer memproses data atau melaksanakan fungsi-fungsi tertentu.

4. **"Jasa komputer"** (computer service) ialah hasil dari produksi penggunaan satu komputer, informasi yang disimpan dalam komputer, atau orang yang menjalankan komputer, termasuk waktu penggunaan komputer, pemrosesan data, dan fungsi-fungsi penyimpanan.

5. **"System komputer"** ialah setiap macam kombinasi dari satu komputer atau jaringan komputer dengan dokumentasi, piranti lunak komputer, atau fasilitas fisik yang mendukung komputer atau jaringan komputer.

6. **"Piranti lunak komputer"** – computer software – ialah seperangkat program komputer, prosedur, dan dokumen yang tergabung yang penting bagi jalannya atau berfungsinya suatu komputer, system komputer, atau jaringan komputer.

8. **Digital crimes**
   Kejahatan komputer yang menjadikan data komputer sebagai sasarannya dikenal pula dengan nama "digital crimes". Digit secara harafiah berarti

angka dari nol sampai sembilan. Digital goods ialah "barang" yang berupa denyut elektronis yang berisi data dan informasi yang seringkali mengandung penemuan yang sangat berharga.

9. **Cyber crimes**
   Cyber crimes ialah kejahatan komputer yang dilakukan di "cyberspace" (alam cyber), yaitu diangkasa raya dengan munculnya berbagai transaksi niaga (E-commerce) dan infromasi lainnya yang berharga di cyberspace tersebut yang seringkali disebut "cybers-shop" atau "swalayan cyber".

10. **Internet**
    Internet suatu jaringan media informasi yang dikembangkan tahun 1980 dan dipergunakan secara eksklusif oleh lembaga-lembaga pemerintah Amerika Serikat untuk keperluan penelitian di bidang pertahanan (defence research). Melalui Internet beberapa pejabat dapat menyampaikan informasi atau "bulletin board" kepada seluruh jajarannya di seluruh dunia. Namun dalam perkembangan selanjutnya penggunaannya diperluas untuk berbagai kepentingan. Penemuan yang penting ini akhirnya diikuti dan dikembangkan oleh fihak lainnya yang menciptakan World Wide Web (WWW), yang bekerjasama dengan Internet Service Provider (ISP) seperti CompuServe, Demon Internet, dan lain-lainnya yang berfungsi antara lain untuk menyimpan dan menyebarkan informasi dan transaksi lainnya.[5]

11. **Internet Service Provider (ISP)**
    ISP ialah institusi yang memberikan jasa untuk menghubungkan pengguna (user) dengan Internet.

12. **Pengertian kejahatan komputer**
    Mengenai apa yang dimaksud dengan kejahatan komputer beberapa sarjana hukum memberikan pengertian luas, sedangkan yang lainnya yang sempit.

Pengertian sempit

Sarjana yang menganut pandangan yang sempit memberikan pengertian atau definisi kejahatan komputer sebagai "tindak pidana yang dilaksanakan dengan menggunakan teknologi canggih, tanpa penguasaan ilmu mana tindak pidana tidak mungkin dapat dilaksanakan" *(.....any illegal act for which knowledge of computer technology is essential for its perpetration).* Pakar 'computer law' yang terkenal seperti Don Parker dan Nycum yang menganut pengertian sempit menyatakannya sebagai "setiap perbuatan yang melawan hukum dimana pengetahuan khusus mengenai

[5] Barret, Neil, DIGITAL CRIME, Policing the Cybernation, Kokan Page, 1997, hal. 18-24.

teknologi komputer sangat penting untuk pelaksanaan, penyidikan atau penuntutan".[6]

Pengertian luas

Beberapa sarjana yang menganut pengertian luas seperti Comer memberikan pengertian kejahatan komputer *(computer fraud)* sebagai "setiap perbuatan yang dilakukan dengan itikad buruk untuk tujuan keuangan yang melibatkan komputer"[7] *(.....any financial dishonesty that takes place in a computer environment is a computer fraud).*

The British Law Commission mengartikan *"computer fraud"* sebagai "manipulasi komputer dengan cara apapun yang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain. Mandell membagi "computer crime" atas dua kegiatan, yaitu:

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan;
2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.

U.S. Department of Justice merumuskan "computer crime" secara sempit, yaitu "setiap perbuatan melawan hukum dimana pengetahuan komputer diperlukan untuk pelaksanaan, penyidikan atau penuntutan". *(Any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution).* [8]

Organization of European Community Development merumuskan "computer-related crime" sebagai:

> *"Any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data".* (Setiap perbuatan yang melawan hukum, tidak etis atau tanpa hak sehubungan dengan proses otomatis dan transmisi data). [9]

Kaspersen merumuskannya secara luas, yaitu:

"setiap perbuatan melawan hukum yang secara langsung

---

[6] Parker, D.B.Fighting Computer Crime (1983), hal.23. Lihat pula Wasik (1991), hal. 3.

[7] Wasik, hal. 2 note 8.

[8] Scholjlberg, hal. 4. Buku ini ditulis berdasarkan penelitian mengenai kejahatan komputer yang dilakukannya di Amerika Serikat selama 1 tahun (1981-1982).

[9] Poullet, Yves, "The Law and New Information Technology: A Comparative Approach to the Laws of Continental Europe", dalam buku Gordon Hughes, Essays on Computer Law, Longman Professional, 1990, hal.599-600. Ia adalah Director of Research for Computer Sciences and Law, Facultes Universitaires Notre-Dama de la Paix, Perancis.

mengganggu proses program komputer yang telah dirancang". *("Any illegal act which directly interferes with the planned course of automated data processing").* [10]

Sarjana Jerman Ulrich Sieber, merumuskan kejahatan komputer secara lebih luas lagi..[11] Ia menggolongkan kejahatan komputer sebagai berikut:

Kejahatan Komputer yang berhubungan dengan Ekonomi (Computer-related Economic Crimes) yang terdiri dari:

1. Penipuan dengan manipulasi komputer. *(Fraud by Computer Manipulation)*
2. Spionase komputer dan pembajakan perangkat lunak. *(Computer Espionage and Software Piracy)*
3. Sabotase komputer *(Computer Sabotage)*
4. Pencurian waktu kerja komputer. *(Theft of Services)*
5. Memasuki DP System tanpa hak dan 'hacking' *(Unauthorized Access to DP Systems and 'hacking')*
6. Komputer sebagai alat untuk melakukan kejahatan tradisionil *(The Computer as a Tool for Traditional Business Offences)*

Neil Barrett dalam bukunya yang berjudul "*Digital Crime-Policing Cybernation*"[12] membagi kejahatan komputer sebagai:

1. Crimes against computer, yang meliputi
   a. Theft of computer components
   b. Hackers and digital vandalism, dan
   c. Computer infections

2. Crimes supported by computers, yang meliputi:
   a. Computer pornography
   b. Bootleg software distribution (penyebaran hak cipta tanpa ijin)
   c. Fraud on the Internets
   d. Electronic money laundering

Komisi Franken dari Belanda dan Komisi Inggris yang bertugas menyusun rencana undang-undang tentang kejahatan komputer tidak memberikan pengertian mengenai apa "computer crime" itu walaupun dalam rencana itu disebutkan beberapa perbuatan penyalah gunaan

[10] Kaspersen (1990), hal. 342.
[11] Sieber, Ulrich. The International Handbook on Computer Crime, John Wiley & Sons (1986), hal.21-26.)
[12] Barrett, Neil, Digital Crime - Policing the Cybernation- 1997, Kogan Page.

komputer yang tidak dapat dijangkau oleh undang-undang hukum pidana yang berlaku sekarang. [13]

Dari kedua rancangan undang-undang tersebut tidak terlihat adanya penggunaan definisi mengenai kejahatan komputer. Bahkan usul untuk membuat definisi 'komputer', "data" dan "program" dalam Komisi Inggris tidak mendapat persetujuan mayoritas. Mengingat pesatnya perkembangan teknologi informatika dikhawatirkan pemberian definisi tidak akan sesuai lagi dengan perkembangan baru oleh karena itu diserahkan kepada pengadilan untuk memberikan pengertiannya. Dalam penjelasan resmi Computer Misuse Act 1990 disebutkan:

> *A number of terms are defined in section 17, but "computer", "data" and "program" are not defined in the Act and should, therefore, be given their ordinary meaning by the courts.* [14]

Tahun 1984 the Criminal Justice section of the American Bar Association memberikan definisi yang luas terhadap kejahatan komputer yaitu yang meliputi:

> 'Criminal activities directed against computers and criminal activities in which computers were used as the instruments to perpetrate the crime' (semua tindak pidana yang ditujukan terhadap komputer dan tindak pidana dimana komputer dipergunakan sebagai alat untuk melakukan tindak pidana)[15]

Pemberian pengertian itu dirasakan penting agar ada keseragaman tentang apa kejahatan komputer itu, hal mana sangat bermanfaat bagi studi ilmiyah, penulisan, penyidikan dan penuntutan, dan untuk mempermudah penyusunan statistik pidana, sehingga dapat diketahui mana yang termasuk kejahatan komputer dan mana yang tidak.

II. AMANDEMEN U.S. FEDERAL PENAL CODE

Dengan memperhatikan semkin beragamnya kejahatan komputer dan semakin canggihnya cara sipelaku kejahatan melaksanakan niat jahatnya, Undang-undang Federal Amerika Serikat telah beberapa kali menyempurnakan undang-undang hukum pidana mengenai "Computer Crime" dengan memberikan penjabaran lebih lanjut apa yang yang termasuk kejahatan

[13] Lihat Report of the Dutch Committee on Computer Crime, Ministry of Justice, The Hague (1988).
[14] Lihat The British Commission on Computer Misuse (1990).
[15] .Rostoker, Michael D and Rines, Robert H. Computer Jurisprudence(1986), hal.334.

komputer, barang (property), dan definisi sarana dan kegiatan yang berhubungan dengan komputer dan pemakaiannya. Amandemen terakhir dilakukan September 2001.

Chapter 33 tentang Computer Crimes memperluas pengertian barang (propery) sehingga meliputi barang yang berwujud (tangible goods) dan barang yang tidak berwujud (intangible goods) yang meliputi jaringan komputer, system komputer atau data; dan segala macam penggunaan komputer.[16]

III. AMANDEMEN INDIAN PENAL CODE: ELECTRONIC COMMERCE ACT 1998

India mencoba menyempurnakan beberapa undang-undang demi untuk memberantas kejahatan computer secara efektif. Selain menyempurnakan pasal-pasal dalam Penal Code yang berhubungan dengan barang (property) yang merupakan "tangible object sehingga meliputi pula "intangible objects" seperti data computer dan sarana penunjang lainnya, India pada tahun 1998 telah mengundangkan undang-undang khusus tentang Computer Crime yang dimasukkan dalam Part XII "Electronic Commercial Criminal Act" 1998. Diaturnya computer crime dalam bagian tersebut oleh karena pembuat undang-undang khawatir bahwa amandemen dalam Penal Code belum bisa menjangkau segala jenis kejahatan komputer yang mungkin muncul dikemudian hari. Dikhawatirkan pula bahwa pengadilan akan ragu-ragu menerapkan ketentuan pidana untuk kasus-kasus tertentu.[17]

Pasal 49 ECA 1998 mengatur kejahatan komputer sebagai perbuatan dengan sengaja memasuki, merusak, atau mencoba memasuki data base computer, computer, system informasi atau jaringan komputer (computer network), dengan maksud:

(a) Secara melawan hukum menguasai, memperoleh, menggunakan atau menghalangi orang lain untuk memperoleh keuntungan uang, barang, data atau rekaman elektronis, mengkopi atau merusak data atau rekaman elektronis, menggunakan atau mengganggu fungsi komputer, jaringan komputer atau system informasi, atau melakukan kejahatan yang diatur dalam Indian Penal Code, atau
(b) Dengan sengaja menipu, memperoleh, atau mencoba memperoleh jasa komputer dengan memalsukan identitas, atau menggunakan uang orang

---

[16] Chapter 33: Computer Crimes -
Definitions
(16) "Property" means:
(A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or
(B) the use of a computer, computer system, computer network, computer software, or data.

[17] Lihat Lampiran II tentang Electronic Commercial Act.

lain tanpa ijin dengan cara memasang atau menempelkan fasilitas atau perlengkapan atau dengan cara lainnya.

(c) Dengan sengaja dan tidak hati-hati memasukkan atau membiarkan masuknya virus komputer kedalam komputer apa saja, system komputer, atau jaringan komputer tanpa ijin sipemilik. [18]

Dengan diundangkannya ECA ini diharapkan kejahatan komputer yang tidak dapat dihukum berdasarkan Penal Code 1860, dapat dihukum berdasarkan undang-undang ini.

Dari definisi yang bermacam-macam ini dapat diambil kesimpulan bahwa pengertian yang luas ialah tindak pidana apa saja yang dilakukan dengan memakai komputer ("hardware dan software") sebagai sarana/alat, atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Sedangkan yang sempit ialah tindak pidana yang dilakukan dengan menggunakan teknologi komputer yang canggih.

Di dalam praktek sehari-hari kedua macam kejahatan sama-sama dapat menimbulkan bahaya yang besar baik bagi harta benda maupun keselamatan jiwa manusia.

[18] For the purpose of this Act, any person who commits any of the following acts is guilty of an offense of computer crime:

(a) Intentionally accesses, damages or conceals, or attempts to access, damage or conceal, temporarily or permanently, any computer data base, computer, information system or computer network, without permission from the owner, in order to either:
  (i) wrongfully control, obtain, make use of or prevent others from deriving the benefits of money, property, data or electronic records;
  (ii) copy or destroy any data or electronic records;
  (iii) use or disrupt any functions of computers, computer networks or information systems; or
  (iv) commit any act that is an offense under the Indian Penal Code.

(b) Knowingly, and with the intent to defraud, obtains or attempts to obtain any computer services by false representation, false statement or unauthorized charging to the account of another, by installing or tampering with any facilities or equipment, or by any other means.

(c) Intentionally or recklessly introduces or allows the introduction of any computer virus into any computer, computer system or computer network without permission of the owner.

BAB III
JENIS KEJAHATAN KOMPUTER DAN PERMASALAHAN HUKUMNYA

1. PENGANTAR

Teknologi komputer telah menimbulkan banyak permasalahan hukum pidana terutama disebabkan oleh karena undang-undang hukum pidana menurut sejarahnya dibentuk antara lain untuk melindungi harta kekayaan berupa barang yang merupakan "tangible object", yaitu sesuatu yang secara fisik dapat dilihat, dicium atau diraba. Waktu peraturan mengenai hal ini diundangkan pembuat undang-undang belum memikirkan bahwa di kemudian hari akan muncul suatu teknologi baru yang menciptakan "data komputer" yang merupakan "electronic impulses" (denyut elektronis) yang mempunyai wujud dan pengertian lain dari pada barang. Bahwa dengan kemajuan teknologi telekomunikasi data-data tersebut dapat diproses dengan cepat dan disebarkan ke berbagai penjuru dunia dalam waktu singkat.

Sehubungan dengan hal tersebut permasalahan hukumpun timbul tentang apakah tindak pidana terhadap data komputer, yang seringkali mempunyai nilai yang tinggi dapat dipersamakan dengan tindak pidana terhadap barang seperti diatur dalam beberapa pasal Kitab Undang-Undang Hukum Pidana, seperti: pencurian, penggelapan, penipuan, perusakan, tanpa hak memasuki pekarangan orang lain, dan lainnya.

Sehubungan dengan dapat disimpannya secara elektronis berbagai macam informasi dalam data komputer, dan tidak lagi dicatat di atas kertas, apakah perbuatan pemalsuan, pengkopian, manipulasi informasi dalam data komputer dan perusakan data komputer dapat dipersamakan dengan pemalsuan surat atau dokumen dan perusakan barang.

Selanjutnya dengan ramainya lalu-lintas informasi melalui jaringan internet dan lainnya di "cyber space", apakah penyalahgunaan informasi tersebut masih dapat ditanggulangi oleh Penal Code - KUHP dan peraturan perundangan lainnya. Apakah sabotase computer atau system computer suatu negara yang sangat vital seperti yang dimiliki Departemen/Lembaga Pertahanan, Telekomunikasi, Perhubungan, Penerbangan, dan lainnya, yang dapat mengakibatkan kerugian yang sangat fatal baik terhadap Negara, keselamatan jiwa manusia maupun harta-benda masih dapat ditanggulangi oleh hukum pidana "tradisionil".

Dari kasus-kasus yang pernah terjadi, dan dengan adanya putusan hakim yang saling bertentangan membuktikan bahwa kejahatan komputer yang beraneka ragam bentuknya sejak semula telah menimbulkan kesulitan dalam penerapan hukumnya. Untuk dapat mengerti apa yang menjadi permasalahan

hukum pada setiap bentuk kejahatan komputer, terlebih dahulu perlu diketahui jenis-jenis kejahatan komputer.

Para pakar *"computer law"* telah mencoba membagi jenis kejahatan komputer atas beberapa katagori. Beberapa pakar membagi jenis kejahatan komputer atas tindak pidana yang masih dapat dituntut berdasarkan undang-undang hukum pidana "tradisionil" dan jenis-jenis baru yang belum ada pengaturannya. Dari kasus yang pernah terjadi memang ternyata bahwa beberapa kejahatan komputer masih dapat diselesaikan dengan peraturan pidana tradisionil walaupun hakim kadang-kadang harus memberikan interpretasi yang luas, namun bagi beberapa jenis lainnya ternyata tidak dapat dijangkau oleh peraturan pidana yang berlaku, dan hakimpun enggan untuk melakukan interpretasi yang terlalu menyimpang. Putusan hakim tingkat pertama yang terlalu menyimpang biasanya dibatalkan dalam tingkat banding atau kasasi apabila dimintakan banding dan kasasi Hugo Cornwall, Datatheft, Mandarin: London, 1990. Pakar dari Amerika Serikat yang telah menulis beberapa buku mengenai kejahatan komputer antara lain Data Theft, (1990) membagi kejahatan komputer atas:

1. datafraud,
2. dataspying,
3. dan data-theft.

Pakar Jerman Ulrich Sieber membagi kejahatan komputer yang berhubungan dengan ekonomi (computer-related economic crimes) atas:

1. Fraud by computer manipulation.
2. Computer Espionage dan Sofware Piracy.
3. Computer Sabotage.
4. Theft of Services.
5. Unauthorized Access to DP systems dan "HackTraditional business offences assisted by data processing. Sieber (1986), hal.3-20.

Pakar Inggris Martin Wasik membagi kejahatan komputer atas:

1. Unauthorized access and unauthorized use;
2. Fraud and information theft;
3. Associated offences. Wasik (1991), hal.69-156.

Pakar Inggris lainnya Colin Tapper membagi kejahatan komputer atas:

1. Seeking direct advantage by fraud, theft or deception;
2. Using computer facilities for indirect private gain;
3. Securing unauthorized access to computing facilities;
4. Causing damage to the less tangible facets of a computer system.

Pembagian kedua pakar Inggris tersebut disesuaikan dengan permasalahan hukum beberapa kejahatan komputer yang belum terjangkau

oleh undang-undang pidana yang berlaku di Inggris, yang dibicarakan oleh Scottish Law Commission dalam rancangan undang-undang mengenai Computer Crime yang dikeluarkan tahun 1986 dan 1987, dan oleh The (British) Law Commission for England and Wales dalam Report on Computer Misuse yang dikeluarkan tahun 1988 dan 1989.

Sarjana Eropah lainnya seperti Schjo/lberg dari Denmark (1986) membagi kejahatan komputer atas beberapa jenis-jenis kejahatan yang sering terjadi dan menimbulkan permasalahan hukum seperti:

1. Pencurian;
2. Penggelapan;
3. Penipuan;
4. Pemalsuan;
5. Tanpa hak memasuki data program (DP) system;
6. Tanpa hak menggunakan komputer dan pencurian waktu atau fasilitas komputer. (Unauthorised use of a computer and theft of computer time and services).

Di negeri Belanda, Komisi Franken dalam Rancangan Undang-Undang mengenai Kejahatan Komputer mengusulkan penalisasi beberapa perbuatan penyalahgunaan komputer, yaitu:

1. dengan sengaja memasukkan, mengubah, menghapuskan atau menempatkan di luar fungsi data komputer atau program komputer, dengan maksud untuk secara melawan hukum memindahkan uang atau mengusahakan hal lain yang berharga;
2. dengan sengaja memasukkan, mengubah, menghapuskan atau menempatkan di luar data komputer atau progam komputer, dengan maksud untuk memalsu;
3. dengan sengaja memasukkan, mengubah, menghapuskan atau menempatkan di luar fungsi data komputer atau program komputer dengan maksud untuk menghambat berfungsinya suatu sistem komputer atau sistem telekomunikasi;
4. melanggar hak eksklusif dari si pemilik dari suatu program komputer yang dilindungi dengan maksud mengeksploitasi program secara komersial dan menjualnya di pasar;
5. dengan sengaja berusaha masuk kepada atau dengan sengaja mencegat fungsi dari suatu sistem komputer atau sistem telekomunikasi, atau dengan cara melanggar tindakan-tindakan pengamanan, atau dengan tujuan-tujuan yang tidak jujur atau yang merugikan. [19]

Beberapa ketentuan baru tersebut dimasukkan kedalam beberapa pasal

[19] Lihat Report of the Dutch Committee on Computer Crime, Ministry of Justice, 1988.

Strafrecht sebagai tambahan/penyempurnaan dan yang lainnya dijadikan pasal-pasal baru.

Dalam rancangan undang-undang Komisi Franken membedakan tiga kepentingan yang harus dilindungi undang-undang hukum pidana sehubungan dengan penggunaan komputer, yaitu:

1. tersedianya atau bekerjanya sarana (availability atau beschicksbaarheid),
2. integritas (integrity atau integriteit) dan
3. sifat khusus data (exclusivity atau exclusiviteit).

Untuk dapat melaksanakan sistim komputer dengan lancar, sistim tersebut harus terjamin dari segala macam gangguan. Kasus-kasus yang terjadi menunjukkan bahwa dengan adanya gangguan terhadap sarana atau data komputer tersebut pekerjaan suatu perusahaan atau instansi pemerintah menjadi terhenti yang mengakibatkan kerugian yang besar kepada yang bersangkutan, dan kadang-kadang menimbulkan korban jiwa.

Perbuatan yang dapat mengganggu tersedianya sarana ialah:
Sabotase, perusakan, membuat tidak bekerja, memindahkan data, mengganggu, membuat gangguan sedemikian rupa sehingga sipemilik tidak dapat menggunakan sistim komputer tersebut.

Perbuatan yang dapat mengganggu tersedianya atau bekerjanya data ialah:
menghapuskan, memindahkan, merusak data, membuat data tidak dapat dicapai atau dimasuki oleh yang berhak.

Perbuatan yang dapat mengganggu integritas sarana ialah: memanipulasi data.

Perbuatan yang dapat mengganggu integritas data ialah:
pemasukan data yang tidak benar, merubah data, menambah data.

Perbuatan yang dapat mengganggu sifat khusus data yaitu kerahasiaan dan kemandirian (privacy) adalah:

terhadap sarana : tanpa ijin memasuki sistim;
terhadap data : mengadakan pemeriksaan (memata-matai/mengintip), menyebarkan dan mempublikasikan.

Perbuatan yang mengganggu pemakaian adalah:
terhadap sarana : penggunaan tanpa ijin terhadap data: penggunaan yang tidak benar dan tanpa hak, memperbanyak, pemakaian untuk komersil.[20]

[20] *Ibid*, hal.13-18.

Neil Barrett [21] membagi kejahatan computer atas:

A. Crime Against Computer, yang meliputi
   a. Theft of computer components
   b. Hackers and digital vandalism
   c. Computer infections

B. Crime Supported by Computers, yang meliputi:
   a. Computer pornography
   b. Bootleg software distribution
   c. Fraud on the internet
   d. Electronic money laundering

Dari pembicaraan para pakar tersebut beberapa jenis kejahatan komputer yang menimbulkan permasalahan hukum adalah sebagai berikut:

1. Pencurian software dan Penggelapan
2. Penipuan biasa dan penipuan melalui internet
3. Pemalsuan
4. Sabotase dan perusakan, termasuk dengan menggunakan virus
5. Tanpa hak menggunakan komputer dan waktu/fasilitas komputer (Unauthorised use of computer and Misuse (Theft) of Computer Time and Facilities)
6. Tanpa hak memasuki sistim komputer - hacking
7. Electronic money laundering

2. JENIS KEJAHATAN KOMPUTER DAN PERMASALAHANNYA

A. PENCURIAN DAN PENGELAPAN

1. Pencurian dan Pengelapan

Dengan dipergunakannya komputer untuk menyimpan dan memproses informasi bagi berbagai macam kegiatan para pelaku kejahatan komputer menyadari bahwa agar dapat berhasil diperlukan pengetahuan tentang komputer. Mengingat ilmu tersebut dengan mudah dapat dipelajari, biasanya sipelaku terlebih dahulu mempersiapkan diri dengan ilmu komputer.

Dalam hal objek yang akan dicuri atau digelapkan dilindungi dengan system pengaman yang ketat sipelaku seringkali membujuk orang dalam untuk membuka system pengaman atau password yang digunakan dengan imbalan tertentu. Apabila usaha ini tidak berhasil

[21] Lihat Barrett, Neil: "Digital Crime" – Policing the Cybernation (1997),

sipelaku sering pula menculik dan memaksa petugas komputer untuk membuka rahasia system komputer yang dipergunakan.

Dalam pencurian dan penggelapan cara yang lazim dipergunakan ialah dengan memanipulasi data atau memasukan keterangan palsu kedalam komputer, yang bisa dilakukan dengan merubah data atau menambah data tersebut. Perbuatan tersebut dikenal dengan nama "data didling".

Pemprosesan data dari suatu perusahaan besar seperti bank biasanya melibatkan beberapa orang, seperti yang membuat program, yang mencatat/memasukkan data, yang mengirimkan, yang memberikan kode, yang melakukan pengecekan, dan lainnya. Kemungkinan pemalsuan data dapat dilakukan dalam salah satu proses tersebut, terlebih lagi jika ada kerjasama dengan atau antara semua petugas komputer, proses memanipulasi data dapat berjalan dengan lebih lancar lagi.

Manipulasi data dapat dilakukan misalnya dengan memalsukan dokumen yang akan dimasukan, mengganti disket dengan yang palsu yang telah dipersiapkan sebelumnya, atau merubah sumber data. Apabila perusahaan atau bank tersebut telah menggunakan system Internet dan istem penbgaman tidak terlalu ketat, maka dengan teknologi yang lebih canggih sipelaku kejahatan dapat memasuki dan memanipuasi data perusahaan dari jauh melalui remote terminal.

Objek pencurian bisa bermacam-macam. Seringkali data komputer lebih menarik oleh karena berisi informasi atau rahasia yang sangat bernilai untuk dijual. Seringkali pula manipulasi itu digunakan untuk memperoleh keuntungan keuangan atau barang. Dengan merubah data sipelaku atau kawannya seakan-akan berhak atas sejumlah uang.

Dalam pencurian barang dengan memanipulasi data dimaksudkan untuk menyesatkan petugas pengawas atau pemilik sehingga tampaknya barang-barang milik perusahaan telah rusak, tak berguna atau telah habis terjual, padahal barang tersebut telah dicurinya atau digelapkan jika sipelaku adalah pegawai perusahaan tersebut.

Salah satu contoh kasus yang lazim dilakukan Amerika Serikat dan Negara lainnya ialah petugas komputer perusahaan mencuri sejumlah barang dengan merubah data komputer yang berisi daftar barang. Dengan perubahan data tersebut dimaksud untuk menghilangkan sejumlah barang sehingga sipelaku dapat memiliki barang itu tanpa terlihat dalam laporan bulanan. Biasanya sesudah berlangsung lama kehilangan ini baru diketahui.

Dengan berkembangnya system Internet, perdagangan kini mulai banyak dilakukan melalui jaringan ini. Ternyata bahwa para pelaku kejahatan komputer telah memulai kegiatannya dengan melakukan

manipulasi informasi data dan penipuan disamping "joycomputing" atau "hacking".

Kejahatan yang sering terjadi ialah pemesanan barang melalui Internet dengan menggunakan credit card orang lain tanpa hak, menggunakan identitas yang tidak benar untuk melakukan transaksi jual beli misalnya dengan menggunakan nama perusahaan yang terkenal, mengintersepsi komunikasi antara sipenjual dan sipembeli demi untuk kepentingannya, memindahkan barang atau informasi yang akan dijual kedalam kekuasaannya dengan memanipulasi transaksi yang sedang berlangsung dan lainnya.

Apabila pembayaran dilakukan dengan kartu kredit seringkali identitas kartu kredit sipemilik disadap di tengah jalan dan kemudian dipergunakan oleh sipelaku kejahatan untuk kepentingannya. Segala beban pembayaran penggunaan kartu krerdit tentunya dibebankan kepada sipemilik yang lengah tersebut. Mengingat belum tersedianya pengamanan untuk penggunaan kartu kredit dalam system Internet, penerbit kartu kredit (American Express, Visa atau Master Card) menasehati untuk tidak mempergunakannya dalam E-Commerce dengan Internet.

Dalam kasus kejahatan komputer dengan memanipulasi data dimana yang menjadi objek adalah uang atau barang, pada umumnya ketentuan pidana "tradisionil" mengenai pencurian atau penggelapan dapat diterapkan. Namun kejahatan yang menjadi obyek data (software) terlebih lagi yang dilakukan dengan melalui jaringan Internet dapat menimbulkan permasalahan hukum yang serius.

Bagaimana ruwetnya menanggulangi kejahatan computer yang dilakukan di "cyber space" dapat dilihat dari kasus-kasus mutakhir yang terjadi hampir setiap hari, yang diberitakan melalui internet.

Kejahatan komputer atau cyber crimes yang terjadi tersebut di atas sangat merugikan masyasrakat luas sehingga perlu penanggulangan yang efektif. Beberapa "hackers" telah dapat dideteksi dan ditangkap, namun sejumlah besar lainnya masih tetap berkeliaran. Seringkali korban tidak mau melaporkan bahwa komputer mereka telah menjadi sasaran kejahatan, sehingga mempersulit penanggulangan kejahatan komputer.

2. Salami Technique

Seringkali penggelapan dilakukan dengan cara mengambil uang dalam jumlah yang tidak terlalu banyak, misalnya mengambil "pecahan" uang nasabah yang disimpan di suatu bank. Namun oleh karena dilakukan atas sejumlah nasabah dan dalam waktu relatip lama maka jumlahnya menjadi besar. Oleh karena yang menjadi objek sasaran ialah nasabah yang uang simpanannya banyak, maka si pemilik uang itu sendiri biasanya tidak memperhatikan kehilangan "beberapa

dollar" dari uang simpanannya itu disitu. Uang yang digelapkan itu kemudian dimasukan dalam pembukuan fiktif atau pembukuan sipelaku atau orang tertentu yang dapat diambil setiap saat dengan prosedure yang normal. Para pelaku seringkali lolos dari penelitian oleh karena biasanya sipemilik uang tidak akan memperhatikan atau merasakan adanya kehilangan oleh karena jumlahnya yang kecil itu.

Pada umumnya pembukuan yang fiktif dapat dilakukan dengan lebih berhasil apabila menggunakan sistim komputer daripada sistim manual, terlebih lagi apabila sistim kontrol atau sistim pengamanan tidak efektif. Administrasi penggajian pegawai yang menggunakan sistim komputer seringkali menjadi sasaran kejahatan komputer, misalnya dengan menciptakan nama palsu. Pada perusahaan yang banyak pegawainya sering terjadi manipulasi gaji, yaitu dengan mengurangi gaji beberapa pegawai tertentu dan dimasukan dalam daftar gajinya atau orang gaji orang tertentu, atau dengan menciptakan nama fiktif yang berhak mendapat gaji. Berhubung dengan banyaknya pegawai sulitlah bagi petugas pengawas atau pimpinan perusahaan untuk mengetahui dengan cepat apabila ada penyelewengan.

Kasus penggelapan lainnya yang sering terjadi ialah pada instansi yang biasa membayar tunjangan pensiun dan kesejahteraan sosial. Kasus-kasus seperti itu sering terjadi di Amerika Serikat dan beberapa negara lainnya berhubung dengan dipergunakannya sistim komputer, dan diperkirakan akan semakin bertambah di masa-masa mendatang. Kesulitan untuk mendeteksi bertambah apabila yang menjadi pelakunya adalah orang dalam atau bekerja sama dengan orang dalam yang mengetahui seluk-beluk pengoperasian sistim komputer perusahaan.

Dalam salah satu kasus penggelapan sipelaku yang adalah pegawai dari satu kantor sosial telah berhasil mencairkan lebih dari $100,000 yang dilakukan bersama-sama orang luar. Hal mana dipermudah oleh karena pegawai tersebut diserahi tanggung jawab pengoperasian komputer kantor tersebut. Dengan menciptakan nama-nama palsu ia telah berhasil membuat cek palsu yang diterima oleh kawan-kawannya di tempat lain. Setelah cek berhasil diuangkan data palsu dalam komputer dihapus kembali sehingga waktu diadakan pemeriksaan oleh badan pemeriksa keuangan kehilangan tersebut tidak segera diketahui. [22]

Kasus yang pernah terjadi menunjukkan pula bahwa seringkali terjadi bahwa manager, operator komputer dan sejumlah karyawan lainnya dari satu perusahaan bekerja sama dalam pemalsuan dan manipulasi komputer yang mengakibatkan kerugian besar pada

[22] Schjolberg, hal.60.

perusahaan tersebut dan sulit untuk diteliti, seperti kasus perusahaan asuransi Equity Funding Corporation yang terjadi tahun 1964 sampai tahun 1972 di Amerika Serikat, dimana yang menjadi korban ialah para nasabah, pemegang saham, dan perusahaan reasuransi lainnya. Lebih dari 60,000 polis asuransi palsu berhasil diciptakan yang mengakibatkan kerugian lebih dari US$2 miliar, termasuk kerugian yang diderita pemegang saham. Setelah berlangsung beberapa tahun lamanya barulah kejahatan itu dapat diketahui.

Dari contoh memanipulasi data untuk mendapatkan keuntungan tertentu pada umumnya ketentuan pidana mengenai pencurian dan penggelapan dapat diterapkan.

3. Electronic Piggybacking

Cara lain untuk "mencuri" ialah dengan menyembunyikan terminal atau alat penghubung kedalam sistim komputer itu secara diam-diam. Dengan melalui terminal tersebut data komputer dapat dipelajari atau ditransfer untuk "dicuri" apabila komputer sedang tidak dipergunakan. Semakin banyak komputer dihubungkan kepada "central terminal" semakin besar kemungkinan seseorang untuk dapat menyadap data komputer tanpa diketahui.

Dalam salah satu kasus yang terjadi di Amerika Serikat seorang bekas pengawas suatu perusahaan komputer dengan menggunakan remote terminal dari tempatnya di negara bagian lain telah memasuki sistim komputer perusahaan itu untuk mendapatkan informasi dari program yang sedang dibuat untuk suatu badan federal.[23]

Ia telah menggunakan "password" temannya untuk dapat memasuki sistim komputer perusahaan itu dan mentransfer data yang ada kepada komputer pribadi. Peristiwa itu dapat diketahui petugas komputer disitu yang mengetahui bahwa sipemilik kode tersebut tidak sedang menggunakan komputer. Dalam pemeriksaan terdakwa mengakui maksud perbuatannya itu ialah untuk menjual informasi tersebut kepada pihak ketiga.

4. Permasalahan Hukum

Undang-Undang Hukum Pidana yang mengatur tentang pencurian dan penggelapan hampir disemua sistim hukum pidana mensyaratkan sipelaku mengambil ("menguasai") sesuatu barang milik orang lain secara melawan hukum dengan maksud untuk memilikinya secara tetap (permanen). Pasal 362 Kitab Undang-Undang Hukum Pidana mengatur:

"Barangsiapa mengambil barang, yang seluruhnya atau sebagian

[23] Lihat 'pencurian software'.

kepunyaan orang lain, dengan maksud untuk memiliki barang itu dengan melawan hukum dana karena mencuri dengan pidana penjara selama-lamanya lima tahun atau denda sebanyak-banyaknya sembilan ribu rupiah".

Pasal 372 Kitab Undang-Undang Hukum Pidana mengatur:

"Barangsiapa dengan sengaja dan dengan melawan hukum memiliki barang, yang sama sekali atau sebagian kepunyaan orang lain, dan yang ada padanya bukan karena kejahatan, karena bersalah melakukan penggelapan, dipidana penjara selama-lamanya empat tahun atau denda sebanyak- banyaknya sembilan ratus rupiah".

Menurut sejarahnya yang dimaksud dengan barang ialah sesuatu yang berwujud atau dapat diraba (tangible object). Dengan dicuri atau digelapkannya barang milik orang lain maka penguasaan atas barang itu beralih kepada sipencuri atau kepada yang menggelapkan. Persyaratan tersebut tercantum hampir pada semua "Penal Code" yang berlaku di sebagian besar negara-negara. [24]

5. Pencurian Software

Permasalahan hukum pencurian dan penggelapan timbul apabila yang dicuri atau digelapkan adalah data komputer atau "digital goods".

Sebelum Undang-undang Hukum Pidana disempurnakan, tampaknya pengadilan di beberapa negara tidak selamanya sependapat mengenai apakah data komputer sama dengan barang, hal mana terbukti dengan adanya putusan-putusan yang bertentangan satu sama lainnya, seperti terlihat pada putusan-putusan yang dijatuhkan oleh pengadilan-pengadilan di beberapa negara seperti Belanda, Perancis, Inggris, Canada, Australia dan Amerika Serikat.

Data komputer dapat "dicuri"atau "digelapkan" tanpa mengambil "disket" ("hard disk") atau "carrier" yang berisi data. Dengan memasuki sistim komputer sipelaku kemudian secara melawan hukum mentransfer atau mengkopi data tersebut kedalam komputernya ditempat itu atau ditempat lain melalui jaringan (kadang-kadang melalui Internet) yang telah ada.

Dengan diambilnya data tersebut maka akan diperoleh informasi atau rahasia-rahasia yang berharga yang mungkin tersimpan dalam data itu. Perpindahan tersebut terjadi secara elektronis tanpa merubah atau

[24] Lihat misalnya pasal 127, Penal Code Austria; pasal 461 dan 463, Penal Code Belgia; pasal 379, Penal Code Perancis; pasal 242 dan 246, Penal Code Jerman Barat; pasal 624, Penal Code Italia; pasal 235, Penal Code Jepang; pasal 461, Penal Code Luxemburg; dan untuk Inggris pasal 4(a), English Theft Act 1968). Lihat Sieber (1986), hal. 38-39.

mengurangi isi data semula. Seringkali data yang dicuri itu berisi keterangan penting dari seseorang atau rahasia hasil penemuan dalam bidang ilmu pengetahuan tertentu atau kedokteran yang mempunyai nilai yang tinggi untuk dijual.

Salah satu cara untuk memasuki sistim komputer tersebut ialah dengan menggunakan kode ("password") orang lain yang diperolehnya secara melawan hukum, atau membujuk petugas komputer untuk memberitahukan password komputer tersebut. Dengan cara demikian ia dapat memasuki data komputer secara leluasa dan "mencuri" data yang dikehendakinya.

Pada umumnya ketentuan pidana "tradisionil" yang berlaku tentang pencurian atau penggelapan tidak dapat diperlakukan atas pengambilan "data komputer" yang berupa "intangible object". Seperti telah diuraikan di atas, ketentuan pidana mengenai pencurian atau penggelapan dapat diterapkan apabila sipelaku menggunakan komputer untuk mengambil atau menggelapkan sesuatu barang atau harta kekayaan seperti uang tunai, cek, surat berharga, atau barang lainnya yang merupakan "tangible object". Pada umumnya pengadilan di hampir semua negara menerapkan prinsip hukum tentang pencurian dan penggelapan dalam menangani kasus seperti itu. Namun putusan Chambre Criminelle de la Cour de Cassation tanggal 8 Januari 1979 telah memutus bahwa "membuat foto-kopi sebuah dokumen merupakan "pencurian" oleh karena sipelaku untuk beberapa waktu telah menguasai "data-carrier" yang berisi dokumen tersebut".[25] Putusan ini banyak ditentang oleh sarjana hukum Perancis.

Putusan yang serupa dijatuhkan oleh Hof Arnhem tanggal 27 Oktober 1983 dalam kasus yang terkenal dengan "disc-pack arrest", yang memutus bahwa "membuat foto-kopi satu data komputer oleh seorang pegawai tanpa ijin pemilik merupakan suatu penggelapan" (melanggar pasal 321 Wetboek van Strafrecht).[26] Putusan inipun telah ditentang oleh banyak sarjana hukum Belanda, yang pada pokoknya tidak menyetujui perluasan "goed" kepada "data komputer".

Dalam perkara Oxford v. Moss, Pengadilan Tinggi di Inggris pada tahun 1979 telah memutus bahwa perbuatan seorang mahasiswa 'melihat soal ujian' tanpa mengambil kertas ujian tidak termasuk pencurian. Demikian pula dalam kasus R. v. Lloyd, perbuatan "meminjam film" yang kemudian dibuat kopinya, oleh Pengadilan Tinggi dinyatakan tidak termasuk pencurian, oleh karena tidak ada barang yang hilang.[27]

Dalam satu kasus terkenal yang terjadi di negara bagian

---

[25] *Ibid*, hal.53.

[26] N.J. 1984, 80 tanggal 27 Oktober 1983.;

[27] (1978) 68 Cr App R 183; Lihat Marett, Paul, Information Law and Practicve, Gower, 1991, hal. 4-5.

California, yaitu Ward v Superior Court, [28] Hakim Superior Court di California membebaskan terdakwa dari dakwaan melakukan pencurian dengan pertimbangan bahwa "electronic impulses" (data komputer) bukan merupakan "article" (barang) sebagaimana dimaksud dalam ketentuan undang-undang pidana yang berlaku mengenai pencurian. Putusan negara bagian ini sering diikuti oleh pengadilan negara bagian lainnya.

Dalam salah satu perkara yang hampir sama yang terjadi di negara bagian Colorado, terdakwa oleh Pengadilan Colorado telah dibebaskan dari dakwaan melakukan pencurian data dengan pertimbangan bahwa "karena tidak ada barang yang diambil maka terdakwa harus dibebaskan". ("since nothing tangible had been taken, the charge was dismissed").[29]

Dalam kasus U.S. v. Seidlitz, pengadilan federal memutus bahwa pencurian "property" yang dalam perdagangan antar negara bagian tidak meliputi perbuatan mengambil 'informasi' yang disimpan dalam data komputer.[30] Dalam kasus ini terdakwa dibebaskan oleh Pengadilan Federal dengan alasan "data komputer" tidak sama dengan barang (property), dan dalam kasus ini tidak ada "property" yang dipindahkan. Dalam pertimbangannya disebutkan

> *"The offence theft of goods in interstate commerce was held not to extend to the copying of computer software by the use of a remote terminal and the transmission of electronic signals from on state to another, since no transportation of property had occurred".*[31]

6. Penyalahgunaan "cash-card" atau kartu debit

Dalam hal yang diambil adalah uang dari mesin pembayar otomatis seperti "cash-dispenser" atau "automatic teller machine" (ATM) melebihi dana yang ada atau dananya sudah tidak ada, persoalan hukum timbul tentang apakah penyerahan uang oleh Automatic Teller Machine (ATM) tanpa menipu atau memanipulasi data komputer, yaitu dengan menggunakan "password" atau "PIN" yang syah termasuk pencurian ataukah merupakan perkara perdata belaka.

Tampaknya pengadilanpun belum sependapat mengenai ini. Untuk mengatasi persoalan tersebut pengadilan-pengadilan di beberapa negara melakukan interpretasi luas (broad interpretation) yaitu menerapkan pasal pencurian atau penggelapan untuk perbuatan penyalahgunaan "cash-card" seperti itu, seperti yang dilakukan di

---

[28] Ward v Superior Court (1972).
[29] Putusan Pengadilan Colorado, 197 Colo 260, 591 P2d 1036 (1979).
[30] U.S. v. Seidlitz, 1978.
[31] Untuk mencangkup hal ini lihat amandemen Penal Code tahun 1991 di dalam Bab III.

Canada, Belanda, Swiss, Inggris, Australia dan sebagian besar negara bagian Amerika Serikat.

Beberapa negara lainnya seperti Jepang, Belgia, Jerman Barat (dulu), Yunani, dan Luxemburg berpendapat bahwa perbuatan tersebut tidak termasuk pencurian oleh karena uang yang disimpan disitu (deposit money) tidak dapat dianggap sebagai "tangible" tetapi sebagai hak untuk menuntut (claim), oleh karena itu lebih bersifat perdata.[32] Sejauh ini belum ada kasus pidana yang diproses di pengadilan Indonesia sehubungan dengan hal tersebut.

Dalam hal kartu debit atau cash-card diperoleh secara melawan hukum, misalnya dengan mencuri untuk mengambil sejumlah uang, pada umumnya para sarjana sependapat bahwa ketentuan tradisionil mengenai pencurian atau penipuan dapat diterapkan. Demikianlah putusan yang dijatuhkan oleh hakim Austria, Belgia, Perancis, Jerman, Jepang dan Swiss diperlakukan. Demikian pula pendapat umum dan praktek di Portugis dan Itali dan Indonesia.

Dalam hal pemilik kartu mengambil uang dari "cash dispenser" atau "auto teller machine" (ATM) melebihi dari apa yang disimpannya, di beberapa negara seperti Belgia dan Australia, pasal pencurian tetap diperlakukan. Hal ini mungkin terjadi jika system ATM sedang "off-line" (sibuk).

Dalam kasus Kennison v. Daire terdakwa oleh Supreme Court of South Australia telah dinyatakan bersalah melakukan pencurian oleh karena walaupun ia telah menutup rekeningnya di Saving Bank of South Australia, ia telah mengambil sejumlah uang dalam salah satu ATM yang sedang "off-line". Dalam tingkat banding putusan itu dikuatkan oleh High Court of Australia.[33]

Dalam kasus R. v. Evenett (1987) terdakwa telah berhasil mengambil uang melalui ATM yang sedang 'off-line' sebesar $ 778.97 padahal dana pada bank tersebut (National Australia Bank) tinggal $181.03. Court of Criminal Appeal membatalkan putusan pengadilan negara bagian Queensland yang membebaskan terdakwa, dan memutus bahwa perbuatan terdakwa mengambil uang melebihi dana yang ada sebagai pencurian.[34]

Namun Cour de Cassation di Perancis dalam putusannya tanggal 24 Nopember 1983 telah memutus bahwa perbuatan tersebut bukan merupakan pencurian melainkan pelanggaran kewajiban yang telah disepakati yang diatur dalam hukum perdata ("breach of contractual obligation"), dengan demikian tidak termasuk pengertian yang diatur

---

[32] Sieber (1986), hal. 39-40.

[33] Kennison v. Daire (1985)

[34] Lihat Brown (1990), "Computer-Related Crime in Australia: ATM Abuse." dalam buku Gordon Hughes, Essays on Computer Law (1990), hal.224-247.

dalam pasal 379 Penal Code (mengenai pencurian) atau pasal lainnya dari Penal Code[35].

7. Upaya Penyempurnaan

Untuk bisa memperluas pengertian pencurian dan penggelapan agar meliputi data komputer beberapa negara telah menyempurnakan pasal-pasal mengenai kedua tindak pidana itu, misalnya dengan memperluas pengertian "property", article" atau "thing of value" sehingga meliputi 'data komputer".[36]

Beberapa negara bagian telah merubah undang-undang pidana mengenai "property" sehingga termasuk juga:

> *"electronic impulses, electronically processed or produced data or information, commercial instruments, computer software or computer programs, in either machine or human readable form, computer services, any other tangible or intangible item of value relating to a computer system or computer network, and any copies thereof."* [37]

Sedangkan beberapa negara lainnya dengan membuat peraturan tersendiri atau menyempurnakan ketentuan khusus mengenai "membocorkan rahasia dagang dan rahasia industri" sehingga berlaku juga bagi orang luar, menyempurnakan ketentuan mengenai "persaingan curang" (unfair competition), atau menyempurnakan undang-undang mengenai hak-cipta.

India pada tahun 1998 menyempurnakan Penal Code 1860 melalui Electronic Commercial Act 1998 agar dapat mencangkup segala jenis kejahatan komputer yang mungkin belum terjangkau oleh Penal Code tersebut.

Namun para pakar negara-negara Europa tampaknya tidak setuju untuk memperluas pengertian barang seperti tercantum dalam pasal-pasal mengenai pencurian dan penggelapan terhadap "data komputer", oleh karena berbeda dalam dua hal, yaitu: pertama, pencurian terhadap "data komputer" tidak akan menimbulkan hilangnya barang tersebut dari pemiliknya, dan kedua, bahwa "informasi" yang terkandung dalam data komputer walaupun merupakan milik seseorang, namun berdasarkan "right for free information flow" (dilindungi oleh European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950) haruslah disebar-luaskan. [38]

---

[35] Sieber, ibid.
[36] Lihat Bab III contoh amendemen Penal Code dibeberapa negara.
[37] Lihat misalnya Penal Code dari Negara Bagian Montana (s.45.2.101(54)(k)(1981).
[38] Sieber (1990), hal. 123-124.

Oleh karena itu negara-negara tersebut melindungi data komputer melalui ketentuan khusus, antara lain yang melarang perbuatan "mentransfer, memasuki, merubah, merusak atau menghilangkan data komputer secara melawan hokum" dengan tujuan mengambil keuntungan, atau melalui pasal penipuan (computer fraud), yaitu 'setiap perbuatan memanipulasi data komputer yang dilakukan secara melawan untuk keuntungan sipelaku atau orang lain'.

Hoge Raad dalam "electricity arrest" yang diputus tahun 1921 dengan tegas menyatakan bahwa "property concept" harus diterapkan secara sempit, sehingga tidak meliputi "intellectual products". Demikian pula pendapat dari Komisi Franken dalan Rancangan Undang-Undang mengenai Kejahatan Komputer.[39]

Sepanjang mengenai gangguan atau perusakan terhadap sarana atau media dan data komputer Komisi tersebut mengusulkan penyempurnaan dari ketentuan pidana mengenai perusakan dan sabotase.[40] Untuk penyalahgunaan "cheque-card" atau "cash-card" Komisi mengusulkan peraturan tersendiri sebagai Usulan 18, yang diletakkan dekat pasal mengenai pemalsuan.Usulan 18: Peraturan baru ditaruh dekat pasal 225 Sr. dan 226 Sr. (pemalsuan) berhubung dengan penggunaan chechue card yang berbeda dengan dokumen.[41]

B. PEMALSUAN

Ketentuan pidana mengenai pemalsuan (forgery) yang pada umumnya berlaku di sebagian besar undang-undang pidana mensyaratkan dapat dilihat dan dibacanya ("visual readibility") dokumen yang dipalsukan itu. Yang dimaksudkan disini ialah bahwa pemalsuan itu dibuat pada suatu dokumen yang dapat dilihat dengan mata telanjang misalnya pada kertas, oleh karenanya tidak meliputi dokumen yang dipalsukan melalui data komputer (electronically stored data).[42]

---

[39] Report of the Dutch Committe, alinia 54-55.

[40] Lihat Bab IV Butir 2.3.

[41] Bunyi usulan 18:

Barang siapa yang dengan sengaja mengeluarkan suatu cheque card palsu atau dipalsukan, atau yang merubah, menambah atau menghapus data yang disimpan didalam atau diatas sebuah cheque card, dengan maksud untuk dengan melawan hukum menguntungkan dirinya sendiri atau orang lain, dipidana dengan pidana penjara selama-lamanya 6 tahun dan denda dalam katagori kelima, atau salah satu dari kedua pidana tersebut.

Barang siapa yang dengan sengaja menggunakan sebuah cheque card yang dihasilkan dari perbuatan tersebut dalam alinea 1 , dihukum dengan pidana yang sama.

[42] Lihat misalya pasal-pasal: 223 Penal Code Austria, pasal 193 Penal Code Belgia, pasal 145 Penal Code Perancis, pasal-pasal 193-214 Penal Code Luxemburg, dan pasal-pasal 251-7, dan 317 Penal Code Swiss.

Pasal tersebut pada dasarnya sama dengan pasal mengenai "pemalsuan" yang diatur dalam Kitab Undang-Undang Hukum Pidana.

Pasal 263 ayat 1 KUH Pidana mengatur:

> "Barangsiapa membikin surat palsu atau memalsukan surat, yang dapat menerbitkan sesuatu hak, sesuatu perutangan atau yang dapat membebaskan daripada utang atau yang dapat menjadi bukti tentang sesuatu hal, dengan maksud untuk memakai atau menyuruh orang lain memakai surat itu seolah-olah surat itu asli dan tidak dipalsukan, jikalau pemakaian surat itu dapat mendatangkan kerugian, maka karena memalsukan surat, dipidana dengan penjara selama-lamanya enam tahun".

Dilihat dari sejarah pembentukan pasal tersebut yang dimaksud "surat" adalah "kertas" diatas mana diberi suatu tulisan yang merupakan ekspresi dari pikiran manusia, yang menurut ketentuan yang berlaku merupakan suatu berita acara, surat keterangan yang dibuat sesuai dengan perundang-undangan, surat keterangan ahli, atau surat tertentu lain.

Dalam hukum acara pidana hal-hal yang berkenaan dengan surat tercantum dalam pasal 84 (1) c KUHAP mengenai alat-alat bukti. Menurut pasal 187 Kitab Undang-Undang Hukum Acara Pidana yang dimaksud dengan surat ialah:

Surat sebagaimana tersebut pada Pasa 184 ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah:

a. berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat di hadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu;
b. surat yang dibuat menurut ketentuan peraturan perundangan-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabanya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan;
c. surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi dari padanya;
d. surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian lain.

Ibid.

Menurut pendapat beberapa pakar hukum pidana tulisan itu diartikan sebagai setiap benda yang memuat tanda-tanda baca yang dapat dimengerti yang bertujuan untuk mengungkapkan isi pikiran.

Penyalahgunaan kartu kredit

Di beberapa negara telah diundangkan ketentuan pidana khusus mengenai penyalahgunaan "credit card" (credit-card fraud) yang meliputi pemalsuan kartu kredit, yang pada umumnya penerapannya tidak bisa diperluas kepada perbuatan penyalahgunaan "cash card" untuk mengambil uang dari "cash-dispenser" atau "automatic teller machine". Pasal "tradisionil" 301.1 dari Criminal Code Canada menyatakan sebagai suatu kejahatan perbuatan:

1. mencuri atau memalsu kartu kredit;
2. memiliki, menggunakan, atau melakukan transaksi apapun dengan menggunakan kartu kredit yang diperoleh secara melawan hukum, atau
3. menggunakan sebuah kartu kredit yang diketahuinya telah dicabut atau dibatalkan.

Untuk memperluas pengertian tentang "computer fraud" maka pada tahun 1985 diundangkan Criminal Law Amendment Act 1985 dimana perbuatan yang dilarang diperluas keperbuatan manipulasi kepada semua jenis "automated-teller machine" dan "jasa bank", dan pengertian "instrument" diperluas sehingga meliputi 'data' yaitu yang berupa "any material, on which is recorded or marked anything that is capable of being read or understood by a person, computer systems or other device". Maka perbuatan memanipulasi yang dilakukan melalui bahan yang bisa direkam secara elektronis seperti data komputer yang bisa dibaca termasuk kejahatan penipuan.

Komisi Franken berpendapat perlu diatur ketentuan baru mengenai "cash-card" yang sudah lazim dipergunakan sebagai pengganti uang kontan. Penyalahgunaan dapat dilakukan dengan perbagai cara, misalnya dengan memalsukan data, merubah data, atau sipelaku menggunakan cash-card yang dicuri dari orang lain. Dipersoalkan apakah perubahan data pada cash-card dapat disamakan dengan pemalsuan dokumen sebagaimana diatur dalam pasal 225 Sr. Namun untuk menjaga kemungkinan dikembangkannya berbagai macam cash card yang dibuat secara elektronis, Komisi mengusulkan peraturan baru sebagai berikut:[43]

[43] Report of the Dutch Committee on Computer Crime (1988), hal.69-70.

Usulan 18: Peraturan baru ditaruh dekat pasal 225 Sr dan 226 Sr (Pemalsuan) berhubung dengan penggunaan cheque card yang berbeda dengan dokumen.

Barang siapa yang dengan sengaja mengeluarkan suatu cheque card palsu atau dipalsukan, atau yang merubah, menambah atau menghapus data yang disimpan didalam atau diatas sebuah cheque card, dengan maksud untuk dengan melawan hukum menguntungkan dirinya sendiri atau orang lain, dipidana dengan pidana penjara selama-lamanya 6 tahun dan denda dalam kategori kelima, atau salah satu dari kedua pidana tersebut.
Barang siapa yang dengan sengaja menggunakan sebuah cheque card yang dihasilkan dari perbuatan tersebut dalam alinea 1, dihukum dengan pidana yang sama.
Ancaman atas pelanggaran tindak pidana ini adalah 6 tahun, jauh lebih berat dari penipuan, dengan pertimbangan oleh karena "cash card" adalah pengganti alat pembayaran yang syah, seperti uang, yang perlu dijamin pengamanannya.

C. PENIPUAN

Berdasarkan penelitian jenis kejahatan komputer yang banyak dilakukan ialah penipuan yang dilakukan terhadap perusahaan yang berkecimpung dalam kegiatan keuangan seperti bank, asuransi, dan perusahaan besar lainnya yang banyak menggunakan komputer. Para pelakunya selain perorangan ("occupational crime") juga perusahaan itu sendiri ("corporate crime") yang dengan memanipulasi data keuangan diharapkan untuk memperoleh keuntungan keuangan, misalnya untuk menghindari pembayaran pajak dan lainnya. Cara melakukan penipuan yaitu dengan memanipulasi atau merubah data komputer dengan informasi palsu agar memperoleh keuntungan baik bagi sipelaku atau perusahaan itu sendiri maupun untuk orang lain.

Permasalahan hukum

Salah satu syarat penting dalam penipuan ialah "harus ada orang yang ditipu", tidak cukup menipu mesin saja. Dalam kasus penipuan yang dilakukan dengan memanipulasi data komputer pengadilan mengalami kesulitan untuk menerapkan pasal ini karena adanya persyaratan tersebut.

Pasal 378 Kitab Undang-Undang Hukum Pidana mengatur:

> "Barangsiapa dengan maksud untuk menguntungkan dirinya sendiri atau orang lain secara melawan hukum, dengan mempergunakan sebuah nama palsu atau suatu sifat palsu, dengan mempergunakan tipu-muslihat ataupun dengan mempergunakan susunan kata-kata bohong, menggerakkan seseorang untuk menyerahkan sesuatu benda, untuk mengadakan perjanjian hutang ataupun untuk meniadakan piutang, karena salah telah melakukan penipuan, dihukum dengan hukuman penjara selama-lamanya empat tahun".

Salah satu unsur yang harus dipenuhi agar sipelaku dapat dipidana berdasarkan pasal 378 KUHPidana tersebut ialah adanya perbuatan membujuk orang. Unsur "a person be deceived" tersebut tercantum pula dalam undang-undang hukum pidana yang berlaku di negara lain.[44] Oleh karena salah satu syarat adalah harus ada orang yang ditipu maka untuk dapat diterapkannya pasal ini dalam kejahatan komputer haruslah diteliti terlebih dahulu apakah ada orang lain, misalnya petugas komputer data yang ditipu.

Oleh pengadilan beberapa negara seringkali ketentuan mengenai penipuan ini diinterpretasikan secara luas (dilakukan "manoevres fraudleuses") yaitu dengan menjadikan orang yang bertanggung jawab dalam sistim komputer sebagai orang yang ditipu, seperti yang dilakukan oleh hakim-hakim di Belgia dan Perancis. Namun hakim beberapa negara lainnya seperti Inggris enggan memperluas penafsiran pasal mengenai penipuan, karena mereka berpendapat hal tersebut merupakan kewenangan pembuat undang-undang.

Komisi Franken tidak mengusulkan penyempurnaan pasal mengenai penipuan (pasal 326 Sr) oleh karena telah ada yurispudensi H.R. yang memperluas pengertian tentang orang. Dalam beberapa perkara penipuan telah diputus bahwa "Pemerintah Belanda juga dapat dibujuk" untuk melakukan perbuatan tertentu. Tidak menjadi masalah bagaimana caranya penipuan dilakukan, yang penting adalah perbuatan daya tipu yang dibuat sedemikian rupa sehingga korban mempercayainya bahwa itu benar. [45]

Dengan demikian sipemilik dari suatu bank dapat merupakan korban dari penipuan yang dilakukan dengan memanipulasi data komputer.

Dengan Amendment Act tanggal 6 Juni 1985 Denmark telah menyempurnakan pasal 279 Penal Code dengan penambahan ayat baru yang berbunyi:

---

[44] Lihat misalnya pasal-pasal: 146 Penal Code Austria, 279 Penal Code Denmark, 263 Penal Code Jerman Barat (dulu), 386 Penal Code Yunani, 640 Penal Code Australia, 246 Penal Code Jepang, 496 Penal Code Luxemburg, bab 9 pasal 1 Penal Code Swedia, atau pasal 148 Penal Code Swiss. Sieber (1986), hal.3-11.

[45] Report of the Dutch Committee, hal.68-69.

Section 279a.

> Barang siapa yang dengan maksud untuk memperoleh keuntungan bagi dirinya atau orang lain secara melawan hukum dengan cara-cara yang melawan hukum merubah, menambah atau menghapus data yang berisi program untuk pemrosesan atau dengan cara lainnya yang melawan hukum berusaha untuk mempengaruhi hasil dari proses data tersebut, bersalah karena melakukan penipuan dengan komputer (computer fraud).

D. SABOTASE DAN PERUSAKAN

Komputer, data komputer dan alat lainnya dapat dirusak dengan pelbagai cara. Para pelaku sering melakukan perusakan dengan cara membakar, meledakkan, atau dengan memasukkan sesuatu metal seperti kunci mobil atau obeng kedalam komputer. Kasus yang terjadi menunjukkan alasan perusakan bisa bermacam-macam, diantaranya oleh karena alasan politik atau persaingan antara perusahaan.

Pada awal tahun 1970 sejumlah mahasiswa telah merusak beberapa pusat komputer di Amerika Serikat dan beberapa negara Eropa karena alasan politik. Pada waktu yang hampir bersamaan lebih dari 30 serangan dilakukan oleh beberapa kelompok pada beberapa pusat komputer di Itali dan Perancis. Perbuatan tersebut telah mengakibatkan kerugian yang besar kepada negara dan perusahaan yang bersangkutan.[46]

Beberapa situs di Internet hampir setiap hari memberitakan terjadinya hacking yang menyebabkan terkontaminasinya system komputer dengan virus yang mengakibatkan tidak berfungsinya komputer itu. Sejumlah besar komputer di Jepang belum lama ini diserang virus yang dilakukan oleh sejumlah hackers, sehingga merusak data komputer.

Pada umumnya undang-undang pidana tradisionil mengenai perusakan atau penghancuran, "damage, destruction atau mischief") dapat diterapkan apabila yang dirusak berupa "physical object", misalnya komputer atau alat-alat lainnya.

> Pasal 406 ayat (1) Kitab Undang-Undang Hukum Pidana mengatur: Barang siapa dengan sengaja dan secara melawan hukum, menghancurkan merusakkan, membuat hingga tidak dapat dipakai lagi atau menghilangkan sesuatu benda yang seluruhnya atau sebagian adalah kepunyaan orang lain, dihukum dengan hukuman penjara selama-lamanya dua tahun dan delapan bulan atau dengan hukuman denda setinggi-tingginya empat ribu lima ratus rupiah.

---

[46] Schjolberg, hal.18.

Namun apabila yang dirusak adalah data komputer, tanpa merusak disket atau carriernya sendiri, maka permasalahan hukum timbul, seperti yang akan dibicarakan di bawah ini.

Perusakan data secara otomatis

Data yang disimpan dapat dirubah, dirusak atau dibuat tidak berfungsi lagi dengan kekerasan fisik ataupun secara elektronis. Pengrusakan yang dilakukan secara elektronis biasanya baru diketahui ketika komputer dihidupkan. Dengan tidak tampaknya data yang dimaksud dalam layar monitor atau tidak dapat dicetak, tentu ada sesuatu kesalahan atau kerusakan pada data komputer.

Salah satu cara pengrusakan data yang dilakukan secara elektronis disebut "logic bomb". Suatu "logic bomb" adalah suatu perintah yang diprogramkan kedalam data komputer yang berisi perintah untuk mengacaukan program komputer atau untuk menjadikan tidak berfungsinya lagi program komputer setelah waktu tertentu atau kalau ada petugas yang memeriksa sesuatu dalam program komputer tersebut. Cara ini disebut juga "trojan horse" yaitu suatu perintah yang diberikan secara diam-diam untuk merusak program komputer.

Dalam satu kasus yang terjadi sekitar tahun 1970 seorang programmer yang karena tidak senang telah diberhentikan dari suatu perusahaan telah menggunakan "trojan horse" pada program komputer perusahaan pada hari-hari terahir ia bekerja dengan memerintahkan agar setelah dua tahun program komputer tidak akan berfungsi lagi. Sistim komputer berjalan dengan wajar selama dua tahun, dan kemudian semua data yang ada menjadi hilang karena terhapus secara otomatis. Kasus seperti ini sering terjadi di Amerika Serikat dan beberapa negara Eropah.

Permasalahan hukum

Perusakan data yang merupakan "intangible" dibeberapa negara sering menimbulkan persoalan hukum. Ketentuan pidana yang berlaku di sebagian besar negara mensyaratkan barang yang dirusak adalah barang yang bersifat "tangible" ("physical damage"). Oleh karena data digital goods merupakan "intangible" maka ketentuan pidana mengenai perusakan fisik tidak berlaku bagi perusakan data ("logical damage").

Namun di beberapa negara lainnya seperti Austria, Canada, Denmark, Jerman Barat (dulu), Yunani, Itali, Norwegia, dan Inggris, perusakan yang dilakukan dengan sengaja terhadap informasi yang tersimpan dalam pita atau disket dianggap sebagai perusakan (vandalism atau malicious mischief)

terhadap barang ("property").[47] Pendapat ini didasarkan kepada pertimbangan bahwa sipelaku dengan perbuatannya itu telah merusak atau mengganggu berfungsinya pita atau disket yang berisi data.

Di negara dimana telah dikeluarkan ketentuan pidana yang melarang perusakan baik yang bersifat "tangible" maupun "intangible", misalnya seperti diatur dalam pasal 387 Canada Criminal code, atau Chapter 33 Computer Crimes Federal Penal Code, Indian Electronoc Commercial Act 1991, perbuatan ini tidak menimbulkan masalah hukum lagi. Menurut pasal tersebut termasuk "mischief" adalah "damage or destruction of tangible property and the obstruction, interruption, or interference with the lawful use of tangible property..."(Termasuk tangible ialah perusakan atau intervensi atas penggunaan tangible property). Dengan demikian keruskan pada data komputer termasuk perbuatan "mischief".

Dalam kasus R. v. Turner (1984), Ontario High Court of Justice telah memutus terdakwa bersalah melakukan tindak pidana perusakan oleh karena walaupun tidak ada kerusakan fisik komputer namun dengan dirubahnya data yang tersimpan dalam pita komputer maka telah terjadi gangguan terhadap berfungsinya sistim komputer tersebut.[48]

Ketentuan pidana mengenai "mischief" atau "destruction" di beberapa negara seperti Belgia, Finlandia, negara Bagian New York dan Tasmania, membatasi perusakan hanya pada "physical medium" saja, sehingga merusak atau merubah data tanpa merusak 'physical medium' tidaklah termasuk tindak pidana "destruction" (lihat misalnya pasal-pasal 528 dan 559, Penal Code Belgia ; dan pasal 273, Criminal Code Tasmania. [49]

Persoalan hukum lainnya yang belum jelas pemecahannya ialah dalam hal sipemilik komputer tidak dapat menjalankan program komputer (tidak dapat memasuki sistim komputer) oleh karena perbuatan sipelaku. Dalam kasus ini belum diketahui apakah ada perubahan atau kerusakan yang ditimbulkan baik terhadap "physical medium" atau "logical medium" oleh karena sipemilik atau yang berhak mengoperasikan komputer tidak dapat mencapai program komputer.

Untuk mengisi kekurangan ini beberapa negara telah menyempurnakan ketentuan pidana mengenai "perusakan", "destruction", "damage" atau "mischief" ini. Dengan Penal Code Amendement Act tahun 1985 Austria telah menyempurnakan pasal 126 dengan mengatur ketentuan

---

[47] Llihat pasal 125, Penal Code Austria; pasal 291, Penal Code Denmark; pasal 303, Penal Code Jerman Barat; pasal 381, Penal Code Yunani; pasal-pasal 420 dan 635, Penal Code Itali; pasal-pasal 420 dan 635, Penal Code Italia; dan pasal 78 dari Criminal Justice Act 1980 Scotlandia atau Criminal Damage Act 1971 Inggris. Lihat pula Sieber (1986), hal. 78.

[48] R. v Turner (1984)3 All ER 565.

[49] Sieber (1990), hal.78-79.

baru seperti yang tercantum dalam pasal 126a tentang damage to Stored Data yang berbunyi:

> *Barangsiapa yang menyembunyikan, merubah, menghapus ataupun menyebabkan tidak berfungsinya suatu data elektronis, magnetis atau data yang disimpan yang secara langsung tidak dapat dilihat atau dibaca, tanpa hak menghilangkan data, karena bersalah dipidana dengan pidana penjara selama-lamanya enam bulan atau denda tidak melebihi 360 pendapatan harian (daily rates).*
>
> *Kalau kerugian yang disebabkan oleh tindak pidana melebihi l0.000 Schillings, pidana yang dijatuhkan ialah pidana penjara selama-lamanya dua tahun atau denda tidak melebihi 360 pendapatan harian.*
>
> *Apabila kerugian yang disebabkan tindak pidana melebihi 200.000 Schillings, pidana yang dijatuhkan ialah pidana antara 6 bulan sampai lima tahun.* [50]

Komisi Franken mengusulkan peraturan baru dan penambahan pada pasal-pasal 161 bis dan 351 Sr agar pasal-pasal ini dapat memidana perbuatan perusakan atas data atau sistim telekomunikasi, sebagai Usulan 1,2 dan 3 dalam rancangan undang-undang tentang kejahatan komputer[51]. Usulan 1: Merupakan peraturan baru - Analogi pasal 161 bis Sr. (Padannya pasal 191 bis KUHP). Kata-kata yang digaris bawahi merupakan tambahan baru.

Barang siapa dengan sengaja menghancurkan, merusak atau menjadikan tidak dapat dipakai lagi, menyebabkan terganggu jalannya atau bekerjanya pekerjaan atau menghalangi tindakan pengamanan suatu alat yang diotomatisasikan untuk penyimpanan atau pengolahan data atau untuk telekomunkasi, diancam:

dengan pidana penjara paling lama enam bulan atau denda menurut kategori ke lima, jika dengan itu menimbulkan, menghalangi atau mempersulit penyimpanan atau pengolahan data atau telekomunikasi untuk kepentingan umum;

dengan pidana penjara paling lama enam tahun atau denda dengan kategori kelima, jika dengan itu menimbulkan bahaya secara umum terhadap barang atau pelaksanaan tugas

---

[50] Ibid, hal.200.

[51] .Report of the Dutch Committee, hal.34-37.

dengan pidana penjara paling lama sembilan tahun atau denda menurut kategori kelima, jika perbuatan itu menimbulkan bahaya yang dapat diduga terhadap nyawa orang lain;

dengan pidana penjara paling lama lima belas tahun atau denda menurut kategori kelima, jika perbuatan itu menimbulkan bahaya yang dapat diduga terhadap nyawa orang lain dan mengakibatkan matinya seseorang.

Usulan 2 : Peraturan baru untuk melindungi alat yang dikomputerisasikan untuk penyimpanan data atau untuk telekomunikasi.

Barangsiapa karena kelalaiannya menyebabkan hancur, rusak atau menjadikan tidak dapat dipakai lagi, atau menyebabkan gangguan pelaksanaan atau berfungsinya alat yang diotomatisasikan untuk menyimpan atau mengolah data atau untuk telekomunikasi, atau untuk mengganggu tindakan pengamanan yang disiapkan pada alat tersebut diancam pidana:

a. dengan pidana penjara atau kurungan paling lama tiga bulan atau denda menurut kategori keempat jika dengan itu menimbulkan menghalangi atau mempersulit penyimpanan atau pengolahan data atau telekomunikasi" untuk kepentingan umum atau menimbulkan bahaya secara umum terhadap barang pelaksanaan tugas;

b. dengan pidana penjara atau kurungan paling lama enam bulan atau denda menurut kategori keempat, jika dengan itu menimbulkan bahaya bagi nyawa orang lain;

c. dengan pidana penjara atau kurungan paling lama satu tahun atau denda menurut kategori keempat, jika menyebabkan matinya orang lain.

Usulan 3: penyempurnaan pasal 351 WvS (sama dengan pasal 408 KUHP). Kata-kata baru WvS atau KUHP yang diberi tanda garis merupakan tambahan baru.

Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan atau membuat tidak dapat dipakai lagi bangunan-bangunan kereta api atau listrik, peralatan yang diotomatisasikan untuk menyimpan atau mengolah data atau untuk telekomunikasi, pengawas air atau instalasi pengeringan, pipa gas, air, atau kotoran, yang dipergunakan untuk kepentingan umum, diancam dengan pidana penjara paling lama tiga tahun atau denda menurut kategori keempat.

Usulan 5 : Peraturan baru, sebagai alinia 2 pasal 354 Sr. agar pidana yang diancamkan untuk perbuatan yang menimbulkan kerugian besar diperberat. (Padanya pasal 412 KUHPidana.)

Barangsiapa melakukan perbuatan pidana seperti dimaksud dalam titel ini yang menimbulkan kerugian berat diancam pidana dengan pidana penjara paling lama empat tahun atau denda menurut kategori kelima

E. TANPA HAK MENGUNAKAN KOMPUTER DAN PENCURIAN WAKTU DAN FASILITAS KOMPUTER (*The Unauhorized Use of Computer, and Theft of Computer time and Facilities*).

Beberapa pakar hukum pidana memasukkan kedalam kejahatan tanpa hak menggunakan komputer juga perbuatan penyalahgunaan waktu dan fasilitas komputer ('theft of computer time and facilities').

Kasus-kasus yang pernah terjadi di beberapa negara menunjukkan bahwa perbuatan ini kadang-kadang tidak menimbulkan kerugian yang berarti kepada pemilik komputer, akan tetapi sering pula menimbulkan kerugian yang besar bagi pemiliknya. Dari kasus-kasus itu seringkali sipelaku yang bekerja di suatu perusahaan telah menggunakan komputer itu untuk keperluan pribadinya untuk beberapa lamanya tanpa diketahui majikannya sehingga menimbulkan kerugian ratusan ribu dolar bagi perusahaan itu.

Dalam satu kasus besar yang terjadi di Amerika Serikat, dua orang direktur dari suatu lembaga teknik telah menggunakan komputer lembaga itu untuk keperluan perusahaan pribadinya yang berkecimpung dalam usaha majalah, usaha dagang dan usaha jual beli suku cadang kapal terbang.[52]

Nilai kerugian sehubungan dengan waktu yang telah dipergunakan diperhitungkan lebih dari $200,000, belum termasuk gaji yang dibayarkan kepada kedua direktur itu sebesar $40,000. Perbuatan mereka dapat diketahui oleh karena data komputer yang terpakai dalam komputer perusahaan itu semakin lama semakin banyak padahal kegiatan perusahaan itu tidak banyak berubah.

Di beberapa negara perbuatan tersebut dapat dipidana berdasarkan pasal pencurian, namun pengadilan beberapa negara lainnya enggan memperluas pengertian tanpa hak menggunakan komputer kepada "theft of computer time" or "services".

---

[52] Schjolberg, hal.25-26.

Permasalahan hukum

Di negara-negara Eropa seperti Norwegia dan Swiss ketentuan pidana yang berlaku hanya berlaku terhadap perbuatan yang menimbulkan kerugian atau ketidaknyamanan kepada sipemilik komputer. Ketentuan pidana di negara-negara seperti Austria, Jerman Barat (dulu), Jepang, dan Inggris tidak menghukum perbuatan memasuki sistim komputer orang lain tanpa bermaksud jahat.

Menurut ketentuan yang berlaku di negara tersebut perbuatan untuk senang-senang "furtum usus" hanya dihukum untuk perbuatan iseng tertentu saja seperti "joyriding" yang menggunakan kendaraan bermotor atau sepeda, misalnya pasal 248b Jerman Barat, dan tidak untuk joycomputing

Beberapa negara seperti Peranccis bahkan tidak mengatur perbuatan "furtum usus" tersebut, oleh karenanya pengadilan-pengadilan menggunakan ketentuan pencurian untuk "joyriding". Perbuatan ini dapat dibandingkan dengan memasuki pekarangan atau tanah orang lain tanpa menimbulkan kerusakan apapun (trespass).

Perbuatan tersebut tidak dipermasalahkan pula di Belgia, Denmark dan Finlandia, oleh karena telah ada ketentuan yang memidana perbuatan yang tanpa hak menggunakan barang orang lain.[53] Dalam kasus seperti ini perbuatan menggunakan data komputer tidak terlepas dari perbuatan menggunakan komputer yang termasuk pengertian barang milik orang lain[54].

Kaspersen tidak sependapat apabila pasal pidana mengenai pencurian yang diterapkan pada kasus "joyriding" (furtum usus) diterapkan pula pada perbuatan seperti ini[55] Pengadilan-pengadilan di Amerika Serikat tampaknya belum sependapat mengenai apakah perbuatan "tanpa hak menggunakan komputer" dapat diperlakukan juga terhadap "pencurian waktu komputer". Namun dengan diundangkannya ketentuan baru tentang "computer crimes" dalam Federal Penal Code, dimana pengertian "property" diperluas sehingga menjangkau penggunaan jasa komputer (the use of computer service) maka keragu-raguan tersebut dapat dihilangkan.[56]

Dalam satu putusan pengadilan di negara bagian New York dikatakan bahwa "theft of services does not cover the unauthorized use of computers". (Pencurian waktu komputer tidak termasuk perbuatan tanpa hak menggunakan komputer). Namun pengadilan federal dalam kasus yang serupa telah memutus sebaliknya [57]

---

[53] Misalnya pasal 461 Penal Code Belgia, atau pasal 293 Penal Code Denmark.
[54] Sieber (1986), ibid.
[55] Kaspersen (1990), hal 344-345.
[56] Lihat Chapter 33, Computer Crimes: Definitions.
[57] Lihat kasus US v. Sampson.

Lund v. Commonwealth of Virginia (1977)

Dalam kasus yang terjadi di negara bagian Virginia seorang mahasiswa tingkat akhir menggunakan komputer sekolah untuk mengetik disertasi. Perbuatannya itu diketahui dan ia dituntut melakukan pencurian. Ia tidak mengetahui bahwa untuk itu perlu ijin, dan pembimbingnya pun lalai untuk memintakan ijin baginya, padahal sebetulnya ijin akan diberikan asal saja diminta sebelumnya.

Ia didakwa melakukan pencurian ("grand larceny"). Dari bukti-bukti yang diajukan terungkap bahwa "print out" yang dihasilkan tidaklah berharga (worthless "scrap paper"), akan tetapi biaya penggunaan komputer itu sendiri bernilai antara $5,000 sampai $26,000. Terdakwa oleh pengadilan tingkat pertama dinyatakan bersalah melakukan pencurian. Namun dalam tingkat banding Supreme Court of Virginia telah membebaskan terdakwa dengan pertimbangan "ketentuan pidana mengenai pencurian tidak dimaksud untuk diperluas terhadap perbuatan pencurian waktu dan penggunaan komputer kecuali apabila secara tegas diatur oleh undang-undang tersebut. Demikian pula halnya berdasarkan "common law" hal-hal tersebut tidak termasuk pencurian."

Dalam putusan tersebut dipertimbangkan bahwa "*a larceny statute drawn to the obtaining of goods or chattels was incapable of applying to the obtaining of services, even though they were worth a considerable sum of money*". (Ketentuan mengenai pencurian barang atau surat berharga tidak dapat diterapkan terhadap pencurian waktu komputer, walaupun hal tersebut mempunyai nilai yang tinggi).[58]

Untuk mengisi kekurangan itu oleh negara bagian Virginia kemudian dikeluarkan amandemen yang mengatur "property juga meliputi "computer time or services or data processing services or information or data stored in connection therewith".[59]

People v. Weg, (1982)[60]

Dalam kasus yang hampir sama pengadilan di New York telah membebaskan terdakwa karena didakwa melakukan "theft of computer time and services". Dalam kasus ini terdakwa didakwa melakukan pelanggaran pencurian yang diatur dalam Theft of Services Act. Terdakwa adalah pegawai dari New York Board of Education yang menggunakan komputer kantor untuk berbagai keperluan pribadi, antara lain untuk menghitung

[58] 113 Misc.2d 1017, 450 N.Y. S.2d 957 (Crim. Ct.1982).Lihat Rostoker, hal. 343-344.
[59] Lihat Penal Code Virginia, Va.18.2-152.1.
[60] 450 N.Y.S at 961.

data peternakan kuda yang tidak ada hubungan dengan pekerjaannya. Pengadilan membebaskan terdakwa dari dakwaan pencurian dengan alasan bahwa pembuat undang-undang tidak bermaksud untuk menghukum setiap pegawai yang menggunakan komputer tanpa ijin. Dasar hukum lainnya yang ipertimbangkan ialah penafsiran terhadap kata "business" dalam undang-undang yang oleh pengadilan tidak dimaksudkan kepada lembaga pendidikan seperti Board of Education tersebut oleh karena itu aktivitasnya tidak termasuk yang dimaksud dalam undang-undang itu (... the Board of Education did not conduct a business, and, therefore, its activities were not governed by the statute).

United States v. Sampson, (1978)

Dalam kasus ini hakim District Court dari Northern District of California telah memutus sebaliknya. Dalam putusannya dikatakan bahwa "the use of the computer and the product of such uses would appear to the court to be a "thing of value" (penggunaan komputer dan hasilnya merupakan ""barang berharga" milik pemerintah). Dalam putusannya hakim menegaskan bahwa penggunaan fasilitas komputer tanpa ijin tak dapat dipisahkan dari identitas fisik dari komputer itu sendiri.

Dalam kasus ini terdakwa didakwa telah memasuki sistim komputer milik NASA dengan menggunakan tilpon di rumahnya, dan menggunakannya untuk kepentingan pribadi, yang dianggap merupakan pelanggaran atas undang-undang hukum pidana Bab 18 U.S.C. pasal 641 tentang pencurian. Kerugian NASA atas penggunaan komputer diperkirakan $1,924.[61]

Pengadilan berpendapat bahwa menggunakan komputer milik pemerintah merupakan pelanggaran atas ketentuan pidana federal mengenai pencurian yang mengatur:

> *Barangsiapa menggelapkan, mencuri, mengambil atau dengan sengaja memindahkan untuk kepentingannya atau kepentingan orang lain, atau tanpa ijin menjual, membawa atau menghilangkan setiap catatan, bukti penerimaan uang, uang atau barang lainnya yang berharga milik pemerintah Amerika Serikat bersalah oleh karena melakukan tindak pidana pencurian.*

F. TANPA HAK MEMASUKI SISTIM KOMPUTER (*Unauthorised Access to a Computer /Hacking*)

Istilah lainnya untuk kejahatan komputer ini adalah "unauthorised use of computer system", "illegal access", atau "unlawful entry". Istilah

[61] 6 C.L.S.R. 879 (N.D.Cal. 1978)

yang populer ialah "hacking". Seseorang tanpa hak seringkali memasuki suatu sistim komputer dengan perbagai alasan. Kadang-kadang hanya dengan dasar ingin tahu saja apa yang terkandung dalam data komputer tersebut, namun seringkali dibarengi dengan maksud-maksud jahat tertentu.

Cara memasuki sistim komputer dapat bermacam-macam, baik secara langsung dengan menggunakan komputer yang ada di kantor tersebut, ataupun dengan menggunakan terminal luar (remote terminal) di tempat lain. Perbuatan ini kadang-kadang tidak menimbulkan kerugian kepada sipemilik komputer, akan tetapi seringkali menimbulkan kerugian, yaitu dengan rusaknya atau terhapusnya sejumlah data komputer. Setidak-tidaknya dengan telah bisa "diintipnya" data komputer yang bersangkutan, sipemilik merasa perlu untuk memperbaiki sistim pengamanan, yang kadang-kadang memerlukan biaya yang besar.

Suatu kasus "hacking" yang terjadi belum lama ini di negeri Belanda telah menjadikan sasarannya suatu sistim pertahanan penting milik Departemen Pertahanan Amerika Serikat, diberitakan dalam Harian International Herald Tribune tanggal 22 April 1991.

Kasus itu merupakan perbuatan sejumlah "hackers" yang berhasil menerobos sistim komputer Departemen Pertahanan Amerika Serikat melalui komputer di tempat mereka (remote terminal), dan selama enam bulan terus memonitornya. Yang membuat rawan ialah usaha mereka itu diberitahukan kepada pemancar televisi setempat yang kemudian turut merekamnya. Sedangkan perbuatan tercela tersebut belum ada pengaturannya dalam Wetboek van Strafrecht.[62]

Perbuatan memasuki sistim komputer orang lain secara melawan hukum tersebut secara langsung tidak merugikan sipemilik, oleh karena sipelaku biasanya hanya ingin mengetahui saja apa yang terkandung dalam data komputer. Namun secara tidak langsung dapat merugikan, karena dengan dapat dimonitornya kegiatan yang ada dalam system komputer tersebut yang membuktikan bahwa "security measures" yang ada telah

---

[62] Lihat International Herald Tribune, "When The Law Allows Computer Raid", tanggal 22 April 1991, pagina 1 dan 4. WHEN THE LAW ALLLOWS COMPUTER RAIDS:

New York--Beyond the reach of American law, a group of Dutch computer intruders have been openly defying U.S. military, space and intelligence authorities for almost six months. Recently they broke into a U.S. military computer while being filmed by a crew from a Dutch television station.

The intruders, working over local telephone lines that enable them to tap U.S. computer networks at almost no cost, have not done serious damage, federal investigator say. They have not penetrated the most secure government computer systems. But they have entered a wide range of computers, includding those at the Kennedy Space Center, the Pentagon's Pacific Fleet Command, the Lawrence University, via an international computer network known as the Internet.

The information on these systems is not classified. But the computers store a great variety of material, including routine memorandums, unpublished reports and data from experiments. Federal officials said the group had tampered with some information stored on systems they have illegally entered.

US government officials said that they had been tracking the interlopers, but no arrests had been made because *there are no laws in the Netherlands barring unauthorized computer access.* (huruf miring dari penulis).

dapat diterobos, diperlukan usaha-usaha baru untmemperbaiki cara-cara pengamanan. Untuk ini tentu saja diperlukan waktu dan biaya yang besar.

Biaya perbaikan sistim komputer

Walaupun dalam berita hanya disebutkan perbuatan "have not done serious damage", namun diperkirakan bahwa kerugian yang diderita cukup besar. Penelitian-penelitian yang pernah dilakukan terhadap "cost of restoring a computer system" untuk meneliti kebocoran dan penyusunan suatu "security device" yang baru membuktikan bahwa biaya perbaikan memakan waktu yang relatip cukup lama dan biaya yang besar.

Laporan-laporan yang pernah diberikan kepada suatu komisi penyusunan undang-undang mengenai kejahatan komputer di Inggris - The Law Commission on Computer Misuse - khususnya mengenai bahaya "hacking" tersebut pada pokoknya mengungkapkan bahwa:

> *"...restoring a commercial computer system that has been illegitimately entered can amount to hundreds of thousands of pounds for rebuilding the system, and for the loss of the system while those operations take place.*[63]

Berdasarkan alasan tersebut oleh banyak negara menaruh perhatian untuk memidana perbuatan tercela itu, dan dalam hal undang-undang pidana yang berlaku tidak dapat diperlakukan atas perbuatan itu, usaha penyempurnaan dilakukan agar undang-undang pidana dapat menjangkau perbuatan tersebut.

Di Inggris, 'hacking' atau 'unauthorized access' merupakan salah satu perbuatan yang mendapat perhatian dari The Law Commission on Computer Misuse, oleh karena ternyata undang-undang hukum pidana mengenai pencurian dan penipuan yang telah beberapa kali dirubah tidak dapat menjangkau kejahatan komputer jenis tersebut, terbukti dengan adanya putusan House of Lords yang melepaskan terdakwa Gold dan Schifreen, yang melakukan 'hacking' atas sistim komputer perusahaan Perstel, satu perusahaan yang berkecimpung dalam jasa informasi.

Dengan dibebaskannya kedua terdakwa atas dakwaan pemalsuan (forgery) maka Theft Act 1968 dan 1978, dan Forgery Counterfeiting Act 1981 yang sebelumnya dianggap sebagai senjata ampuh untuk menanggulangi pelbagai kejahatan komputer, ternyata tidak dapat diterapkan terhadap kasus pemalsuan tersebut, sehingga dengan agak tergesa-gesa akhirnya Computer Misuse Act 1990 diundangkan.

[63] "Lihat Report of The British Law Commission on Computer Misuse (1989), alinia 1.31.

Mengingat perbuatan 'hacking' kalau dibiarkan akan dapat menimbulkan ekses yang membahayakan, Komisi Inggris berpendapat agar undang-undang mengenai kejahatan komputer disempurnakan untuk dapat mencakup semua perbuatan penyalahgunaan komputer.

Kasus-kasus 'hacking' yang pernah terjadi seringkali mengganggu sistim komputer, yang akhirnya dapat menimbulkan kerugian pihak pemilik komputer dan bahkan dapat membahayakan keselamatan jiwa jika komputer yang dirusak berkaitan dengan transportasi masal, baik di udara, laut maupun di darat. Pada akhir-akhir ini kasus yang pernah terjadi jumlahnya banyak sekali, dan seringkali diberitakan dalam beberapa situs di Internet.

Berikut beberapa contoh kasus lama kerugian akibat "hacking" di Inggris :

- kerugian yang dialami oleh beberapa travel agency dengan adanya pesanan-pesanan palsu melalui data komputer;
- kekacauan yang terjadi pada sistim komputer dari perusahaan yang menggunakan robot yang hampir membunuh petugas;
- kekacauan sistim komputer suatu perusahaan yang menyebabkan pengiriman ribuan surat dan uang kepada orang-orang yang tidak berkepentingan,
- kerusakan yang dialami system pertahanan beberapa negara,
- dan banyak lagi kejadian lainnya.

Komisi Inggris berpendapat bahwa kasus-kasus itu dianggap cukup relevan untuk menyatakan perbuatan ini sebagai tindak pidana.

Kerusakan lain yang timbul pada sistim komputer akibat 'hacking' ini bisa terjadi akibat tersebarnya "virus" pada sistim komputer. Beberapa waktu sebelum Computer Misuse Act 1990 diundangkan beberapa perbuatann yang merusak komputer terjadi di Inggris, antara lain, kerusakan terhadap data komputer suatu universitas yang berisi hasil research selama 2 tahun; dan kerusakan yang dialami sistim komputer beberapa perusahaan besar yang mengakibatkan perusahan tersebut ditutup untuk perbaikan beberapa lamanya.

Para 'hackers' sendiri seringkali sukar untuk dilacak oleh karena sulit untuk mencari jejak mereka, apalagi kalau dilakukan dari terminal luar atau dari "cyberspace".[64]

Untuk menanggulangi masalah ini Komisi Inggris mengusulkan tiga peraturan baru, yaitu yang melarang perbuatan memasuki sistim komputer orang lain tanpa hak, baik sekedar ingin tahu saja ataupun untuk maksud-maksud jahat tertentu ('hacking for a further purpose'), yaitu:

[64] Lihat Report of The British Commission on Computer Misuse, (1989); juga Wasik, hal.70-85.

1. Tanpa hak memasuki komputer.
2. Tanpa hak memasuki komputer dengan maksud untuk melakukan atau mempermudah melakukan suatu tindak pidana yang serius.
3. Tanpa hak merubah data komputer.[65]

Rancangan ini akhirnya disetujui Parlemen dan dijadikan Computer Misuse Act 1990 yang mulai berlaku tanggal 29 Agustus 1990. Ancaman pidana untuk kejahatan kesatu adalah 6 bulan pidana penjara atau denda, sedangkan perkaranya dapat diperiksa secara 'sumir'. Untuk kejahatan kedua dan ketiga adalah 5 tahun penjara atau denda, atau pidana penjara dan denda (pasal (5) (a) dan (b)).

Kemajuan di bidang komputer dan Internet telah menciptakan pula hackers yang canggih yang seringkali dapat menerobos system komputer orang lain baik untuk senang-senang atau untuk merusaknya. Dampak perbuatan mereka sekarang semakin dirasakan.[66]

Permasalahan Hukum

Di beberapa negara perbuatan ini tidak menimbulkan banyak permasalahan hukum oleh karena pengadilan menerapkan ketentuan undang-undang yang melarang perbuatan menggunakan barang orang lain tanpa ijin ('unauthorized or illegal use of another person's property'), misalnya pasal 461 Penal Code Belgia dan pasal 293 Penal Code Denmark.

Seperti halnya Inggris, di beberapa negara lainnya seperti Austria, Canada, Jerman dan Belanda ketentuan yang ada hanya diperlakukan terhadap perbuatan tertentu saja, misalnya 'joyriding', atau terhadap perbuatan yang menimbulkan kerugian atau ketidaknyamanan kepada pemilik.[67]

Ketentuan "tradisionil" yang melindungi "keamanan tempat tinggal" (domestic peace) (seperti diatur dalam pasal 439 Penal Code Belgia; pasal 123, Penal Code Jerman Barat; atau pasal 614, Penal Code Italia) atau menghukum perbuatan merubah atau membuat duplikat kunci (seperti diatur dalam pasal 399 Penal Code Perancis) tidak dapat diterapkan terhadap perbuatan memasuki tanpa ijin suatu 'pekarangan' komputer secara elektronis.

Juga perbuatan 'membuka surat tanpa ijin' seperti diatur dalam pasal 118 Penal Code Austria dan pasal 202 Penal Code Jerman Barat (dulu) tidak dapat diterapkan terhadap perbuatan 'tanpa hak memasuki sistim

[65] Ibid, alinia 2.2-2.3.
[66] Lihat Barrett, 1996: Hackers and digital vandalism, hal. 39-52.
[67] Piragoff, hal.118-119.

komputer'.[68] Ketentuan pidana yang mengatur pelanggaran terhadap sistim telekomunikasipun tampaknya sulit diterapkan terhadap pelanggaran terhadap sistim antar komputer yang tidak bersifat untuk umum ('closed computer system'). Dalam kasus R. v. Michael MacLaughlin, Supreme Court Canada memutus bahwa "telecommunications facility does not include a 'closed' computer system in which terminals are linked directly to the main computer."[69]

Usul penyempurnaan

Untuk dapat menjangkau integritas sistim komputer, Departemen Kehakiman Canada menyusun amandemen undang-undang yang melarang perbuatan-perbuatan tersebut, yang kemudian menjadi Criminal Law Amendment Act, 1985. Pasal 301.2(1)(b) menyatakan sebagai suatu tindak pidana

> *"...barang siapa secara tidak jujur dan tanpa hak ...dengan memakai sarana elektromagnit, akoustik, mekanis atau alat lain menyadap (mengintersepsi) atau menyebabkan tersadapnya, baik secara langsung maupun tidak langsung, setiap fungsi dari satu sistim komputer.*[70]

Beberapa negara lainnya telah membuat ketentuan baru yang melarang perbuatan 'memasuki sistim komputer tanpa hak', seperti yang diatur dalam pasal 1, 2 dan 3 Computer Misuse Act 1990 Inggris. Pasal 502(d)(2) dari California Penal Code yang berlaku mulai 1 January 1985, menjadikan sebagai suatu pelanggaran (misdemeanor) perbuatan yang hanya berupa 'mere access', yaitu 'barangsiapa yang dengan sengaja memasuki sesuatu sistim komputer, jaringan komputer, program komputer, atau data, yang diketahuinya bahwa memasuki sistim itu dilarang oleh sipemilik atau sipenyewa (lesee).

Untuk perbuatan yang lebih berat diatur dalam pasal 502(b), (c) dan (d)(1) yang memidana dengan sanksi yang lebih berat perbuatan-perbuatan 'fraud, extortion, obtaining property or certain information or incapacitating a computer system'.[71]

Undang-undang federal baru The Counterfeit Access Device and Computer Fraud and Abuse Act 1984 yang berlaku sejak tanggal 12 Oktober 1984 memidana setiap orang yang melakukan perbuatan secara tanpa memasuki komputer yang dipergunakan oleh agen-agen federal,

---

[68] Lihat pasal 118 Penal Code Austria dan pasal 202 Penal Code Jerman Barat

[69] . R. v McLaughlin (1980) 53 CCC (2d) 417.

[70] Piragoff, hal.105; Sieber (1986), hal 88.

[71] Sieber, hal.89.

bank-bank, biro perkreditan ('credit bureaus') dengan maksud untuk mendapatkan informasi rahasia yang dapat merugikan pemerintah Amerika Serikat, atau keuntungan negara lain, untuk mendapatkan informasi dari lembaga keuangan atau 'consumer reporting agency'; atau dengan sengaja menggunakan, merubah, menghancurkan, atau mengumumkan keterangan, atau menghalangi dipergunakannya komputer tertentu oleh yang berhak.[72] Tampaknya ketentuan itu belum lengkap sehingga diadakan beberapa perubahan dalam Chapter 33 tentang Computer Crimes.[73]

Ketentuan baru pasal 263(2) Penal Code Denmark tentang 'Datakriminalitet' menjadikan suatu tindak pidana perbuatan 'memasuki sistim informasi atau program orang lain yang dimaksudkan untuk dipergunakan dalam suatu pemrosesan data'. Selain daripada itu pasal 263 (3) mengancam dengan pidana yang lebih berat apabila perbuatan itu dilakukan 'dengan maksud untuk mengetahui atau mendapatkan informasi rahasia dagang suatu perusahaan'.

Pasal itu berbunyi:

> *Barangsiapa secara melawan hukum, memasuki informasi atau program orang lain yang digunakan dalam sistim pemrosesan data, karena salahnya dipidana dengan denda, pidana kurungan atau pidana penjara selama-lamanya 6 bulan.*
> *Apabila perbuatan tersebut dalam sub seksi 1 dan 2 dilakukan dengan maksud untuk mendapatkan atau mengetahui informasi tentang rahasia dagang dari suatu perusahaan atau dilakukan dengan keadaan yang memberatkan, pidana yang dijatuhkan akan ditambah dengan pidana penjara selama-lamanya 2 tahun.*

Pasal 21 dari Swedish Data Protection Act tanggal 2 April 1973 yang disempurnakan tanggal 1 Juli 1982, memidana 'setiap orang yang memasuki sistim komputer tanpa hak'. Pasal tersebut berbunyi:

> *Barangsiapa secara melawan hukum memasuki rekaman yang digunakan untuk memproses data secara otomatis, atau yang secara melawan hukum membuat perubahan-perubahan atau penghapusan-penghapusan rekaman dalam suatu arsip, dipidana karena salahnya melakukan perbuatan memasuki data ('data trespass') dengan denda atau pidana penjara selama-lamanya dua tahun, kecuali apabila perbuatan itu dipidana berdasarkan Kitab Undang-Undang Hukum Pidana.* [74]

---

[72] Publ. L.98-473, H.J. Res. 648-354,sect.1030. Lihat pula Sieber (1986), hal.88-89.
[73] Lihat Bab III Amendemen Federal Penal Code.
[74] Ibid, hal. 239.

Pasal 167 Kitab Undang-Undang Hukum Pidana hanya mengatur perbuatan memasuki rumah, ruangan atau pekarangan secara melawan hukum, dan sesuai dengan pendapat para sarjana pada umumnya, tidak dapat diperluas kepada pengertian tanpa hak memasuki sistim komputer. Pasal itu berbunyi:

1. Barangsiapa masuk dengan paksa ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain secara melawan hukum atau berada disitu secara melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak segera pergi dari situ, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.
2. Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu, atau barangsiapa tanpa setahu yang berhak terlebih dahulu serta bukan karena kekeliruan masuk dan kedapatan di situ pada waktu malam, dianggap masuk dengan paksa.
3. Bila ia mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, maka ia diancam dengan pidana penjara paling lama satu tahun empat bulan.

Pidana tersebut dalam ayat (1) dan (3) dapat ditambah sepertiga bila yang melakukan kejahatan dua orang atau lebih dengan bersekutu.

Komisi Franken mengusulkan peraturan baru yang melarang perbuatan 'hacking' ini dalam rancangan undang-undang mengenai kejahatan komputer, sebagai usulan 15, yang dapat diterapkan terhadap pelaku orang luar maupun orang dalam yang tugasnya menggunakan komputer, sebagai berikut :

Usulan 15: Peraturan baru. Merupakan 'computer trespass' atau 'hacking', diletakan dekat pasal 138 Sr. (pasal 167 KUHPidana) tentang 'huisvredebruik'.

Barang siapa secara melawan hukum memasuki alat yang dikomputerisasi yang telah dilindungi, yang dipergunakan untuk menyimpan atau mejalankan data, atau bagian yang dilindungi disana, diancam pidana selama-lamanya 6 bulan atau denda dalam kategori ketiga.

Barang siapa yang telah memasuki sistim dengan menggunakan kemampuan palsu, dengan cara-cara menipu atau dengan mengunakan kode palsu dianggap telah memasuki alat itu.

Dalam penjelasan Komisi tersebut dikatakan bahwa yang dimaksud dengan 'memasuki' ialah memasuki secara elektronis, dan bukan secara fisik.

Untuk menjaga agar suatu pekarangan atau rumah tidak dimasuki biasanya dipasang tanda larangan 'dilarang masuk'. Dalam sistim komputer larangan ini berwujud keharusan menggunakan 'password' atau 'PIN' atau tanda pengenal lainnya, jika akan memasuki sistim komputer. Tanpa menggunakan tanda pengenal sipelaku dapat dinyatakan bersalah memasuki secara melawan hukum.[75]

G. LAIN-LAIN

1. Tindak pidana membuka rahasia (spionase)

Ketentuan yang berlaku di beberapa negara mengenai membocorkan rahasia negara dapat diperlakukan terhadap perbuatan membocorkan rahasia yang terkandung dalam data komputer yang dilakukan oleh siapa saja.

Pasal 112 Kitab Undang-Undang Hukum Pidana mengatur:

> *Barangsiapa dengan sengaja mengumumkan, atau mengabarkan atau menyampaikan surat-surat, kabar dan keterangan tentang sesuatu hal kepada negara asing, sedang ia mengetahui, bahwa surat, kabar atau keterangan itu harus dirahasiakan karena kepentingan negara, dipidana dengan pidana penjara selama-lamanya tujuh tahun.*

Namun perlindungan terhadap pembocoran rahasia perusahaan yang mungkin terkandung dalam data komputer pada umumnya hanya dapat diperlakukan terhadap perbuatan pegawai yang diberi tugas untuk merahasiakannya atau bekas pegawai, dan tidak dapat diperluas terhadap orang luar. (Lihat misalnya pasal 309 Penal Code Belgia, pasal 623 Penal Code Italia, pasal 273 W.v.S Belanda, dan pasal 323 KUHP).[76]

Pasal 323 Kitab Undang-Undang Hukum Pidana mengatur:

1. Barangsiapa dengan sengaja memberitahukan hal ihwal tentang sesuatu perusahaan dagang, kerajinan atau pertanian, tempat ia bekerja atau dahulunya telah bekerja, sedang ia diwajibkan

[75] Lihat Laporan Komisi Franken (Report of the Dutch Committee), hal.55-58.
[76] .Sieber (1986), hal.57.

merahasiakan hal ihwal itu, dipidana dengan pidana penjara selama-lamanya sembilan bulan atau denda sebanyak-banyaknya sembilan ribu rupiah.

2. Kejahatannya itu hanya dituntut atas pengaduan dari pengurus perusahaan itu.

Mengingat berharganya rahasia perusahaan tersebut maka untuk memperoleh ganti kerugian dalam praktek dipergunakan ketentuan Hukum Perdata, misalnya dalam ketentuan mengenai 'persaingan curang' (unfair conpetition) atau perbuatan melawan hukum. [77]

Oleh karena rahasia perusahaan seringkali disimpan dalam data komputer, maka kemungkinan untuk 'dicuri' oleh pihak luar dengan cepat dan tanpa diketahui menjadi lebih mudah. Agar ketentuan pidana ini dapat diperlakukan terhadap pihak luar, beberapa negara telah menyempurnakan ketentuan pidana mengenai membuka rahasia perusahaan seperti misalnya pasal 202a Penal Code Jerman Barat (dulu) yang tercantum dalam amandemen "Second Law for the Prevention of Economic Crimes of 1986' yang berisi :

Section 202a. Data Espionage

(1) Barangsiapa yang mengambil tanpa hak baik untuk dirinya maupun untuk orang lain, data yang tidak diperuntukkan baginya, dan secara khusus dilindungi agar tidak dimasuki secara tanpa hak, dipidana dengan pidana penjara selama-lamanya tiga tahun atau denda.

(2) Yang dimaksud dengan data dalam subseksi (1) ialah data yang disimpan atau dipancarkan secara elektronis atau magnetis atau dengan cara lain yang secara langsung tidak terlihat.

Selanjutnya pasal 17 ketentuan pidana mengenai *'Unfair Competition'* Jerman Barat telah diperbaiki *oleh 'Second Law for the Prevention of Economic Crime of 1986"* tersebut dengan menambahkan beberapa kata dalam butir 1 dan ketentuan baru yang tercantum dalam butir 2, sehingga berbunyi:

1. Dipidana penjara selama-lamanya tiga tahun atau suatu denda, pegawai, tukang, atau calon pegawai dari suatu

[77] Misalnya seperti diatur dalam pasal 1 Undang-Undang mengenai Unfair Competition Jerman Barat (dulu), pasal 54 Fair Trade Practices Act of 1971 Belgia, pasal 2598 Civil Code Italia, pasal-pasal 1382-1383 Civil Code Perancis, pasal 1401 Kitab Undang-Undang Hukum Perdata Belanda, atau pasal 1365 Kitab Undang-Undang Hukum Perdata Indonesia (BW).

perusahaan, yang selama dalam ikatan kerja tanpa hak memberitahukan kepada orang lain suatu rahasia dagang atau rahasia industri yang dipercayakan kepadanya atau ada padanya sehubungan dengan ikatan kerja, apabila ia lakukan hal tersebut untuk persaingan atau untuk kepentingan pribadi atau untuk kepentingan pihak ketiga, atau dengan maksud untuk menghancurkan usaha sipemilik.

2. Pidana yang sama akan dijatuhkan terhadap barang siapa yang dengan maksud untuk melakukan persaingan atau keuntungan pribadi atau pihak ketiga atau dengan maksud menghancurkan pemilik perusahaan.
3. Memperoleh atau menghasilkan tanpa hak suatu rahasia dagang atau rahasia industri dengan : mempergunakan alat-alat teknis, mereproduksi secara fisik (corporeal reproduction) rahasia, atau memindahkan suatu objek di mana rahasia tersimpan, atau menggunakan tanpa hak atau memberitahukan kepada orang lain suatu rahasia dagang atau rahasia industri yang diperolehnya secara tanpa hak melalui komunikasi seperti tersebut dalam subseksi 1 atau melalui perbuatan seperti disebutkan dalam butir 1 pasal ini yang dilakukan olehnya atau oleh orang lain.
4. Percobaan terhadap tindak pidana ini dipidana.
5. Dalam perkara-perkara khusus yang berat (serius) pidana yang dijatuhkan selama-lamanya lima tahun.

Sebagai pedoman suatu perkara dianggap berat apabila sipelaku mengetahui pada waktu membocorkan (berkomunikasi) bahwa rahasia itu akan dipergunakan di luar negeri atau apabila ia sendiri akan menggunakannya di luar negeri.

Komisi Franken mengusulkan penyempurnaan mengenai tindak pidana 'membuka rahasia' sebagai berikut:

Usulan 13: Amandemen pasal 98, 98 a, 98b, 98c, Sr - (hampir sama dengan pasal 112 dst. KUHP), yaitu dengan menambahkan "....data atau keterangan, dan benda dari mana data atau keterangan berasal", untuk menghilangkan salah pengertian berhubung dipakainya kata-kata data atau keterangan dalam pasal-pasal tersebut.

Barangsiapa dengan sengaja mengumumkan atau menyerahkan kepada orang lain atau badan yang tidak berhak untuk mengetahuinya, suatu data atau suatu keterangan" yang menyajikan rahasia untuk kepentingan

negara atau sekutunya, atau suatu benda yang dapat memberikan data demikian atau keterangan demikian, diancam dengan pidana penjara paling lama enam tahun atau denda menurut kategori kelima, jika ia mengetahui atau patut harus menduga bahwa itu menyangkut data yang demikian.

Ayat kedua pasal ini, begitu pula pasal-pasal 98a,`98 b dan pasal 98 c, masing-masing ditambah kata-kata dapat memberikan data atau keterangan demikian.

Usulan 14: Amandemen pasal 273 WvS - padannya pasal 323 KUHP.

Dimaksud untuk memperluas perlindungan kepada rahasia perusahaan dagang dan perusahaan jasa.

1. Barangsiapa dengan sengaja memberitahukan " atau menggunakan demi untuk maksud keuntungan sendiri" hal-hal khusus tentang suatu perusahaan dagang, industri atau pemberian jasa" dimana ia bekerja atau pernah bekerja yang harus dirahasiakannya, diancam dengan pidana penjara paling lama enam bulan atau denda menurut kategori keempat.
2. Tiada penuntutan tanpa pengaduan pengurus perusahaan itu.

2. Penambahan kata-kata 'atau data yang mempunyai nilai kekayaan dalam dunia perdagangan setelah kata 'barang'.

Usulan 17: Menambahkan "atau data yang mempunyai nilai kekayaan dalam dunia perdagangan "('of gegevens met vermogenswaarde in het handelsverkeer'), kepada:

Pasal 198 Sr.--padannya pasal 231 KUHP ;
Pasal 317 Sr.--padannya pasal 368 KUHP;
Pasal 318 Sr.--padannya pasal 369 KUHP
Pasal 329 Sr.--padannya pasal 383 KUHP;
Pasal 341 Sr.--padannya pasal 379 KUHP;
Pasal 343 Sr.--padannya pasal 399 KUHP;
Pasal 349 Sr.--padannya pasal 404 KUHP ayat 1 butir 1 dan ayat 2;

3. Perlindungan hak cipta mengenai 'program komputer' melalui Undang-Undang Hak Cipta.

Selain menyempurnakan undang-undang hukum pidana, sejumlah negara telah menyempurnakan undang-undang mengenai perlindungan hak cipta (copy-right) sehingga juga meliputi 'program komputer'.

Dengan berkembangnya system Internet, setiap software yang berisi copyrights (hak cipta) yang berupa "digital goods" dengan mudah menjadi sasaran pencurian dan pengkopian yang illegal dan kemudian diperjualbelikan lagi. Dengan diperolehnya software ciptaan seseorang atau perusahaan, sipelaku kejahatan dengan mudah memanipulasi atau merubah, atau menjual kepihak lain hasil curian atau sadapannya itu.

Berbagai usaha pengamanan telah dilakukan oleh para pencipta agar ciptaannya tidak gampang disadap atau dicuri secara elektronis, antara lain dengan membuat code atau karakter khusus atau "encryption". Namun seringkali pula hackers dapat membukan kode tersebut sehingga dengan mudah membacanya dan mengkopinya.

Undang-Undang Perlindungan Hak Cipta No. 7 tahun 1987 yang menyempurnakan Undang-Undang Hak Cipta No. 6 tahun 1982 memberikan perlindungan terhadap ciptaan dalam bidang ilmu pengetahuan, seni, dan sastra, yang diantaranya adalah 'program komputer' atau 'komputer program' (pasal 11 (1) k.).

Dalam rangka pelaksanaan pembangunan nasional, dan dengan memperhatikan semakin pentingnya peranan dan penggunaan komputer, maka dalam rangka pengembangan kemampuan nasional, khususnya di bidang pembuatan Program Komputer atau Komputer Program (Computer Program), Pemerintah menganggap sudah waktunya untuk memberikan perlindungan hukum terhadap karya cipta ini.

Alasan mengapa Undang-Undang No. 6 Tahun 1982 perlu disempurnakan dijelaskan dalam latar belakang dan ketentuan umum, antara lain, adalah sebagai berikut:

1. Ancaman pidana yang dinilai terlalu ringan, dan kurang mampu menjadi penangkal terhadap pelanggaran Hak Cipta. Selain itu untuk efektifitas penindakan, dipandang perlu menyesuaikan ancaman pidana penjara dengan ketentuan tentang penahanan dalam Pasal 21 KUHAP.
2. Masih dalam upaya untuk meningkatkan efektifitas penindakan, ketentuan bahwa pelanggaran terhadap Hak Cipta merupakan tindak pidana aduan, juga dinilai tidak sesuai dengan kebutuhan. Pelanggaran tersebut seharusnya memang diperlakukan sebagai

tindak pidana biasa. Penindakannya, dengan begitu tidak lagi semata-mata didasarkan pada adanya pengaduan.

3. Akibat daripada pelanggaran Hak Cipta bukan saja merugikan Pencipta atau Pemegang Hak Cipta, tetapi juga perekonomian pada umumnya. Oleh karena itu, sudah sewajarnya apabila ciptaan atau barang yang terbukti merupakan hasil pelanggaran Hak Cipta, dirampas untuk Negara guna dimusnahkan.
4. Masalah yang perlu pula ditegaskan adalah, adanya hak pada Pemegang Hak Cipta yang dirugikan karena pelanggaran, untuk mengajukan gugatan perdata tanpa mengurangi hak Negara untuk melakukan tuntutan pidana.
5. Seiring dengan langkah di atas, untuk mencegah kerugian yang lebih besar pada pihak yang haknya dilanggar dirasakan perlu adanya penambahan ketentuan yang selama ini belum ada, yaitu penegasan tentang kewenangan Hakim untuk memerintahkan penghentian kegiatan pembuatan, perbanyakan, pengedaran, penyiaran, dan penjualan ciptaan atau barang yang merupakan hasil pelanggaran Hak Cipta sebelum putusan Pengadilan. Lihat Penjelasan atas Undang-Undang Nomor 7 Tahun 1987 tentang Perubahan atas Undang-Undang Nomor 6 Tahun 1982 tentang Hak Cipta.

Undang-Undang No. 7 Tahun 1987 ini mengatur sanksi yang jauh lebih berat daripada Undang-Undang No. 6 Tahun 1982. Pasal 44 berbunyi:

1. Barangsiapa dengan sengaja dan tanpa hak mengumumkan atau memperbanyak suatu ciptaan atau memberi izin untuk itu, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.100.000.000.-(seratus juta rupiah).
2. Barangsiapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran Hak Cipta sebagaimana dimaksud dalam ayat 1, dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp.50.000.000.-(lima puluh juta rupiah).
3. Barangsiapa dengan sengaja melanggar ketentuan Pasal 16, dipidana dengan pidana penjara paling lama (3) tahun dan/atau denda paling banyak Rp.25.000.000,- (dua puluh lima juta rupiah).

Pasal 46 UUPHC 1987 menegaskan bahwa tindak pidana sebagaimana dimaksud dalam pasal 44 adalah kejahatan (bukan pelanggaran). [78]

[78] Pembahasan mengenai perbedaan Undang-Undang No. 7 Tahun 1987 dan Undang-Undang No. 6 Tahun

Pasal 44 Undang-Undang Hak Cipta memberikan perlindungan bagi pemegang Hak Cipta terhadap perbuatan :

1. dengan sengaja dan tanpa hak mengumumkan atau memperbanyak suatu ciptaan atau memberi izin untuk itu;
2. dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran Hak Cipta
3. dengan sengaja melanggar ketentuan Pasal 164.
4. dengan sengaja melanggar ketentuan Pasal 18;[79]

Tidak selalu orang yang dipotret akan setuju bahwa potretnya diumumkan tanpa diminta persetujuannya. Pasal 18 (pasal 19, 20 UU No. 19/2002) mewajibkan permintaan persetujuan yang bersangkutan atau dari ahliwarisnya.

Undang-undang No. 7 tahun 1987 diganti dengan Undang-undang No. 12 tahun 1997, dan terahir dengan Undang-undang No. 19 tahun 2002. Sanksi pidana yang diatur dalam Undang-undang ini jauh lebih berat dari Undang-undang No. 7 tahun 1987. Sedangkan kewenangan untuk memeriksa pelanggaran atas hak cipta kini dilimpahkan ke Pengadilan Niaga.[80]

Dalam hal terjadi pelanggaran terhadap program komputer diluar yang diatur dalam undang-undang ini, maka ketentuan pidana lainnya seperti tersebut di atas dapat diterapkan sepanjang tidak bertentangan dengan prinsip-prinsip hukum yang berlaku.

4. Undang-Undang Tindak Pidana Korupsi

Undang-undang ini merupakan salah satu senjata ampuh atau sering disebut sebagai *"all embracing act"* untuk menanggulangi kejahatan komputer sepanjang yang dirugikan adalah negara atau badan yang mendapat bantuan negara.

Pasal 1 mengatur siapa-siapa dan perbuatan apa yang dapat dipidana berdasarkan undang-undang ini sebagai berikut:

1982, lihat Kansil, Hak Milik Intelektual Bumi Aksara, 1990. Lihat pula Andi Hamzah, Aspek-Aspek Pidana di Bidang Komputer, 1987.Untuk Undang-undang No. 19, 2002 lihat Hadi Setia Tunggal, SH, Harvarindo, 2003.

[79] UUPHC-1987 dalam pasal 16 (yang menggantikan pasal 16 UUHC-1982) menegaskan bahwa, Pemerintah setelah mendengar pertimbangan Dewan Hak Cipta, dapat melarang pengumuman setiap ciptaan yang bertentangan dengan kebijaksanaan Pemerintah di bidang pertahanan dan keamanan negara, kesusilaan, serta ketertiban umum. Ketentuan baru ini dimaksudkan untuk mencegah beredarnya ciptaan yang merendahkan antara lain nilai-nilai keagamaan, ataupun masalah kesukuan dan ras, yang apabila diumumkan dapat menimbulkan gangguan atau bahaya terhadap pertahanan keamanan negara, bertentangan dengan norma kesusilaan umum yang berlaku dalam masyarakat, dan ketertiban umum.

[80] Pasal 59, 60.

Dihukum karena tindak pidana korupsi ialah:

> *Barangsiapa dengan melawan hukum melakukan perbuatan memperkaya diri sendiri atau orang lain, atau suatu Badan, yang secara langsung atau tidak langsung merugikan keuangan negara dan atau perekonomian negara, atau diketahui atau patut disangka olehnya bahwa perbuatan tersebut merugikan keuangan negara atau perekonomian negara.*

Beberapa kasus-kasus kejahatan komputer yang terjadi di Indonesia yang menyangkut bank negara atau yang mendapat bantuan dari negara diadili dan diputus berdasarkan undang-undang ini. Namun kasus-kasus yang terjadi menunjukkan bahwa korban kejahatan komputer tidak saja negara akan tetapi juga pihak swasta yang tentunya tidak dapat dilindungi oleh undang-undang ini.

Biasanya ketentuan pidana yang diterapkan badan swasta ialah pencurian, penggelapan atau penipuan. Terlihat perbedaan yang prinsipil dari kejahatan komputer yang diadili berdasarkan Undang-Undang Tindak Pidana Korupsi dan yang diadili berdasarkan pasal-pasal dalam KUHPidana tersebut.

Perbedaan yang terutama ialah mengenai ancaman pidana yang diatur dalam masing-masing tindak pidana itu.:

- Untuk pencurian (pasal 362 KUHP) ancaman pidananya adalah 5 tahun atau pidana denda paling banyak sembilan ratus rupiah;
- Untuk penggelapan (pasal 372 KUHP) ancaman pidananya adalah 4 tahun atau denda paling banyak sembilan ratus rupiah; dan
- Untuk penipuan (pasal 378) ancaman pidana adalah 4 tahun.

Sedangkan untuk tindak pidana korupsi ancaman pidananya adalah:

seumur hidup, atau
penjara selama-lamanya 20 tahun dan/atau
denda setinggi-tingginya 30 (tiga puluh) juta rupiah (pasal 28).

Selain daripada itu dapat dijatuhkan pidana tambahan seperti tercantum dalam pasal 34 sub a, b, dan c. yang berbunyi sebagai berikut:

Pasal 34.

Selain ketentuan-ketentuan pidana yang dimaksud dalam KUHP maka sebagai hukuman tambahan adalah:

- Perampasan barang-barang tetap maupun tak tetap yang berwujud dan yang tak berwujud, dengan mana atau mengenai mana tindak pidana itu dilakukan atau yang seluruhnya atau sebagian diperolehnya dengan tindak pidana korupsi itu, begitu pula harga lawan barang-barang yang menggantikan barang-barang itu, baik apakah barang-barang atau harga lawan itu kepunyaan siterhukum ataupun bukan;
- Perampasan barang-barang tetap maupun tak tetap yang berwujud dan tak berwujud yang termasuk perusahaan siterhukum, dimana tindak pidana korupsi itu dilakukan begitu pula harga lawan barang-barang yang menggantikan barang-barang itu, baik apakah barang-barang atau harga lawan itu kepunyaan siterhukum ataupun bukan, akan tetapi tindak pidananya bersangkutan dengan barang-barang yang dapat dirampas menurut ketentuan tersebut sub a pasal Pembayaran uang pengganti yang jumlahnya sebanyak-banyaknya sama dengan harta-benda yang diperoleh dari korupsi;

Keadaan tersebut dirasakan merupakan suatu 'diskriminasi' dalam soal penerapan hukum, dan juga pidana yang dijatuhkan, oleh karena berdasarkan ketentuan yang berlaku dimungkinkan untuk mengadili perkara dengan pasal-pasal dalam Undang-Undang Tindak Pidana Korupsi bagi perbuatan-perbuatan dimana pihak yang dirugikan adalah Negara, dengan kemungkinan dijatuhi pidana dan denda yang tinggi, sedangkan bagi perbuatan-perbuatan dimana yang menjadi korban adalah pihak swasta murni, tidak mungkin diterapkan Undang-Undang Tindak Pidana Korupsi. Hal ini tentunya dapat menimbulkan ketidakpuasan pihak-pihak tertentu.

Dengan semakin besarnya kerugian yang dapat ditimbulkan oleh kejahatan komputer, ancaman pidana pada pasal-pasal mengenai pencurian, penggelapan, penipuan, perusakan, dan tindak pidana lainnya yang menggunakan komputer harus diperberat.

Komisi Franken dalam rancangan undang-undang telah mengusulkan ancaman pidana yang lebih berat bagi kejahatan komputer yang menimbulkan kerugian besar atau korban manusia.

Model Computer Penal Code

Berhubung dengan makin canggih dan berkembanganya kejahatan komputer yang seringkali menimbulkan kerugian yang besar bagi lembaga-lembaga negara, swasta dan perorangan, dan agar penerapan hukum bagi sipelaku kejahatan komputer lebih seragam, beberapa lembaga hukum dan perguruan tinggi telah mencoba mengembangkan "model penal code computer crime" sehingga dapat menjangkau semua jenis kejahatan komputer dari yang sederhana hingga yang canggih.

Beberapa model penal code dan penal code yang diperlakukan dibeberapa Negara dapat dilihat dalam Bab III dan Lampiran I, II, III dan IV.

BAB IV
PENYEMPURNAAN UNDANG-UNDANG HUKUM PIDANA (PENAL CODE) DIBEBERAPA NEGARA DALAM UPAYA PENANGGULANGAN KEJAHATAN KOMPUTER

Berdasarkan pengamatan para pakar internasional pemberantasan penyempurnaan undang-undang hukum pidana tentang kejahatan komputer harus dilaksanakan secara komprehensif, yaitu dengan mempelajari lagi setiap peraturan perundang-undangan dimana sarana komputer terlibat. Hal mana dimaksudkan agar kekosongan dalam satu undang-undang dapat diisi oleh undang-undang lainnya.

Di beberapa negara penyempurnaan hukum pidana dilaksanakan dengan mengamandemen Hukum Pidana (Penal Code) yaitu dengan mengundangkan beberapa ketentuan baru mengenai kejahatan komputer dan mengamandemen undang-undang yang berkaitan dengan penggunaan komputer, Electronic commerce, Internet fraud, money-laundering, dan undang-undang mengenai Hak Cipta (Copyrights).

Pengertian barangpun harus diperluas juga meliputi "digital goods" seperti data, piranti lunak, jaringan komputer system computer, system Internet, penggunaan komputer (use of computer), dan lainnya. Dari uraian pada Bab II dapat disimpulkan bahwa kejahatan komputer pada pokoknya dapat dibagi atas 2 kategori, yaitu:

1. Komputer beserta berbagai fasilitas yang tersedia sebagai objek kejahatan, dan
2. Komputer sebagai sarana untuk melakukan kejahatan

Kerugian yang dapat ditimbulkan oleh kedua jenis kejahatan sama besarnya. Dengan menghancurkan komputer dan segala fasilitas yang ada maka secara praktis pekerjaan dari lembaga atau siapapun yasng menggunakan komputer menjadi terhenti. Untuk menanggulangi kejahatan komputer yang semakin canggih terhadap kedua aspek tersebut sejumlah Negara telah menyempurnakan hukum pidana mengenai kejahatan komputer, antara lain dengan mengatur definisi tentang barang (property) sehingga meliputi pula:

1. "intangible goods" seperti:
    - system komputer,
    - jaringan komputer,
    - piranti lunak (software) dan
    - data, dan
2. penggunaan komputer, termasuk penggunaan
    - data komputer,

- system komputer,
- jaringan komputer,
- piranti lunak atau data.

Dengan penyempurnaan tersebut segala bentuk kejahatan komputer diharapkan dapat dituntut berdasarkan dalam ketentuan ini.
Berikut ini contoh beberapa penyempurnaan undang-undang hukum pidana yang dilakukan oleh beberapa Negara.

Dengan penyempurnaan tersebut segala bentuk kejahatan komputer diharapkan dapat dituntut berdasarkan dalam ketentuan ini.
Berikut ini contoh beberapa penyempurnaan undang-undang hukum pidana yang dilakukan oleh beberapa Negara.

I. AMANDEMEN US FEDERAL PENAL CODE

Pemerintah Federal Amerika Serikat telah menyempurnakan pasal-pasal Penal Code yang berkaitan dengan kejahatan komputer sehingga berbagai jenis kejahatan komputer yang canggih diharapkan dapat dipidana berdasarkan ketentuan ini.

Chapter 33 tentang Computer Crimes mengatur:

Definisi:

(1) "Akses" berarti mendekati, memerintahkan, berhubungian dengan., menyimpan data, menelusuri atau menyadap data dari, merubah data atau piranti lunak komputer di dalam, atau perbuatan lainnya menggunakan sumber komputer apapun, jaringan komputer, program komputer atau sistem komputer.

(2) Jumlah keseluruhan berarti jumlah :
   (a) kerugian langsung atau tidak langsung yang diderita korban, termasuk nilai uang, barang, atau jasa yang dicuri atau menyebabkan tidak dapat dipulihkan kembali oleh karena pelanggaran tersebut; atau
   (b) setiap pengeluaran yang diperlukan oleh korban untuk menjaga agar suatu komputer, jaringan komputer, program komputer, atau system komputer tidak dirubah, diambil, dirusak, dihapus, atau diganggu oleh tindakan jahat.

(3) Yang dimaksud dengan "Pembawa komunikasi umum"*(communication common carrier)* ialah seorang yang memiliki atau mengoperasikan suatu system telepon di Negara ini yang meliputi perlengkapan atau

fasilitas untuk pengiriman, transmisi, atau penerimaan komunikasi dan yang menerima imbalan dari orang yang menggunakan system itu.

(4) Yang dimaksud dengan "Komputer" ialah alat elektronis, magnetis, optik, kimia-elektris (electrochemical), atau alat pemroses data yang cepat yang menghasilkan fungsi logis, aritmatik, atau penyimpanan dengan memanipulasikan denyut elektronis atau magnit dan meliputi semua fasilitas masuk (input), keluar (output), pemrosesan, penyimpanan, atau komunikasi yang dihubungkan atau dikaitkan kepada alat tersebut.

(5) Yang dimaksud dengan "Jaringan komputer" ialah interkoneksi dari dua atau lebih komputer atau system komputer dengan satelit, microwave, hubungan, atau sarana komunikasi dengan kemampuan untuk mengirimkan informasi diantara komputer tersebut.

(6) Yang dimaksud dengan "program komputer" ialah sejumlah data yang teratur yang mengandung instruksi-instruksi yang berkode atau keterangan yang apabila dioperasikan oleh komputer menyebabkan komputer memproses data atau melaksanakan fungsi-fungsi tertentu.

(7) Yang dimaksud dengan "jasa komputer" (computer service) ialah hasil dari produksi penggunaan satu komputer, informasi yang disimpan dalam komputer, atau orang yang menjalankan komputer, termasuk waktu penggunaan komputer, pemrosesan data, dan fungsi-fungsi penyimpanan.

(8) Yang dimaksud dengan "system komputer" ialah setiap macam kombinasi dari satu komputer atau jaringan komputer dengan dokumentasi, piranti lunak komputer, atau fasilitas fisik yang mendukung komputer atau jaringan komputer.

(9) Yang dimaksud dengan "piranti lunak komputer" – computer software – ialah seperangkat program komputer, prosedur, dan dokumen yang tergabung yang penting bagi jalannya atau berfungsinya suatu komputer, system komputer, atau jaringan-komputer.

(10) Yang dimaksud dengan "virus komputer" ialah program komputer atau sejumlah instruksi yang tidak dikehendaki (unwanted) yang dimasukkan kedalam satu memori computer, system operasi, atau program komputer yang sengaja dibuat dengan kemampuan untuk menggandakan dirinya atau mempengaruhi program-program lain atau arsip-arsip dalam komputer dengan menempelkan satu program atau sejumlah instruksi lainnya yang tidak dikehendaki ke satu atau lebih program komputer atau arsip.

(11) Yang dimaksud dengan "data" ialah kumpulan (representation) informasi, ilmu, fakta-fakta, konsep-konsep, atau instruksi-instruksi yang sedang disiapkan atau telah disiapkan dengan cara yang resmi, dan dimaksudkan untuk disimpan atau diproses, sedang disimpan atau sedang diproses, atau telah disimpan atau diproses dalam satu komputer. Data

dapat dipersonifikasikan (embodied) dalam bentuk apapun, termasuk tetapi tidak terbatas kepada hasil cetakan komputer, media penyimpan magnetis, media penyimpan laser, dan lubang-lubang, atau dapat disimpan tersendiri dalam memori computer.

(12) Yang dimaksud dengan "persetujuan efektif" termasuk persetujuan oleh orang yan secara resmi berwenang untuk bertindak atas nama pemilik. Suatu persetujuan tidak efektif apabila:

- digerakan oleh suatu tipuan, seperti diatur dalam Seksi 31.01, atau digerakkan dengan paksa;
- diberikan oleh orang yang diketahui sipelaku bahwa orang itu tidak secara resmi diberi wewenang untuk bertindak atas nama sipemilik.
- diberikan oleh seorang yang dengan alasan usia muda, sakit jiwa atau kelainan jiwa, atau dalam pengaruh intoksikasi diketahui oleh si pelaku bahwa orang itu tidak boleh membuat keputusan tentang kepemilikan;
- diberikan khusus untuk mengetahui pelaksanaan suatu pelanggaran; atau
- digunakan untuk tujuan lain daripada tujuan yang telah diberikan.

(13) Yang dimaksud dengan "Penggunaan elektris" ialah seperti yang dimaksud oleh Seksi 31.002, Utilities Code.

(14) Kerugian (harm) termasuk sebagian atau seluruh perubahan, kerusakan, atau penghapusan data yang tersimpan, interupsi jalannya komputer, pemasukan virus komputer, atau kerugian lainnya, ketidakmanfaatan, atau luka yang mungkin secara wajar yang diderita sebagai akibat dari perbuatan sipelaku.

(15) Pemilik ialah orang yang:

- Mempunyai hak atas barang, kepemilikan barang, apakah secara sah atau tidak, atau suatu hak kepemilikan barang yang lebih tinggi dari sipelaku.
- Mempunyai wewenang untuk membatasi hak untuk masuk ke barang; atau
- Memiliki hak (lisensi) atas data atau piranti lunak komputer.

(16) Yang dimaksud dengan "barang" (property) ialah:

- barang pribadi yang bersifat "tangible" termasuk komputer, system komputer, jaringan komputer, piranti lunak komputer, atau data; atau
- pemakaian komputer, system komputer, jaringan komputer, piranti lunak komputer atau data.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, § 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.
Amended by Acts 1997, 75th Leg., ch. 306, § 1, eff. Sept. 1, 1997; Acts 1999, 76th Leg., ch. 62, § 18.44, eff. Sept. 1, 1999.

II. PELANGGARAN PENGAMAN KOMPUTER

(a) Seseorang melakukan suatu pelanggaran apabila orang itu mengetahui memasuki satu komputer, jaringan komputer, atau system komputer tanpa persetujuan efektif dari pemilik.

(b) Suatu pelanggaran dalam seksi ini merupakan pelanggaran Kelas B kecuali apabila waktu melakukan pelanggaran sipelaku mengetahui mendapat keuntungan itu dengan menipu atau merugikan orang lain, atau merubah, merusak, atau menghapus barang, dimana pelanggaran itu termasuk:
   (1) Pelanggaran Kelas B apabila jumlah kerugian kurang dari $1,500.
   (2) Kejahatan bisa dimasukan penjara apabila:
      - jumlah kerugian $1.500.atau lebih tetapi kurang dri $20,000.; atau
      - jumlah kerugian kurang dari $1,500. dan terdakwa telah dihukum dua atau lebih sebelumnya karena melakukan pelanggaran berdasarkan bab ini;
   (3) melakukan kejahatan tingkat tiga apabila jumlah kerugian $20.000. atau lebih akan tetapi kurang dari $100,000.
   (4) melakukan suatu kejahatan tingkat pertama apabila jumlah kerugian $200,000. atau lebih.

(c) Apabila keuntungan yang diperoleh dengan jalan menipu korban atau merugikan korban, atau barang dirubah, dirusak, atau dihapus yang bertentangan dengan seksi ini, yang dilakukan apakah secara tunggal, kelakuan dapat dipertimbangkan sebagai suatu pelanggaran dan nilai keuntungan yang diperoleh dan kerugiaan yang timbul yang disebabkan oleh penipuan, merugikan, atau merubah, merusak, atau menghapus barang boleh dihitung dalam menentukan tingkatan pelanggaran.

(d) Seseorang yang merupakan subjek penuntutan menurut seksi ini dan seksi lainnya dari undang-undang ini boleh dituntut oleh salah satu atau kedua seksi tersebut.

Beberapa pasal amandemen penal code tersebut mulai efektif September 1, 2001.

Faktor Pemaaf

Merupakan factor pemaaf mutlak terhadap penuntutan berdasarkan Section 33.02 bahwa pelaku adalah pejabat, pegawai, atau agen dari pejabat umum komunikasi atau pemanfaatan listrik (electric utility) dan melakukan perbuatan yang disebutkan di atas dalam rangka pekerjaan waktu melaksanakan suatu aktivitas yang memerlukan kejadian dalam pelaksanan tugas atau terhadap dalam pelaksanan tugas atau terhadap perlindungan hak-hak atau kepemilikan dari pejabat umum komunikasi atas pemanfaatan listrik.

III. PENAL CODE NEGARA BAGIAN CALIFORNIA – PASAL 502

Beberapa model Penal Code Kejahatan Komputer untuk Negara bagian telah disusun untuk menanggulangi berbagai bentuk kejahatan komputer yang berkembang. Salah satu model Penal Code California berbunyi sebagai berikut:

Pasal 502 berisi ketentuan tentang apa yang termasuk kejahatan komputer sebagai berikut:

> *Merupakan kejahatan seseorang yang dengan sepengetahuannya memasuki dan tanpa ijin merubah, merusak, menghapus, menghancurkan, atau penggunaan lainnya setiap data, komputer, system koputer, atau jaringan komputer dengan maksud untuk menipu, membohongi (deceive), atau memeras, atau dengan melawan hukum menguasai atau memperoleh uang, barang, atau dengan melawan hukum memasuki dan tanpa ijin mengambil, mengkopi, atau menggunakan setiap data dari suatu komputer, system komputer, atau jaringan komputer, atau dengan sepengatahuannya memasuki dan tanpa ijin menambah, merubah, merusak, menghapus, atau merusak setiap data, piranti lunak, atau program, atau sepengetahuannya dan tanpa ijin mengganggu atau menyebabkan terganggu jasa komputer, atau dengan sepengetahuannya dan tanpa ijin memberikan atau membantu memberikan sarana untuk memasuki suatu komputer, sistem komputer, atau jaringan komputer atau memasukan kontaminan komputer.*

a. Pengertian

Pasal 502 berisi pula definisi atau penjelasan tentang hal-hal yang berkaitan dengan "komputer", seperti: akses, jaringan komputer, program atau software komputer, jasa komputer, system komputer, data, dokumen pendukung, kerugian, biaya yang dikeluarkan korban, kontaminan

komputer (computer contaminant), yang pada dasarnya sama yang diatur dalam Federal Penal Code.

b. Peraturan Perguruan Tinggi tentang Kejahatan Komputer yang mengacu ke California Penal Code

Mengingat banyaknya ekperimen yang dilakukan oleh mahasiswa antara lain untuk memasuki system komputer yang dimiliki oleh institusi Negara maupun swasta dan perguruan tinggi yang seringkali merusak atau mengganggu jalannya system dan data komputer yang bersangkutan, beberapa Negara bagian telah mengeluarkan ketentuan pidana yang melarang perbuatan "hacking" tersebut. Dengan dasar ketentuan undang-undang hukum pidana tersebut Perguruan Tinggi mempunyai kewajiban untuk mengatur lebih lanjut penggunaan komputer oleh mahasiswa yang melarang memasuki komputer tanpa ijin..

Salah satu ketentuan telah dikeluarkan oleh California Polytechnic State University, yaitu yang berupa Administrative Bulletin 90-3. Bulletin ini dikeluarkan sebagai pengaturan lebih lanjut dari Senate Bill 304 (Computer Crime) dalam Chapter 1076 yang dimasukkan dalam Penal Code California. Pasal tersebut mengatur bahwa:

> *Komunitas perguruan tinggi, universitas Negara bagian, atau lembaga pendidikan di Negara bagian ini diwajibkan untuk memasukan dalam peraturan (universitas) tentang pelanggaran yang berkaitan dengan penggunaan komputer sebagai suatu pelanggaran khusus terhadap kebijaksanaan, dan peraturan tentang tingkah laku mahasiswa perguruun tinggi yang dapat dijadikan alasan untuk menjatuhkan tindakan disiplin.*

Dengan dasar Penal Code Pasal 502 dan ketentuan Universitas tercantum dalam Administrative Bulleting 90-03 dikeluarkan peraturan intern universitas yang menyatakan bahwa:

> *Merupakan perbuatan melawan hukum barang siapa dengan sengaja memasuki dan tidak mendapat ijin merubah, mengkopi, merusak, menghapus, merusak, atau penggunaan lainnya terhadap data komputer apapun, system komputer, atau jaringan komputer dengan maksud untuk menipu, mengelabui, atau memeras, atau secara salah menguasai atau memperoleh uang, barang, piranti lunak, atau data atau memasukan kontaminasi (virus) kedalam komputer.*

Aktivitas tersebut dapat mengakibatkan penindakan disiplin oleh universitas, tuntutan hukum, termasuk denda dan/atau pemenjaraan, dan/atau penuntutan oleh korban kejahatan komputer dengan dasar kerugian yang diderita.

Setiap perbuatan ilegal itu tersebut diatas dapat mengakibatkan tindakan disiplin, dan/atau denda, penjara, dan/atau gugatan perbuatan melawan hukum oleh korban.....

IV. TEXAS COMPUTER CRIMES LAW

Amandemen Computer Crimes Law ini pada pokoknya hampir sama dengan Federal Penal Code tentang Computer Crimes.:

Pada tahun 1985, Undang-undang Kejahatan Komputer untuk negara bagian Texas mulai diberlakukan, yang berbunyi:

It is a crime to make unauthorized use of protected computer systems or data files on computers, or to make intentionally harmful use of such computers or data files. The seriousness of such a crime ranges from Class B misdemeanor to third-degree felony.
(Di bawah undang-undang negara ini, penggunaan sistem komputer data file yang dilindung pada komputer secara tidak sah, atau secara sengaja penggunaan komputer atau file data yang merugikan dinyatakan sebagai suatu kejahatan. Keseriusan dari kejahatan seperti itu mulai dari pelanggaran hukum ringan kelas B sampai kejahatan pidana tingkat-tiga).

Texas Computer Crimes Statute

Teks lengkap pasal undang-undang kejahatan komputer (Penal Code) seperti di bawah ini. (terjemahan bebas)

Undang-Undang Kejahatan Komputer TEXAS

Bagian 1 Judul 7. Bab 33. Kitab Undang-Undang Hukum Pidana Texas.

Pasal 33.10. Definisi. Di dalam bab ini:

(1) Penyampaian sarana komunikasi' berarti seseorang yang memiliki atau mengoperasikan suatu sistem telepon di negara ini yang termasuk peralatan atau fasilitas untuk pengantaran, transmisi, atau penerimaan komunikasi dan yang menerima kompensasi dari orang-orang yang menggunakan sistem tersebut.

(2) 'Komputer' berarti suatu alat elektronik yang melaksanakan fungsi logika, aritmatika, atau fungsi memori dengan manipulasi elektronik atau denyut magnetis, dan termasuk semua input, output, pengolahan, penyimpanan, atau fasilitas komunikasi yang dihubungkan atau terhubung dengan alat. 'Komputer' termasuk suatu jaringan dari dua atau lebih komputer yang saling berhubungan untuk berfungsi atau berkomunikasi bersama-sama.

(3) 'Program komputer' berarti berbagai data yang diatur yang merupakan perintah atau pernyataan yang dikodekan yang ketika dieksekusi oleh suatu komputer menyebabkan komputer untuk memproses data atau melaksanakan fungsi spesifik.

(4) 'Sistem keamanan komputer' berarti rancangan, prosedur, atau langkah-langkah lain sehingga orang yang bertanggung jawab untuk mengoperasikan dan menggunakan suatu komputer, bekerja untuk membatasi penggunaan komputer untuk orang-orang atau penggunaan tertentu bahwa pemilik atau pemilik lisensi dari data yang disimpan atau dirawat oleh suatu komputer di mana pemilik atau pemilik lisensi berhak untuk menyimpan atau memelihara data bekerja untuk membatasi akses pada data.

(5) 'Data' berarti suatu representasi informasi, pengetahuan, fakta, konsep, atau instruksi yaitu disiapkan atau telah disiapkan dengan cara tersusun dan dimaksudkan untuk disimpan atau diproses, disimpan atau diproses, atau sedang disimpan atau telah diproses di dalam suatu komputer.

Data mungkin dibuat di dalam suatu bentuk, termasuk tetapi tidak terbatas pada hasil print komputer, media penyimpanan magnetis, dan kartu pos, atau mungkin disimpan secara internal di dalam memori komputer tersebut.

(6) 'Utiliti listrik' mempunyai arti dijelaskan oleh Subbagian (c), Pasal 3, UU Pengaturan Utiliti Umum (Pasal 1446c, Undang-Undang Sipil Vernon Texas).

Pasal 33.02.Pelanggaran atas keamanan komputer

(a) Seseorang melakukan suatu pelanggaran jika orang tersebut :

(1) menggunakan suatu komputer tanpa persetujuan yang berlaku dari pemilik komputer atau seseorang yang diberi hak akses lisensi pada komputer dan pelaku mengetahui bahwa ada suatu sistem keamanan komputer yang dimaksudkan mencegah dia melakukan penggunaan komputer; atau"

(2) mendapat akses ke data yang disimpan atau yang dijaga oleh suatu komputer tanpa persetujuan yang berlaku dari pemilik atau pemegang lisensi untuk data tersebut dan pelaku mengetahui bahwa ada suatu sistem keamanan komputer yang dimaksudkan mencegahnya untuk memperoleh akses untuk data tersebut.

(b) Seseorang melakukan suatu pelanggaran jika orang tersebut dengan sengaja atau dengan sadar memberi suatu kata sandi, mengidentifikasi kode, nomor identifikasi pribadi, atau informasi rahasia lainnya mengenai suatu sistem keamanan komputer kepada orang lain tanpa persetujuan yang berlaku dari orang yang menggunakan sistem keamanan komputer untuk membatasi penggunaan dari suatu komputer atau untuk membatasi akses ke data yang disimpan atau dirawat oleh suatu komputer.

(c) Suatu pelanggaran di bawah bagian ini adalah suatu pelanggaran hukum ringan kelas A.

Pasal 33.03. Akses yang merugikan

(a) Seseorang melakukan suatu pelanggaran jika orang tersebut dengan sengaja atau dengan sadar:

(1) menyebabkan suatu komputer menjadi tidak berfungsi atau mengganggu operasi suatu komputer tanpa persetujuan yang berlaku dari pemilik komputer atau seseorang yang diberi hak atas akses lisensi komputer; atau

(2) mengubah, merusak, atau menghancurkan data atau suatu program komputer yang disimpan, dirawat, atau yang diproduksi oleh suatu komputer, tanpa persetujuan yang berlaku dari pemilik atau pemegang lisensi dari data atau program komputer tersebut.

(b) Suatu pelanggaran di bawah pasal ini adalah:

(1) suatu pelanggaran hukum ringan kelas B jika perbuatan tersebut tidak menyebabkan suatu kerugian atau kerusakan atau jika nilai dari kerugian atau kerusakan disebabkan oleh perbuatan tersebut adalah kurang dari $200;
(2) suatu pelanggaran hukum ringan kelas A jika nilai dari kerugian atau kerusakan disebabkan oleh perbuatan tersebut adalah $200 atau lebih tetapi kurang dari $2,500; atau
(3) suatu kejahatan pidana tingkat-tiga jika nilai dari kerugian atau kerusakan yang disebabkan oleh perbuatan tersebut adalah $2,500 atau lebih.

Pasal 33.04. Pelanggaran.

Sebagai suatu pelanggaran dapat dituntut dibawah Pasal 33.02 dan 33.03 dari UU ini bahwa pelaku adalah seorang petugas, karyawan, atau agen dari suatu penyedia sarana komunikasi atau utilitas listrik dan melakukan tindakan atau tindakan-tindakan yang dilarang selama bekerja; atau terlibat di dalam suatu kegiatan yang perlu untuk penyampaian pelayanan atau untuk perlindungan dari hak-hak atau pemilikan dari penyampaian sarana komunikasi atau utilitas listrik.

Pasal 33.05. Bantuan oleh Jaksa Agung

Jaksa agung, jika diminta untuk melakukan demikian oleh seorang jaksa penuntut umum, dapat membantu jaksa penuntut umum di dalam menyelidiki atau penuntutan dari suatu pelanggaran di bawah bab ini atau suatu pelanggaran lain yang melibatkan penggunaan suatu komputer."

V. INDIAN - ELECTRONIC COMMERCIAL ACT – 1998

India telah menyempurnakan Penal Code dengan mengeluarkan Electronic Commercial Act – 1998, agar dapat mencangkup beberapa jenis kejahatan komputer baru dan kejahatan dalam tata-niaga elektronis. Penyempurnaan dimasukkan dalam Part XII tentang Computer Crime yang berbunyi:

Computer Crime.

Untuk tujuan Undang-undang ini, barang siapa yang melakukan salah satu dari perbuatan-perbuatan tersebut di bawah ini bersalah melakukan kejahatan komputer :

(a) Dengan sengaja memasuki, merusak atau menyembunyikan, atau mencoba untuk memasuki, merusak, astau menyembunyikan, baik sementara atau untuk selamanya, setiap data base, komputer, system informasi atau jaringan komputer, tanpa ijin dari pemilik, dengan maksud apakah:
    (i) secara melawan hukum menguasai, memperoleh, menggunakan atau menghalangi orang lain untuk memperoleh uang, barang, data atau catatan elektronis;
    (ii) mengkopi atau merusak setiap data atau catatan elektronis;
    (iii) menggunakan atau mengganggu setiap fungsi komputer, jaringan komputer, atau system informasi; atau
    (iv) melakukan setiap perbuatan yang merupakan pelanggaran dalam Undang-undang Hukum Pidana India.
(b) Dengan sepengetahuannya dan dengan maksud untuk menipu, memperoleh atau mencoba untuk memperoleh setiap jasa komputer dengan memberikan indentitas palsu, keterangan palsu atau tanpa hak membebankan biaya kepada orang lain, dengan memasang atau menempelkan dengan setiap fasilitas atau perlengkapan, atau dengan cara-cara lainya.
(c) Dengan sengaja atau secara tidak hati-hati memasukkan atau membiarkan masuknya virus komputer ke dalam komputer, system komputer atau jaringan komputer tanpa ijin sipemilik.

Dengan diundangkannya seksi baru diharapkan bahwa perbuatan yang beraneka ragam dapat yang merugikan dapat dianggap sebagai kejahatan komputer. Pengundangan ini dimaksud sebagai penambahan atas Indian Penal Code, 1860, yang sudah mencantumkan beberapa bentuk kejahatan yang melalui atau berkaitan dengan komputer. Dengan undang-undang ini setiaap kejahatan yang diatur dalam Penal Code yang berkaitan dengan komputer disebut kejahatan komputer.

Dijelaskan pula bahwa beberapa kejahatan yang termasuk dalam kejahatan komputer namun tidak jelas pengaturannya dalam Penal Code, seperti memasukkan virus, pengganggguan terhadap jalannya komputer, dan penipuan untuk mendapatkan jasa komputer, dapat dimasukan dalam amandemen ini.

Selain itu dengan undang-undang ini dapat dipidana perbuatan mengintervensi hak orang lain atas uang tunai – cybercash- melalui jaringan "cyber", dan barang-barang digital (digital goods) yang tidak terjangkau oleh Penal Code. Demikian pula, tanpa hak mengkopi, menguasai atau merusak

"barang intangijble" (data, catatan elektronis) yang tidak dapat dituntut berdasarkan Penal Code, dapat dituntut berdasarkan undang-undang baru ini.

Sanksi pidana

Dengan telah diaturnya beberapa kejahatan komputer jenis baru, maka sanksi pidana yang diaturpun menjadi bervariasi pula, tergantung berat ringannya tindak pidana, yang berkisar antara pidana penjara sampai dengan 3 tahun atau denda sampai dengan Rs.5,00.00 atau keduanya.

Penyitaan

Setiap keuntungan (uang atau barang) yang merupakan hasil kejahatan dan alat yang dipegunakan untuk melakukan kejahatan harus disita.

Kejahatan komputer merupakan bahaya besar oleh karena langsung atau tidak langsung dapat merugikan kepentingan negara dan masyarakat mengingat besarnya kepentingan yang tergantung pada sistim komputer, oleh karena itu harus selalu diwaspadai. Untuk memberantasnya antara lain dapat dilakukan dengan menyempurnakan peraturan perundang-undangan pidana yang berlaku agar dapat menjangkau semua jenis kejahatan komputer.

Bentuk atau tata-cara penyusunan undang-undang mengenai kejahatan komputer yang dibuat oleh beberapa negara dapat dibagi atas 4 kelompok pendekatan, yaitu:

1. Pendekatan melalui penyempurnaan ketentuan tentang barang atau hak-milik ('property approach');

   Sebagai dasar pertimbangan ialah bahwa hak-hak mengenai kebendaan yang berupa 'tangible object' berlaku juga bagi data komputer. Pendekatan ini dilakukan oleh Pemerintah Federal Amerika Serikat dan negara-negara bagian di Amerika Serikat yang dalam undang-undang baru memperluas pengertian "article' atau 'property' atau 'thing of value' meliputi juga 'data komputer' atau 'electronic impulses', jaringan komputer, system komputer, program komputer, dan lainnya.

   Sedangkan pengertian "computer" diperluas sehingga termasuk semua piranti lunak dan fasilitas yang berkaitan.

2. Pendekatan melalui penyempurnaan ketentuan tentang pemalsuan (forgery approach);

   Pendekatan ini menekankan pentingnya 'integritas' data, oleh karena itu diadakan penyempurnaan atas ketentuan mengenai pemalsuan, misalnya terhadap 'instrument' yang diperluas sehingga meliputi 'electronic impulses'. Pendekatan ini dilakukan antara lain oleh Inggris dan Canada.

3. Pendekatan melalui penyempurnaan ketentuan tentang 'informasi' (information approach);

Pendekatan ini menekankan pentingnya rahasia 'informasi', oleh karena itu setiap perbuatan penyalahgunaan rahasia yang terkandung dalam data komputer harus dilarang.
Negara-negara yang menggunakan pendekatan ini pada umumnya ialah negara-negara Skandinavia (Norwegia, Denmark dan Finlandia.)

4. Pendekatan gabungan (mixed approach)

Pendekatan ini menggabungkan ketiga pendekatan diatas, yaitu dengan menambah/menyisipi beberapa kata-kata atau kalimat dalam ketentuan yang berlaku, dan pengaturan. Dengan makin bertambahnya perbuatan-perbuatan penyalahgunaan komputer yang harus dipidana, sekarang lebih banyak negara yang condong untuk mengikuti pendekatan ini. Sebagai contoh undang-undang atau rencana undang-undang yang melakukan pendekatan ini ialah Rencana Undang-Undang yang diusulkan Komisi Franken.

Pelaku kejahatan komputer sebagian besar adalah mereka yang 'berkerah putih' dengan tingkat pendidikan dan intelegensi yang tinggi sehingga mempersulit usaha untuk melacaknya. Kasus-kasus yang terjadi membuktikan bahwa seringkali kejahatan komputer dilakukan oleh organisasi kejahatan internasional.

Kerugian yang disebakan kejahatan komputer jauh lebih besar daripada yang dilakukan dengan kejahatan tradisionil, oleh karena itu perlu meningkatkan kewaspadaan mereka yang banyak menggunakan komputer.

Sebagai negara yang memasuki ambang teknologi komputer, Indonesia perlu meninjau kembali perundang-undangan pidana yang berlaku, dan sedapat mungkin memperhatikan perundang-undangan yang telah dibuat oleh beberapa negara, mengingat dalam hal-hal tertentu kejahatan komputer berdampak internasional, sehingga dapat menghindari perlindungan bagi kejahatan komputer tertentu.

Tim penyusunan 'Naskah Akademis Peraturan Perundang-undangan tentang Penanggulangan Kejahatan Komputer' yang dibentuk oleh Badan Pembinaan Hukum Nasional, Departemen Kehakiman, menyebut dua kendala yang menyangkut keterbatasan jangkauan KUHPidana, yaitu:

- salah satu norma atau larangan yang terdapat dalam KUHP tidak menjangkau kemampuan teknologi atau adanya kebijaksanaan baru yang dirasa norma atau larangan yang ada dalam KUHP tersebut

belum dapat mendukung lajunya pembangunan dan teknologi. Selain daripada itu perlu peningkatan kerjasama internasional agar kejahatan komputer dapat diberantas secara efektip.

- tidak terdapat norma atau larangan adanya tindak pidana baru akibat meningkatnya teknologi maju, sehingga KUHP seakan-akan bersifat pasif terhadap perkembangan teknologi. Halaman 57 butir 16.1. dan 16.2.

BAB V
ANALISIS DAN TABULASI

A. ANALISIS

Perkembangan tehnologi sekarang ini, telah memungkinkan dilakukannya hubungan bisnis melalui perangkat tehnologi yang disebut dengan *internet.* Perkembangan tehnologi tersebut telah menimbulkan paradigma baru dalam melakukan kontrak di antara pelaku bisnis. Secara konvensional, pelaku bisnis dalam membuat suatu kontrak atau transaksi mangadakan pertemuan secara *face to face* lalu membubuhkan tanda tangan sebagai pertanda penerimaan kesepakatan yang tertuang dalam *contract* tersebut. Namun dengan perkembangan tehnologi, pihak-pihak yang terkait dalam suatu transaksi tidak perlu lagi bertemu secara *face to face,* cukup melalui peralatan komputer dan telekomunikasi, transaksi yang demikian ini lebih dikenal dengan transaksi *e-commerce.*

Disatu sisi tehnologi komputer dan telekomunikasi mempunyai dampak positif dimana para pelaku bisnis lebih mudah dalam menjalankan usahanya, karena dapat menghemat waktu dan tenaga. Namun disisi lain tehnologi ini menimbulkan dampak negatif dimana pihak-pihak tertentu dengan itikad tidak baik mencari keuntungan dengan melawan hukum (cybercrime). Paradigma baru dalam bisnis tersebut secara serta merta juga mempengaruhi peraturan hukum yang berlaku baik domestik maupun internasional dan baik di bidang perdata maupun pidana. Hukum atau peraturan sebagai pedoman perdagangan secara e-commerce ini telah dibuat oleh lembaga-lembaga internasional antara lain:[81] United Nations Commission on International Trade Law (UNCITRAL) yang mengatur tentang : Kelompok Kerja untuk Perdagangan Elektronik (e-commerce) yang selanjutnya disebut sebagai UNCITRAL, Model Undang-undang Perdagangan Elektronik UNCITRAL 1996, Model Undang-undang tanda tangan elektronik *(electronic signiture)* UNCITRAL 2001

European Union yang mengatur tentang Petunjuk 2000/31/EC tentang Petunjuk mengenai Perdagangan Elektronik, Petunjuk 1999/93/EC tentang Petunjuk mengenai Tanda Tangan Elektronik, Petunjuk 95/46EC tentang Petunjuk Perlindungan tanggal.

Organisation for Economic Co-operation and Development (OECD) yang mengatur tentang Rencana Aksi OECD untuk Perdagangan Elektronik 1998, Panduan Kerahasiaan 1980, Panduan Sistem Keamanan Informasi 1992, Panduan Sistem Kriptografi 1997 dan Panduan Perlindungan Konsumen 1999.

International Chamber of Commerce (ICC) yang mengatur tentang Rencana Aksi untuk perdagangan Elektronik se-dunia, Peraturan Standar

[81] Makalah, *E-Commerce,* Indonesian Judicial Training Program, 6-10 January 2003, Singapore

mengenai Tata Cara Lalu lintas Data Perdagangan melalui teletransmisi, Penggunaan Umum untuk Perdagangan Internasional yang dijamin secara digital 1997, Model Ketentuan Kerahasiaan untuk lalu lintas data lintas negara.

Word Trade Organitation (WTO) yang mengatur tentang Program Kerja. Asia Pacific Economic Co-operation (APEC) yang mengatur tentang Satuan Tugas Perdagangan Elektronik, Makalah-makalah, Proyek-proyek dan Kelompok kerja Telekomunikasi dan Informasi.

Negara-negara asing juga telah mengeluarkan peraturan tentang e-commerce misalnya Australia yang disebut dengan Commonwealth Electronic Transaction Act 1999,[82] Singapore yang disebut dengan Electronic Transaction Act of Singapore dan juga di Malaysia dengan undang-undang sejenis.[83]

Indonesia sampai sekarang ini belum mempunyai Undang-undang yang mengatur tentang e-commerce dan cyber crime meskipun dalam transaksi perdagangan di Indonesia sudah umum dan tidak asing lagi mempergunakan elektronik, dan malah sudah sering menimbulkan perkara di bidang perdata maupun pidana. Oleh karena itu secara umum penyelesaian perkara-perkara dengan litigasi yang berhubungan dengan e-commerce dan cybercrime masih mempergunakan dan berpedoman KUHPerdata dan KUHPidana. Namun secara khusus sebenarnya hal ini sudah diatur, misalnya dalam peraturan perundang-undangan tentang hak kekayaan intelektual yaitu UU no. 19 tahun 2002 tentang hak cipta, UU no. 15 tahun 2001 tentang merk, UU no. 14 tahun 2001 tentang paten, UU no. 32 tahun 2000 tentang disain tata letak sirkuit terpadu, UU no. 31 tahun 2000 tentang disain industri, UU no. 30 tahun 2000 tentang rahasia dagang UU no. 36 tahun 1999 tentang telekomunikasi, Keputusan Menteri Perhubungan no. KM.21 tahun 2001 tentang penyelenggaraan jasa telekomunikasi, Keputusan Menteri Perhubungan no. KM 23 tahun 2002 tentang penyelenggaraan jasa internet telepon. Dan sekarang ini telah dirampungkan beberapa rancangan peraturan misalnya Rancangan UU tentang pidana kejahatan teknologi informasi, Rancangan UU tentang tanda tangan elektronik dan transaksi elektronik, Rancangan Keputusan Dirjen tentang persyaratan teknis perangkat ADSL (Asymetric, Digital, Subscriber Line)

Dibawah ini akan dianalisis hasil kuestioner penelitian E-commerce dan cybercrime.

A. Electronic/cyber dan Hakim

Tabel 1 menunjukkan bahwa 70 % lebih responden sama sekali belum pernah menggunakan *internet* dan hanya hampir 15% responden yang pernah menggunakan *internet* beberapa kali.[84] Juga responden sebanyak hampir 62%

---

[82] ibid

[83] Niniek Suparni, *Masalah Cyberspace Problematika Hukum dan Antisipasi Pengaturannya*, Fortun Mandiri Karya, Jakarta cet pertama, Februari 2001, hal 71

[84] lihat tabel 1

tidak pernah mempelajari dan tidak memahami tentang e-commerce, dan hampir 35% responden yang pernah mempelajari e-commerce tapi kurang memahaminya.[85] Hal ini memang sangat memprihatinkan, namun sebenarnya ini disebabkan tidak adanya tantangan untuk para responden untuk mempelajari e-commerce tersebut, terlihat dari tabel 3 dimana 97% lebih responden tidak pernah menangani perkara perdata atau pidana yang berhubungan dengan e-commerce.

Sebenarnya tahun 1982 kejahatan komputer dan cyber telah menarik perhatian masyarakat, dimana terjadi penggelapan dan pencurian dibeberapa Bank malah pada tahun 2000 kejahatan *cyber (cyber crime)* marak dilima kota besar Indonesia dan dalam taraf yang cukup mengkhawatirkan.[86] Penggelapan uang di bank BRI Yogjakarta melalui komputer yaitu dengan cara mentransfer uang melalui kliring kemudian warkat kliring yang diterima dari kliring tersebut oleh oknum pegawai BRI secara melawan hukum dan tanpa sepengetahuan bagian kartu dibebankan kepada rekening orang lain, bukan rekening yang tertulis pada warkat kliring dengan cara membukukan melalui komputer tanpa kartu atau struk mesin (Putusan Mahkamah Agung No 363 K/Pid/1984 tanggal 25 Juni 1984)[87]

Juga kasus pembobolan BNI cabang New York yaitu kasus seorang pegawai yang pernah bekerja di BNI cabang New York sejak tahun 1980 sampai dengan september 1985. Kasusnya, pada waktu masih bekerja yang bersangkutan bertugas sebagai operator komputer untuk mengakses *Citybank New York* atau *Mantrust New York,* oleh karenanya yang bersangkutan memegang *password* dengan kode tertentu. Pada tanggal 31 Desember 1986, yang bersangkutan bekerjasama dengan orang lain berhasil mengoperasikan komputer di sebuah hotel untuk melakukan transfer ke rekening bank tertentu, yaitu dengan menggunakan *USER ID* dan *password enter* dengan melawan hukum. Prosesi tersebut dimulai dengan memerintahkan *Citybank New York* untuk mentransfer dana atas beban rekening BNI kepada rekening BNI di *Mantrust.* Dari sini kemudian yang bersangkutan mentransfer dana ke beberapa bank lainnya untuk keuntungan sendiri.[88]

Kasus mutasi kredit fiktif melalui komputer BDN Cabang Jakarta Bintaro Jaya, dilakukan oleh terdakwa dengan mempersiapkan beberapa rekening untuk menampung mutasi tanpa nota (fiktif), baik dengan cara mempergunakan rekening milik orang lain (dengan persetujuan nasabah) maupun mengaktifkan rekening yang tidak aktif, yang berlangsung 20 Juli 1988 sampai dengan Januari 1989.[89]

---

[85] lihat tabel 2
[86] Niniek Suparni, *op.cit.*, hal 16
[87] ibid hal 12
[88] Ibid hal 13
[89] ibid hal 15

Kasus pemalsuan/pencurian di Bank Danamon Pusat tahun 1998 yang melibatkan terdakwa BH secara bersama-sama dengan KH sehingga mengakibatkan kerugian Bank Danamon sebesar Rp 372.100.000. Modus operandinya dimulai dengan membuka rekening di Bank Danamon Cabang Utama dengan alamat dan nama palsu, dan KH yang bekerja di ruang reknosihasi pada cabang tersebut membantunya. KH dengan diam-diam mempelajari bagaimana mengoperasikan komputer untuk melakukan akses. Setelah mengerti, KH menggunakan komputer di ruang kerjanya dan dengan menggunakan ID *user* dan *password* tertentu memindahkan uang dari rekening rupa-rupa uang muka kantor pusat. Dari sini kemudian dikreditkan ke rekening yang telah dibuka BH di Cabang Utama Bank Danamon.

Pada tahun 1990 juga terdapat kasus di Bank Danamon Glodok Plaza yang modus operandinya hampir sama dengan yang terdapat pada Bank Danamon Pusat. Disamping itu, terdapat kasus uang Tabanas BRI Jatinegera Timur di tahun 1991 dengan modus operandi menyalahgunakan rekening tabanas pasif dengan cara mengubah nama nasabah dan mencantumkan saldo yang sesungguhnya tidak ada. Kemudian dengan mengisi blangko buku tabanas yang tanpa sepengetahuan *teller* dan dengan bekerja dengan pihak lain serta dengan menggunakan *password* milik *teller*, kemudian memindahkan uang tabungan tersebut.

Dari urain kasus–kasus tersebut dapat diketahui bahwa pada dasarnya kejahatan tersebut dilakukan dengan bantuan atau melalui peralatan komputer, telekomunikasi, dan informasi, baik berupa *hardware, software*, maupun *brainware.*

Electronic/cyber dan Hukum

Responden sebanyak 60% lebih menghendaki bahwa tanda tangan bukanlah sesuatu yang mutlak sebagai bukti kesepakatan, dan menyatakan bahwa meskipun tanda tangan tidak ada dalam suatu perjanjian tertulis, perjanjian tersebut dapat memenuhi adanya kesepakatan sebagai salah satu syarat sahnya perjanjian sebagaimana yang dimaksud dalam pasal 1320 KUHPerdata. Pendapat ini memang dapat dibenarkan, karena dalam hukum Indonesia, kesepakatan tidak harus dituangkan dalam bentuk tertulis, namun bisa saja dinyatakan secara lisan. Bila dihubungkan dengan hukum adat, kesepakatan ini tidak begitu dipersoalkan karena transaksi dalam hukum adat dikenal dengan *sistem tunai*. Dengan perkataan lain bahwa kesepakatan itu dianggap ada apabila telah dilakukan tindakan *tunai*, dan tanpa tindakan tunai maka kesepakatan dianggap belum ada. Filosophi adanya tanda tangan adalah sebagai bukti bahwa yang bersangkutan menerima isi kesepakatan yang tercantum dalam suatu perjanjian, yang kegunaannya ditujukan untuk pembuktian.

Subekti, dalam bukunya yang berjudul Hukum Pembuktian menyatakan yang penting dari suatu akte memang penandatanganannya. Dengan menaruh tanda tangannya, seorang dianggap menanggung tentang kebenaran apa yang ditulis dalam akte tersebut atau bertanggung jawab tentang apa yang ditulis dalam akte itu.[90]

Menurut KUHPerdata pasal 1874[91] dan Ordonansi tahun 1867 no 29 tentang ketentuan-ketentuan kekuatan pembuktian tulisan-tulisan di bawah tangan dari orang-orang Indonesia atau yang dipersamakan dengan mereka, dalam pasal 1[92] bahwa sesuatu akte diisyaratkan haruslah ditanda tangani dengan perkataan lain bahwa sesuatu surat yang tidak ditandatangani dianggap bukanlah akte. Lalu akte ini dapat lagi dibagi yaitu akte authentik dan akte dibawah tangan, yang tujuannya adalah untuk tingkat pembuktiannya.

Kembali kepada e-commerce, secara analogi dari uraian di atas, bahwa tanda tangan bukanlah merupakan syarat syahnya perjanjian, tapi kegunaannya diperuntukkan untuk pembuktian. Kelihatannya tanda tangan sebagai pembuktian sangat penting, dimana lembaga-lembaga internasional juga membicarakannya antara lain; United Nations Commission on International Trade Law (UNCITRAL) yang mengatur tentang Model Undang-undang tanda tangan elektronik *(electronic signiture)* UNCITRAL 2001, European Union yang mengatur tentang Petunjuk 1999/93/EC tentang Petunjuk mengenai Tanda Tangan Elektronik. Dan bahkan authentifikasi tanda tangan juga dibicarakan, untuk menentukan keaslian tanda tangan.

Pada tabel 4, responden hampir 40% menyatakan bahwa tanda tangan dalam transaksi dengan mempergunakan media elektronika merupakan salah satu syarat syahnya perjanjian sebagaimana dimaksud pasal 1320 KUHPerdata. Untuk sahnya persetujuan-persetujuan diperlukan empat syarat :

1. mereka sepakat untuk mengikatkan diri;
2. cakap untuk membuat suatu perikatan;
3. suatu hal tertentu;
4. suatu sebab tertentu;

Kedua syarat yang pertama dinamakan syarat subyektif karena kedua syarat tersebut mengenai subjek perjanjian sedangkan kedua syarat terakhir disebutkan syarat obyektif karena mengenai obyek dari perjanjian.[93] Dalam hal terjadi transaksi yang tidak memenuhi syarat subjektif maka perjanjian tersebut dapat dibatalkan dan dalam hal tidak memenuhi syarat objektif maka perjanjian tersebut batal demi hukum. Namun apakah hal ini dapat diterapkan untuk transaksi e-commerce, para responden telah memberikan jawabannya dibawah ini.

---

[90] Subekti, Hukum Pembuktian, PT Pradnya Paramita, Jakarta cet. Kedelapan 1987, hal 28
[91] lihat pasal 1874 KUHPerdata
[92] lihat pasal 1 Ordonansi tahun 1867 no 29
[93] Mariam Darus Badrulzaman, *Aneka Hukum Bisnis*, Alumni, Bandung, 1994, hal 24

Dan dalam hal e-commerce, salah satu pihaknya dapat saja masih berusia dibawah umur. Responden sebanyak hampir 45% meyatakan kontrak tersebut dapat dibatalkan dan 42% lebih responden yang menyatakan kontrak tersebut batal demi hukum.[94] Seseorang dapat dinyatakan cakap melakukan perbuatan hukum diatur dalam KUHPerdata yang berbunyi :

> "Setiap orang adalah cakap untuk membuat perikatan, kecuali jika undang-undang menyatakan bahwa orang tersebut adalah tidak cakap. Orang-orang yang tidak cakap membuat perjanjian adalah orang-orang yang belum dewasa dan mereka yang ditaruh dibawah pengampuan".[95]

Di Indonesia menurut yurisprudensi bahwa seseorang itu dinyatakan cakap bertindak dalam hukum apabila orang tersebut sudah dewasa dan seseorang dinyatakan sudah dewasa apabila orang tersebut telah mencapai umur 21 tahun atau telah menikah. Dalam hal mutu/kwalitas barang yang menjadi objek e-commerce sewaktu diterima oleh pembeli ternyata tidak sesuai dengan kesepakatan dengan komunikasi melalui internet dilakukan, 80% lebih responden menyatakan bahwa pembeli dapat mengclaim/menuntut penjual.[96]

Sebenarnya tentang kesepakatan dalam e-commerce masih diperdebatkan, oleh karena banyaknya paham tentang kapankah lahir/ada kesepakatan tersebut. Bahkan para ahli hukum masih mempersoalkan kapan terjadi penawaran *(offer)* dan kapan terjadi penerimaan (*acceptance*).

Kontrak dalam sistem *Common Law* berpandangan, sebagaimana dalam perkara *Mellen v. Johnson*, 322 Mass. 236 N.E. 2d 658, bahwa penawaran yang terbuka untuk orang banyak tidaklah dianggap sebagai penawaran. Penawaran yang terbuka kepada pihak lain masih dianggap sebagai undangan untuk proses penawaran.[97] Apabila penawaran dalam perkara tersebut dianalogikan terhadap penawaran dalam internet, tentu penawaran tersebut merupakan penawaran yang diperuntukkan untuk orang banyak, sehingga penawaran yang demikian masih dalam taraf undangan untuk proses penawaran.

Beberapa teori yang menyatakan saat terjadinya perjanjian :[98]

- Teori kehendak (*wilstheorie*) mengajarkan bahwa kesepakatan terjadi pada kehendak pihak penerima dinyatakan, misalnya dengan melukiskan surat.
- Teori pengiriman (*verzendtheorie*) mengajarkan bahwa kesepakatan terjadi pada saat kehendak yang dinyatakan itu dikirim oleh pihak yang menerima tawaran.
- Teori pengetahuan (*vernemingstheorie*) mengajarkan bahwa pihak yang menawarkan seharusnya sudah mengetahui bahwa tawarannya diterima.

---

[94] lihat tabel 8
[95] lihat pasal 1329 sampai dengan 1331 KUHPerdata
[96] lihat tabel 7
[97] Victor Purba, *Kontrak Jual Beli Barang Internasional (konvensi Vienna 1980)*, Fakultas Hukum Universitas Indonesia, Jakarta, 2002, hal 34
[98] Mariam Darus Badrulzaman, *loc.cit.*

- Teori kepercayaan (*vertrowenstheorie*) mengajarkan bahwa kesepakatan itu terjadi pada saat pernyataan kehendak dianggap layak diterima oleh pihak yang menawarkan.

Apabila theori tersebut diterapkan dalam e-commerce, tentu akan menimbulkan banyak interpretasi, sehingga sangatlah tepat pandangan responden yang menyatakan bahwa KUHPerdata tidak cukup mengakomodir soal-soal hukum e-commerce dimana 76% lebih responden mengatakan bahwa perlu dibuat ketentuan khusus mengenai e-commerce, dan hanya 19% responden mengatakan bahwa KUHPerdata bisa diterapkan dengan cara penafsiran.[99] Selanjutnya para responden sebanyak 52% menghendaki perlu dibuat tanda tangan elektronik (*digital signature*), dan hanya 16% responden menyatakan tidak setuju penggunaan tanda tangan elektronik.[100] Sebagian besar responden yaitu sebanyak 55% menyatakan bahwa tanda tangan elektronik perlu didaftarkan untuk menjamin para pihak yang bersangkutan dalam transaksi elektronik, dan hanya sebesar 35% responden berkeyakinan bahwa meskipun ada tanda tangan elektronik dan didaftarkan belum menjamin para pihak yang bersangkutan dalam transaksi elektronik.[101] Untuk itu sebenarnya sekarang ini telah dirampungkan beberapa rancangan peraturan misalnya Rancangan UU tentang pidana kejahatan teknologi informasi, Rancangan UU tentang tanda tangan elektronik dan transaksi elektronik, Rancangan Keputusan Dirjen tentang persyaratan teknis perangkat ADSL (Asymetric, Digital, Subscriber Line)

1. Electronic/cyber dan Pengadilan

Transaksi dalam e-commerce berpengaruh pula dalam pembuktian di pengadilan, hampir 70% responden menyetujui bahwa fax dan telepon dapat diterima sebagai alat bukti, dan hampir 30% tetap berpendirian bahwa fax dan telepon tidak dapat dijadikan jadi alat bukti.[102] Tabel 18 menunjukkan bahwa para responden mempunyai wawasan kedepan dan tanggap terhadap perubahan zaman dengan maraknya e-commerce, dimana 85% lebih responden menghendaki perubahan dan penyesuaian dengan perkembangan zaman/teknologi atas sistem pembuktian dalam KUAHPidana maupun dalam acara perdata HIR/RBG dan hanya 12% responden berpendapat bahwa tidak perlu diadakan perubahan sistem pembuktian dalam perkara pidana maupun dalam perkara perdata dalam menangani perkara-perkara yang berhubungan dengan transaksi elektronik.[103] Para responden juga menyetujui dan berpendapat bahwa persidangan dengan menggunakan *teleconfrence* untuk mendengar saksi,

[99] lihat tabel 11
[100] lihat tabel 12
[101] lihat tabel 13
[102] lihat tabel 5
[103] lihat tabel 18

untuk mendengar para pihak yang berperkara, terdakwa tetap dianggap sah.[104] Juga hampir 70% responden berpandangan bahwa gugatan/permohonan dapat didaftarkan ke Pengadilan melalui komputer/e-mail, dan hampir 30% responden berpendapat tidak perlu diatur pendaftaran gugatan/permohonan ke pengadilan melalui e-mail.[105]

Electronic/cyber dan itikad baik

Berdasarkan pengamatan peneliti bahwa hakim di Indonesia, sangat banyak mengadili perkara-perkara didasarkan kepada itikad baik Dalam konvensi Vienna 1980 juga diatur masalah itikad baik (*good faith*), juga di Amerika Serikat dalam Uniform Commercial Code, tentang itikd baik secara tegas dicantumkan *"every contract imposes upon each party a duty of good faith and fair dealing in its performance and enforcement"*[106]

Tabel 6 menunjukkan bahwa para responden sebanyak lebih dari 80% setuju mempergunakan azas itikad baik dalam mempertimbangkan hukum dalam suatu perkara yang mengandung e-commerce, dan hanya hampir 15% yang tidak setuju.[107]

Electronic/cyber dan hukum negara lain

Masalah e-commerce ini tidak saja berlangsung di suatu jurisdiksi tertentu atau dalam suatu negara, namun lintas batas negara, oleh karena itu timbul soal-soal hukum antar negara atau internasional. Pada pokoknya hukum di dunia ini terbagi dua kelompok yaitu sistem *common law* dan *civil law.* Masalah hukum internasional akan timbul jika seseorang dari suatu negara yang menganut sistem *common law* mengadakan transaksi e-commerce dengan seseorang dari suatu negara yang menganut sistem *civil law,* persoalan tersebut adalah hukum mana yang diperlakukan dan hukum acara negara mana yang diperlakukan.

Menyadari akan hal tersebut di atas, 73% responden menghendaki perlu diatur secara khusus mengenai cara dan tempat mengajukan perkara jika terjadi perkara pidana maupun perdata sehubungan dengan penggunaan elektronik, dan hampir 25% responden berpendapat bahwa tidak perlu dibuat aturan secara khusus untuk itu, karena masih dapat mempergunakan pasal 118HIR/154 Rbg.[108]

---

[104] lihat tabel 20
[105] lihat tabel 21
[106] Victor Purba, *op.cit.*, hal 70
[107] Lihat tabel 6
[108] lihat tabel 10

Electronic/cyber dan ISP

Sehubungan dengan pertanggungjawaban Internet Service Provider (ISP) terhadap pihak-pihak yang merasa dirugikan baik secara materil maupun immateril akibat perbuatan orang lain dengan melawan hukum, tabel 14 menunjukan bahwa 42% responden menyatakan bahwa ISP tidak bertanggung jawab atas perbuatan pihak ketiga yang melawan hukum dengan alasan bahwa ISP tidak mungkin melakukan pengawasan terhadap sedemikian banyak pengguna jasa internet, 40% responden menyatakan ISP bertanggung jawab apabila ISP terlibat, 14% responden menyatakan ISP bertanggung jawab sepenuhnya.

Di Indonesia memang ISP belum pernah diajukan ke pengadilan, namun di negara-negara maju misalnya di Amerika Serikat, ISP sudah beberapa kali diajukan ke pengadilan.[109]

Selanjutnya para responden sebesar 92% lebih menghendaki perlu diatur ketentuan-ketentuan hukum mengenai kewajiban-kewajiban ISP terhadap custumer maupun pihak lain yang dirugikan.[110]

Electronic/cyber dan security

Perkembangan tehnologi komputer dan telekomunikasi memang membawa manfaat kepada pelaku bisnis, namun sebaliknya dapat pula membawa kerugian, bilamana orang-orang tertentu mengambil manfaat dengan melawan hukum dari *electronic transaction* yang dilakukan pelaku bisnis.[111]

Tabel 17 menunjukan bahwa 92% responden menghendaki agar diatur ketentuan tentang jaminan keamanan para pengguna internet dalam melakukan e-commerce, sehingga pihak lain tidak dapat access untuk mengambil keuntungan dengan melawan hukum.[112]

Electronic/cyber dan pelanggaran hukum

Sebanyak 70% responden tidak menghendaki pihak lain memasukkan file-file elektronik (*junk mail*) masuk ke e-mail orang tertentu tanpa izin dari orang yang bersangkutan (*users*) dan berpandangan bahwa hal itu merupakan pelanggaran hukum, sementara 24% responden tidak mempersoalkannya dan menyatakan bahwa hal tersebut bukan merupakan pelanggaran hukum.[113] Dalam hal yang hampir sama juga, hampir 90% responden menyatakan bahwa

---

[109] lihat Bab II
[110] lihat tabel 15
[111] lihat no 1 Analisis tentang contoh-contoh cybercrime
[112] lihat tabel 17
[113] lihat tabel 16

apabila merk dagang milik seseorang atau badan hukum yang telah didaftarkan sebagai domein name digunakan oleh orang lain tanpa seijin pemiliknya adalah merupakan perbuatan melawan hukum.[114]

B. TABULASI

1. Apakah saudara pernah menggunakan internet?
   a. Sudah biasa menggunakan internet
   b. Pernah menggunakan internet beberapa kali
   c. Tidak pernah menggunakannya, tetapi tahu caranya
   d. Tidak pernah
   e. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																				JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL						
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E		
1	BANDUNG	0	2	1	10	0	0	0	2	8	0	0	0	0	0	0	0	2	2	0	0	0	0	1	5	0	0	0	0	4	0	1	0	0	3	0		42
2	BANJARMASIN	0	0	0	11	0	1	1	0	12	0	0	0	0	0	0	0	0	0	7	0	0	0	0	7	0	0	1	0	4	0	0	0	2	0	0		46
3	BENGKULU	0	1	3	10	0	2	2	0	9	0	0	0	0	0	0	0	0	0	5	0	0	1	0	8	0	0	2	0	9	0	0	0	0	0	0		52
4	DENPASAR	0	1	4	9	1	3	1	0	0	0	0	0	0	0	0	0	2	0	3	0	0	2	1	2	0	0	3	0	5	0	0	3	0	2	0		49
5	LAMPUNG	0	3	1	7	0	1	5	2	11	0	0	0	0	0	0	0	0	0	0	0	0	1	1	4	0	0	3	0	7	0	0	0	0	0	0		45
6	MAKASSAR	1	1	0	9	0	2	2	0	5	0	0	1	0	3	0	0	1	0	4	0	0	1	0	9	0	0	2	0	6	0	0	0	0	0	0		48
7	MATARAM	0	0	1	15	1	0	0	1	9	0	0	0	0	0	0	0	1	2	2	0	0	2	1	5	0	0	4	1	6	0	0	0	0	0	0		51
8	MEDAN	0	1	3	8	0	0	3	1	5	0	0	0	1	4	0	0	0	2	5	0	0	0	0	1	0	0	3	1	10	0	0	0	2	0	0		50
9	PEKANBARU	0	1	1	12	0	0	4	3	4	0	0	0	0	0	0	0	2	2	1	0	0	1	2	6	0	0	0	0	11	0	0	0	0	0	0		50
10	PALU	0	0	2	6	0	0	0	0	16	0	0	0	0	0	0	1	1	1	4	0	0	1	1	5	0	0	1	0	6	0	0	0	0	0	0		47
11	PONTIANAK	0	2	2	14	0	0	0	0	9	0	0	0	0	0	0	0	0	1	4	0	0	0	1	4	0	0	3	0	2	0	0	1	0	3	0		48
	JUMLAH	1	12	18	111	2	9	18	9	88	0	0	1	2	7	0	1	9	8	35	0	0	9	12	56	0	0	20	11	66	0	1	8	4	10	0		526

JUMLAH (%) A= 2.27% B= 14.58% C= 12.12% D= 70.64% E= 0.38%

[114] lihat tabel 19

2. Apakah saudara pernah mempelajari atau memahami tentang e-commerce dan cybercrime/ digitelcrime?
   a. Pernah dan memahami
   b. Pernah tapi kurang memahami
   c. Tidak pernah
   d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																						JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	1	7	5	0	0	0	10	0	0	0	0	0	0	0	0	0	2	2	0	0	0	3	3	0	0	0	2	2	0	0	0	2	3	0	0	42
2	BANJARMASIN	0	2	9	0	0	0	3	11	0	0	0	0	0	0	0	0	2	5	0	0	0	0	7	0	0	0	1	4	0	0	0	2	0	0	0	46
3	BENGKULU	0	5	9	0	0	1	7	5	0	0	0	0	0	0	0	0	2	3	0	0	1	0	8	0	0	0	4	7	0	0	0	0	0	0	0	52
4	DENPASAR	0	3	12	0	0	3	1	0	0	0	0	0	0	0	0	0	4	1	0	0	0	5	3	0	0	1	6	5	0	0	1	1	3	0	0	49
5	LAMPUNG	0	5	6	0	0	1	12	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	1	4	4	0	0	0	0	0	0	0	45
6	MAKASSAR	1	7	3	0	0	2	3	4	0	0	0	2	3	0	0	0	2	3	0	0	0	3	7	0	0	0	3	3	0	0	0	2	0	0	0	48
7	MATARAM	0	4	13	0	0	0	1	9	0	0	0	0	0	0	0	1	2	3	0	0	0	2	6	0	0	0	3	8	0	0	0	0	0	0	0	51
8	MEDAN	2	0	10	0	0	0	2	7	0	0	0	1	4	0	0	0	2	3	0	0	0	0	1	0	0	2	5	7	0	0	0	2	0	0	0	50
9	PEKANBARU	0	3	11	0	0	0	5	6	0	0	0	0	0	0	0	0	2	3	0	0	0	0	9	0	0	0	1	10	0	0	0	0	0	0	0	50
10	PALU	1	0	7	0	0	0	3	13	0	0	0	0	0	0	0	0	4	3	0	0	0	0	3	0	0	0	1	8	0	0	0	0	0	0	0	47
11	PONTIANAK	1	7	10	0	0	0	4	5	0	0	0	0	0	0	0	0	0	5	0	0	0	2	4	0	0	0	2	3	0	0	0	3	0	0	0	48
	JUMLAH	6	43	95	0	0	7	51	66	0	0	0	3	7	0	0	1	21	31	0	0	1	19	57	0	0	4	32	61	0	0	1	12	10	0	0	528

JUMLAH (%) A= 3.79% B= 34.28% C= 61.93% D= 0.00%

3. Apakah saudara pernah menangani perkara perdata atau pidana yang berhubungan dengan e-commerce atau kejahatan dengan menggunakan internet/komputer
   a. Pernah beberapa kali
   b. Tidak pernah
   c. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																						JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	3	9	1	0	0	0	10	0	0	0	0	0	0	0	0	0	4	0	0	0	0	6	0	0	0	0	4	0	0	0	0	5	0	0	0	42
2	BANJARMASIN	0	11	0	0	0	0	14	0	0	0	0	0	0	0	0	0	7	0	0	0	0	7	0	0	0	0	5	0	0	0	0	2	0	0	0	46
3	BENGKULU	1	13	0	0	0	0	13	0	0	0	0	0	0	0	0	0	5	0	0	0	0	9	0	0	0	0	11	0	0	0	0	0	0	0	0	52
4	DENPASAR	0	15	0	0	0	1	4	0	0	0	0	0	0	0	0	0	5	0	0	0	0	8	0	0	0	0	12	0	0	0	0	5	0	0	0	49
5	LAMPUNG	0	10	1	0	0	1	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	9	0	0	0	0	0	0	0	0	45
6	MAKASSAR	1	10	0	0	0	0	9	0	0	0	0	5	0	0	0	0	5	0	0	0	0	10	0	0	0	0	6	0	0	0	0	2	0	0	0	48
7	MATARAM	1	16	0	0	0	0	10	0	0	0	0	0	0	0	0	0	5	0	0	0	0	8	0	0	0	0	11	0	0	0	0	4	0	0	0	51
8	MEDAN	0	12	0	0	0	0	9	0	0	0	0	5	0	0	0	0	5	0	0	0	0	1	0	0	0	1	13	0	0	0	0	4	0	0	0	50
9	PEKANBARU	1	12	1	0	0	0	11	0	0	0	0	0	0	0	0	0	5	0	0	0	0	7	0	0	0	0	11	0	0	0	0	0	0	0	0	50
10	PALU	0	8	0	0	0	0	16	0	0	0	0	0	0	0	0	0	7	0	0	0	0	7	0	0	0	0	9	0	0	0	0	0	0	0	0	47
11	PONTIANAK	0	18	0	0	0	0	9	0	0	0	0	0	0	0	0	0	5	0	0	0	0	6	0	0	0	0	5	0	0	0	0	5	0	0	0	48
	JUMLAH	7	134	3	0	0	1	123	0	0	0	0	10	0	0	0	0	53	0	0	0	0	75	2	0	0	1	96	0	0	0	0	23	0	0	0	528

JUMLAH (%) A= 1.70% B= 97.35% C= 0.95%

4. Apakah kegiatan transaksi perdagangan melaui media elektronik, sekalipun bukan merupakan transaksi tertulis / tanpa tanda tangan sebagai bukti kesepakatan, dapat dipandang telah memenuhi syarat sahnya suatu perjanjian (psl. 1320 KUH Perdata)
   a. Dapat
   b. Tidak
   c. Jelaskan pendapat saudara
   d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	1	0	0	0	8	2	0	0	0	0	0	0	0	0	4	0	0	0	0	2	4	0	0	0	1	0	4	0	0	4	0	0	1	0	42
2	BANJARMASIN	4	7	0	0	0	7	7	0	0	0	0	0	0	0	0	1	6	0	0	0	0	7	0	0	0	1	4	4	0	0	2	0	0	0	0	46
3	BENGKULU	10	4	0	0	0	10	3	0	0	0	0	0	0	0	0	4	1	0	0	0	4	5	0	0	0	7	4	4	0	0	0	0	0	0	0	52
4	DENPASAR	10	5	0	0	0	4	0	0	0	0	0	0	0	0	0	2	3	0	0	0	1	7	1	0	0	8	4	4	0	0	5	0	0	0	0	49
5	LAMPUNG	8	3	0	0	0	17	2	0	0	0	0	0	0	0	0	0	0	0	0	0	8	1	5	0	0	0	7	2	0	0	0	0	0	0	0	45
6	MAKASSAR	7	3	1	0	0	5	4	0	0	0	4	1	0	0	0	3	2	0	0	0	5	8	2	0	0	0	4	2	0	0	2	0	0	0	0	48
7	MATARAM	10	7	0	0	0	6	4	0	0	0	0	0	0	0	0	3	2	0	0	0	5	3	0	0	0	7	4	0	0	0	0	0	0	0	0	51
8	MEDAN	8	4	0	0	0	8	1	0	0	0	2	3	0	0	0	2	3	0	0	0	1	0	0	0	0	9	5	0	0	0	2	0	1	0	0	50
9	PEKANBARU	6	6	0	2	0	10	1	0	0	0	0	0	0	0	0	3	2	0	0	0	3	4	6	0	0	6	5	0	0	0	0	0	0	0	0	50
10	PALU	2	6	0	0	0	6	9	0	1	0	0	0	0	0	0	3	4	0	0	0	3	4	0	0	0	2	7	0	0	0	0	0	0	0	0	47
11	PONTIANAK	15	3	0	0	0	5	4	0	0	0	0	0	0	0	0	2	2	0	1	0	0	4	1	0	0	4	1	0	0	0	5	0	0	0	0	48
	JUMLAH	92	49	1	2	0	86	37	0	1	0	6	4	0	0	0	27	25	0	1	0	38	38	0	1	0	55	42	0	0	0	20	1	0	2	0	528

JUMLAH (%) A= 61.36% B= 37.12% C= 0.19% D= 1.33%

5. Proses terjadinya dalam transaksi perdagangan melaui e-commerce, fax, telepon, dapat diterima sebagai alat bukti dalam hukum pembuktian menurut KUH Perdata
   a. Dapat
   b. Tidak
   c. Jelaskan pendapat saudara
   d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	1	0	0	0	10	0	0	0	0	0	0	0	0	0	4	0	0	0	0	3	3	0	0	0	0	4	4	0	0	0	4	1	0	0	42
2	BANJARMASIN	10	1	0	0	0	10	4	0	0	0	0	0	0	0	0	4	3	0	0	0	0	7	0	0	0	1	4	4	0	0	2	0	0	0	0	46
3	BENGKULU	14	0	0	0	0	11	2	0	0	0	0	0	0	0	0	4	1	0	0	0	3	6	0	0	0	7	4	0	0	0	0	0	0	0	0	52
4	DENPASAR	8	4	0	3	0	2	2	0	0	0	0	0	0	0	0	5	0	0	0	0	8	0	0	0	0	8	1	0	3	0	5	0	0	0	0	49
5	LAMPUNG	8	2	0	1	0	18	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	5	0	0	0	5	4	0	0	0	0	0	0	0	0	45
6	MAKASSAR	8	2	0	1	0	7	2	0	0	0	5	0	0	0	0	3	2	0	0	0	6	4	0	0	0	5	1	0	0	0	2	0	0	0	0	48
7	MATARAM	12	5	0	0	0	8	2	0	0	0	0	0	0	0	0	4	1	0	0	0	4	4	0	0	0	6	5	0	0	0	1	0	0	0	0	51
8	MEDAN	6	4	2	0	0	7	2	0	0	0	2	3	0	0	0	2	1	0	0	0	1	0	0	0	0	11	3	0	0	0	1	0	2	0	0	50
9	PEKANBARU	10	1	0	3	0	9	2	0	0	0	0	0	0	0	0	4	0	0	0	1	4	4	0	0	0	8	3	0	0	0	0	0	0	0	0	50
10	PALU	0	6	0	2	0	5	10	0	1	0	0	0	0	0	0	5	2	0	0	0	2	5	0	0	0	3	6	0	0	0	0	0	0	0	0	47
11	PONTIANAK	18	0	0	0	0	7	2	0	0	0	0	0	0	0	0	4	0	0	1	0	5	1	0	0	0	5	0	0	0	0	3	2	0	0	0	48
	JUMLAH	106	26	2	10	0	94	29	0	1	0	7	3	0	0	0	39	10	0	4	0	37	39	0	1	0	59	35	0	3	0	17	5	0	1	0	528

JUMLAH (%) A= 67.99% B= 27.84% C= 0.38% D= 3.79%

6. Apakah menurut saudara Azas "Etikad baik" para pihak yang melaksanakan e-commersce dapat dipakai dalam pertimbangan hukum memutus perkara aquo
   a. Dapat
   b. Tidak
   c. Jelaskan pendapat saudara
   d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	13	0	0	0	0	10	0	0	0	0	0	0	0	0	0	4	0	0	0	0	4	2	0	0	0	2	2	0	0	0	4	0	0	1	0	42
2	BANJARMASIN	11	0	0	0	0	10	4	0	0	0	0	0	0	0	0	6	1	0	0	0	0	7	0	0	0	1	4	0	0	0	2	0	0	0	0	46
3	BENGKULU	13	1	0	0	0	13	0	0	0	0	0	0	0	0	0	5	1	0	0	0	7	2	0	0	0	10	1	0	0	0	0	0	0	0	0	52
4	DENPASAR	9	2	0	4	0	4	0	0	0	0	0	0	0	0	0	4	1	0	0	0	7	0	0	1	0	10	0	0	2	0	5	0	0	0	0	49
5	LAMPUNG	10	1	0	0	0	19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	3	0	1	0	9	0	0	0	0	0	0	0	0	0	45
6	MAKASSAR	9	1	0	1	0	8	1	0	0	0	5	0	0	0	0	3	2	0	0	0	9	2	1	0	0	6	0	0	0	0	2	0	0	0	0	48
7	MATARAM	11	6	0	0	0	10	0	0	0	0	0	0	0	0	0	3	2	0	0	0	6	2	0	0	0	9	2	0	0	0	0	0	0	0	0	51
8	MEDAN	7	4	1	0	0	8	1	0	0	0	4	1	0	0	0	4	1	0	0	0	1	0	0	0	0	9	3	1	0	0	1	0	1	2	0	50
9	PEKANBARU	9	2	0	3	0	11	0	0	0	0	0	0	0	0	0	4	0	0	1	0	7	1	0	0	0	5	6	0	0	0	0	0	1	0	0	50
10	PALU	5	1	0	2	0	11	2	0	3	0	0	0	0	0	0	6	1	0	0	0	7	0	0	0	0	7	0	2	0	0	0	0	0	0	0	47
11	PONTIANAK	18	0	0	0	0	8	1	0	0	0	0	0	0	0	0	5	0	0	0	0	6	0	0	0	0	5	0	2	0	0	5	0	0	0	0	48
	JUMLAH	115	18	1	10	0	112	9	0	3	0	9	1	0	0	0	44	8	0	1	0	56	18	0	3	0	73	20	1	2	0	19	1	1	3	0	528

JUMLAH (%) A= 81.06% B= 14.20% C= 0.57% D= 4.17%

7. Apabila mutu/kualitas barang yang menjadi obyek e-commerce ternyata tidak sesuai dengan kesepakatan ketika komunikasi melalui internet dilakukan, saat barang tersebut diterima oleh pembeli, dapatkah dilakukan gugatan oleh pihak pembeli dan alasan hukum apa yang dapat dipakai untuk menuntut oleh pembeli terhadap penjual
   a. Dapat
   b. Tidak
   c. Jelaskan pendapat saudara
   d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	0	0	1	0	9	0	0	1	0	0	0	0	0	0	3	1	0	0	0	5	1	0	0	0	2	2	0	0	0	4	1	0	0	0	42
2	BANJARMASIN	10	1	0	0	0	13	1	0	0	0	0	0	0	0	0	4	3	0	0	0	0	7	0	0	0	1	4	0	0	0	2	0	0	0	0	46
3	BENGKULU	13	1	0	0	0	13	0	0	0	0	0	0	0	0	0	5	0	0	0	0	6	3	0	0	0	9	2	0	0	0	0	0	0	0	0	52
4	DENPASAR	7	3	0	5	0	4	0	0	0	0	0	0	0	0	0	5	0	0	0	0	7	1	0	0	0	7	2	0	3	0	5	0	0	0	0	49
5	LAMPUNG	11	0	0	0	0	18	1	0	0	0	0	0	0	0	0	0	1	0	0	0	4	2	0	0	0	9	0	0	0	0	0	0	0	0	0	45
6	MAKASSAR	11	0	0	0	0	9	0	0	0	0	5	0	0	0	0	4	1	0	0	0	9	1	0	0	0	8	0	0	0	0	2	0	0	0	0	48
7	MATARAM	17	0	0	0	0	4	6	0	0	0	0	0	0	0	0	4	1	0	0	0	8	0	0	0	0	10	0	1	0	0	0	0	0	0	0	51
8	MEDAN	10	2	0	0	0	8	1	0	0	0	4	1	0	0	0	4	1	0	0	0	1	0	0	0	0	13	1	0	0	0	1	0	2	0	0	50
9	PEKANBARU	12	1	0	1	0	0	10	1	0	0	0	0	0	0	0	4	0	0	1	0	7	0	0	2	0	8	1	0	0	0	0	0	0	0	0	50
10	PALU	4	2	0	2	0	12	1	0	3	0	0	0	0	0	0	6	1	0	0	0	5	2	0	0	0	6	2	0	1	0	0	0	0	0	0	47
11	PONTIANAK	18	0	0	0	0	9	0	0	0	0	0	0	0	0	0	4	1	0	0	0	5	0	0	0	0	5	0	0	0	0	5	0	0	0	0	48
	JUMLAH	125	10	0	9	0	99	20	1	4	0	9	1	0	0	0	43	9	0	1	0	57	17	0	3	0	76	14	1	6	0	19	3	0	1	0	528

JUMLAH (%) A= 81.06% B= 14.02% C= 0.38% D= 4.55%

8. Kemungkinan dapat terjadi tanpa sepengetahuan kedua pihak, ternyata salah satu pihak ketika e-commerce dilakukan oleh mereka, salah satu pihaknya masih berusia dibawah umur menurut ketentuan KUH Perdata. Apakah perjanjian / kontrak tersebut batal demi hukum atau dapat dibatalkan (berikan pendapat saudara)
   a. Batal demi hukum
   b. Dapat dibatalkan
   c. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	3	5	5	0	0	6	2	2	0	0	0	0	0	0	0	2	2	0	0	0	3	3	0	0	0	4	1	0	0	0	2	2	1	0	0	42
2	BANJARMASIN	7	4	0	0	0	8	6	1	0	0	0	0	0	0	0	5	1	1	0	0	4	1	0	3	0	0	1	0	4	0	0	1	1	0	0	46
3	BENGKULU	2	10	2	0	0	3	9	1	0	0	0	0	0	0	0	4	1	0	0	0	8	1	0	0	0	4	7	1	0	0	0	0	1	0	0	52
4	DENPASAR	4	5	6	0	0	0	2	2	0	0	0	0	0	0	0	4	1	0	0	0	4	4	0	0	0	4	4	0	4	0	3	2	0	0	0	49
5	LAMPUNG	6	4	1	0	0	7	9	3	0	0	0	0	0	0	0	0	0	0	0	0	3	2	1	0	0	3	6	1	0	0	0	2	0	0	0	45
6	MAKASSAR	5	4	2	0	0	3	5	1	0	0	1	4	0	0	0	4	1	0	0	0	4	6	0	0	0	2	3	1	0	0	0	2	0	0	0	48
7	MATARAM	8	9	0	0	0	7	3	0	0	0	0	2	0	0	0	3	1	1	0	0	5	3	0	0	0	4	7	0	0	0	0	0	0	0	0	51
8	MEDAN	7	4	1	0	0	3	5	1	0	0	3	0	0	0	0	2	3	0	0	0	0	1	0	0	0	1	13	0	0	0	1	3	0	0	0	50
9	PEKANBARU	4	7	3	0	0	2	8	1	0	0	0	0	0	0	0	1	1	3	0	0	3	3	0	0	0	5	5	1	0	0	0	0	0	0	0	50
10	PALU	3	3	2	0	0	6	5	0	0	0	0	0	0	0	0	2	4	1	0	0	4	3	0	0	0	5	3	1	0	0	0	0	0	0	0	47
11	PONTIANAK	5	10	3	0	0	6	3	0	0	0	0	0	0	0	0	3	2	0	0	0	5	1	0	0	0	3	1	1	0	0	1	2	0	0	0	48
	JUMLAH	54	65	25	0	0	51	57	16	0	0	4	6	0	0	0	30	17	6	0	0	43	27	7	0	0	35	50	12	0	0	7	12	4	0	0	528

JUMLAH (%) A= 42.42% B= 44.32% C= 13.26%

9. Apakah saudara pernah membaca atau mengetahui kejahatan yang dkaitkan dengan kartu kredit, modus operandi apa yang biasa dilakukan di wilayah saudara
   a. Tidak pernah
   b. Pernah
   c. Jelaskan
   d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	2	11	0	0	0	3	7	0	0	0	0	0	0	0	0	2	2	0	0	0	2	4	0	0	0	2	2	0	0	0	1	4	0	0	0	42
2	BANJARMASIN	5	6	0	0	0	8	6	0	0	0	0	0	0	0	0	2	5	0	0	0	7	0	0	0	0	4	1	0	0	0	0	2	0	0	0	46
3	BENGKULU	7	7	0	0	0	1	12	0	0	0	0	0	0	0	0	0	5	0	0	0	6	3	0	0	0	7	4	1	0	0	0	0	0	0	0	52
4	DENPASAR	4	11	0	0	0	0	4	0	0	0	0	0	0	0	0	1	4	0	0	0	3	5	0	0	0	3	7	1	0	0	3	1	0	0	0	49
5	LAMPUNG	3	8	0	0	0	6	13	0	0	0	0	0	0	0	0	0	3	0	0	0	3	3	0	0	0	3	8	0	0	0	0	2	0	0	0	45
6	MAKASSAR	7	4	0	0	0	1	8	0	0	0	1	3	0	0	0	2	3	0	0	0	3	7	0	0	0	1	4	0	0	0	0	2	0	0	0	48
7	MATARAM	3	14	0	0	0	6	4	0	0	0	0	0	0	0	0	2	3	0	0	0	3	5	0	0	0	7	4	0	0	0	0	0	0	0	0	51
8	MEDAN	3	9	0	0	0	0	9	0	0	0	1	4	0	0	0	1	4	0	0	0	0	1	0	0	0	6	8	0	0	0	1	3	0	0	0	50
9	PEKANBARU	5	6	0	3	0	4	6	0	1	0	0	0	0	0	0	0	3	1	0	0	4	3	0	0	0	8	3	0	0	0	0	0	0	0	0	50
10	PALU	3	3	0	2	0	8	6	0	2	0	0	0	0	0	0	5	2	0	1	0	4	2	0	1	0	4	5	0	0	0	0	0	0	0	0	47
11	PONTIANAK	3	15	0	0	0	3	6	0	0	0	0	0	0	0	0	2	3	0	0	0	3	3	0	0	0	3	2	0	0	0	1	4	0	0	0	48
	JUMLAH	45	94	0	5	0	40	81	0	3	0	2	7	0	1	0	17	34	1	1	0	38	36	0	3	0	48	46	1	2	0	6	16	0	1	0	528

JUMLAH (%) A= 37.12% B= 59.47% C= 0.38% D= 3.03%

10. Berkaitan dengan cybercrime dan masalah yurisdiksi peradilan, dimana hukum suatu negara tidak dapat menjangkau pelaku kejahatan di luar negaranya, perlukah diatur secara khusus mengenai cara dan tempat mengajukan gugatan bila terjadi sengketa
    a. Perlu
    b. Tidak perlu, karena masih dapat digunakan pasal 118 HIR/154 RBG
    c. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																			JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	10	3	0	0	0	4	6	0	0	0	0	0	0	0	0	4	0	0	0	0	4	2	0	0	0	3	1	0	0	0	4	0	1	0	0	42
2	BANJARMASIN	10	1	0	0	0	11	3	0	0	0	0	0	0	0	0	4	3	0	0	0	7	0	0	0	0	4	1	0	0	0	1	1	0	0	0	46
3	BENGKULU	12	2	0	0	0	9	4	0	0	0	0	0	0	0	0	5	0	0	0	0	4	5	0	0	0	7	4	0	0	0	0	0	0	0	0	52
4	DENPASAR	8	6	0	0	0	2	2	0	0	0	0	0	0	0	0	5	0	0	0	0	7	1	0	0	0	10	2	0	0	0	2	0	3	0	0	49
5	LAMPUNG	6	4	1	0	0	8	10	1	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	5	4	0	0	0	0	0	0	0	0	45
6	MAKASSAR	8	3	0	0	0	8	1	0	0	0	5	0	0	0	0	3	1	0	1	0	5	5	0	0	0	6	0	0	0	0	2	0	0	0	0	48
7	MATARAM	17	0	0	0	0	9	1	0	0	0	0	0	0	0	0	4	1	0	0	0	7	1	0	0	0	9	2	0	0	0	0	0	0	0	0	51
8	MEDAN	8	3	1	0	0	7	1	1	0	0	4	1	0	0	0	4	0	1	0	0	1	0	0	0	0	13	1	0	0	0	3	0	1	0	0	50
9	PEKANBARU	8	3	3	0	0	9	2	0	0	0	0	0	0	0	0	3	1	0	1	0	7	1	0	1	0	6	5	0	0	0	0	0	0	0	0	50
10	PALU	7	1	0	0	0	6	6	4	0	0	0	0	0	0	0	7	0	0	0	0	4	1	0	0	0	4	5	0	0	0	0	0	0	0	0	47
11	PONTIANAK	14	2	2	0	0	7	2	0	0	0	0	0	0	0	0	3	2	0	0	0	4	2	0	0	0	2	3	0	0	0	4	1	0	0	0	48
	JUMLAH	109	28	7	0	0	80	38	6	0	0	9	1	0	0	0	42	8	3	0	0	58	18	1	0	0	69	28	0	0	0	16	6	1	0	0	528

JUMLAH (%) A= 72.54% B= 24.05% C= 3.41%

11. Menurut saudara bisakah ketentuan didalam KUH Perdata diterapkan dengan cara penafsiran terhadap kasus-kasus e-commerce yang khusus terjadi di Indonesia atau perlu dibuat ketentuan khusus mengenai kasus e-commerce?
    a. Bisa
    b. Tidak bisa
    c. Perlu dibuat ketentuan khusus
    d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																			JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	4	0	9	0	0	3	0	7	0	0	0	0	0	0	0	0	0	4	0	0	1	0	4	0	0	0	0	4	0	0	1	0	4	0	0	42
2	BANJARMASIN	2	0	9	0	0	3	0	11	0	0	0	0	0	0	0	1	0	6	0	0	0	0	7	0	0	0	0	5	0	0	1	0	0	0	0	46
3	BENGKULU	4	0	10	0	0	3	0	10	0	0	0	0	0	0	0	0	0	5	0	0	1	0	7	0	0	0	0	10	0	0	0	0	0	0	0	52
4	DENPASAR	6	0	9	0	0	1	0	3	0	0	0	0	0	0	0	0	0	5	0	0	1	0	7	0	0	1	0	11	0	0	0	0	3	0	0	49
5	LAMPUNG	3	0	8	0	0	5	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	0	0	2	0	7	0	0	0	0	0	0	0	45
6	MAKASSAR	3	0	8	0	0	2	0	7	0	0	1	0	4	0	0	1	0	4	0	0	5	0	5	0	0	0	0	6	0	0	0	0	2	0	0	48
7	MATARAM	2	2	13	0	0	0	0	10	0	0	0	0	0	0	0	1	0	4	0	0	4	0	4	0	0	2	0	9	0	0	0	0	0	0	0	51
8	MEDAN	2	0	10	0	0	1	0	8	0	0	1	0	4	0	0	2	0	3	0	0	0	0	1	0	0	3	0	10	0	0	0	0	4	0	0	50
9	PEKANBARU	1	0	10	3	0	3	0	8	0	0	0	0	0	0	0	2	0	2	1	0	2	0	7	0	0	0	0	11	0	0	0	0	0	0	0	50
10	PALU	1	0	5	2	0	3	0	11	2	0	0	0	0	0	0	3	0	4	0	0	1	1	6	0	0	0	0	9	0	0	0	0	0	0	0	47
11	PONTIANAK	4	0	14	0	0	1	0	8	0	0	0	0	0	0	0	1	0	4	0	0	1	1	4	0	0	0	0	4	0	0	2	0	0	0	0	48
	JUMLAH	32	2	105	5	0	25	0	97	2	0	2	0	8	0	0	11	0	41	1	0	16	3	49	8	1	8	2	86	2	0	4	0	17	1	0	528

JUMLAH (%) A= 18.56% B= 1.33% C= 76.33% D= 3.60%

12. Setujukah saudara apabila didalam kontrak secara elektronik digunakan tanda tangan elektronik (digital signature) atau dituangkan dalam bentuk tertulis?
    a. Setuju
    b. Setuju untuk yang sifatnya sederhana
    c. Tidak setuju
    d. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	D	E	D	
1	BANDUNG	4	5	0	4	0	6	4	0	0	0	0	0	0	0	0	3	0	1	0	0	1	2	2	1	0	2	0	2	0	0	2	1	0	2	0	42
2	BANJARMASIN	10	0	0	1	0	9	3	1	1	0	0	0	0	0	0	6	0	1	0	0	7	0	0	0	0	4	0	1	0	0	1	1	0	0	0	46
3	BENGKULU	8	4	2	0	0	10	0	3	0	0	0	0	0	0	0	3	2	0	0	0	2	2	5	0	0	7	3	1	1	0	0	3	0	0	0	52
4	DENPASAR	9	2	1	3	0	1	0	3	0	0	0	0	0	0	0	2	2	0	1	0	3	1	0	4	0	4	1	1	6	0	1	3	0	1	0	49
5	LAMPUNG	7	3	1	0	0	13	3	3	0	0	0	0	0	0	0	0	0	0	0	0	2	3	1	0	0	3	0	5	1	0	0	0	0	0	0	45
6	MAKASSAR	7	4	0	0	0	4	1	3	1	0	1	3	0	1	0	3	1	0	0	0	6	4	3	0	0	4	0	5	1	0	0	0	0	2	0	48
7	MATARAM	12	0	5	0	0	8	1	1	0	0	0	0	0	0	0	5	0	0	0	0	2	3	3	0	0	6	3	3	2	0	0	0	0	0	0	51
8	MEDAN	6	0	5	1	0	6	1	2	0	0	2	1	2	0	0	4	0	1	0	0	0	1	0	0	0	7	3	4	0	0	1	3	0	0	0	50
9	PEKANBARU	5	2	0	7	0	3	0	1	7	0	0	0	0	0	0	0	2	0	3	0	4	2	1	0	0	2	1	1	7	0	0	0	0	0	0	50
10	PALU	3	0	5	0	0	8	2	3	0	0	0	0	0	0	0	4	1	2	0	0	1	3	1	0	0	0	2	4	0	0	0	0	0	0	0	47
11	PONTIANAK	12	3	3	0	0	8	0	1	0	0	0	0	0	0	0	1	3	1	0	0	5	0	1	0	0	1	2	2	0	0	3	1	0	0	0	48
	JUMLAH	83	23	22	16	0	76	15	21	12	0	3	4	2	1	0	31	11	7	4	0	34	21	13	9	0	40	21	20	16	0	8	9	3	3	0	528

JUMLAH (%) A= 52.08% B= 19.70% C= 16.67% D= 11.55%

13. Menurut saudara apakah tanda tangan elektronik harus didaftarkan terlebih dahulu, baru sah digunakan oleh pemiliknya, demi keamanan pihak-pihak yang terlibat dalam kontrak itu dan dengan didaftarkannya tanda tangan tersebut, apakah sudah menjamin para pihak yang bersangkutan?
    a. Ya
    b. Sudah menjamin
    c. Tidak menjamin
    d. Jelaskan
    e. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	3	6	4	0	0	3	4	3	0	0	0	0	0	0	0	3	0	1	0	0	2	2	2	0	0	1	1	2	0	0	2	1	2	0	0	42
2	BANJARMASIN	6	2	3	0	0	7	3	4	0	0	0	0	0	0	0	3	1	3	0	0	7	0	0	0	0	4	0	1	0	0	2	0	0	0	0	46
3	BENGKULU	6	5	3	0	0	1	0	10	2	0	0	0	0	0	0	1	0	4	0	0	1	1	7	0	0	3	2	6	0	0	0	0	0	0	0	52
4	DENPASAR	5	4	3	3	0	0	1	2	1	0	0	0	0	0	0	1	0	3	1	0	1	1	1	5	0	1	2	3	6	0	1	0	2	1	0	49
5	LAMPUNG	2	0	9	0	0	7	4	8	0	0	0	0	0	0	0	0	0	0	0	0	2	1	2	0	0	2	2	7	0	0	0	0	0	0	0	45
6	MAKASSAR	6	2	3	0	0	4	0	5	0	0	1	2	2	0	0	2	3	0	0	0	8	1	1	0	0	2	0	3	1	0	0	0	5	2	0	48
7	MATARAM	4	6	7	0	0	1	2	7	0	0	0	0	0	0	0	0	0	0	0	0	2	1	2	0	0	2	3	3	0	0	2	5	1	5	0	51
8	MEDAN	5	2	5	0	0	3	3	3	0	0	1	1	3	0	0	0	4	1	0	0	1	0	1	0	0	3	3	8	0	0	2	0	2	0	0	50
9	PEKANBARU	5	3	1	5	0	3	1	1	6	0	0	0	0	0	0	0	1	0	4	0	4	0	1	4	0	2	0	3	2	0	0	0	0	0	0	50
10	PALU	4	0	4	0	0	4	4	4	4	0	0	0	0	0	0	2	3	2	0	0	1	4	2	1	0	3	2	4	4	0	2	0	0	0	0	47
11	PONTIANAK	5	9	4	0	0	4	2	3	0	0	0	0	0	0	0	3	1	1	0	0	3	0	2	1	0	1	0	2	0	0	2	1	2	0	0	48
	JUMLAH	51	39	46	8	0	37	24	50	13	0	2	3	5	0	0	15	13	15	5	0	32	12	20	10	0	24	20	36	14	0	14	5	14	1	0	528

JUMLAH (%) A= 33.14% B= 21.97% C= 35.23% D= 9.66% E= 0.00%

14. Bagaimana tanggungjawab internet service provider (ISP) terhadap pihak-pihak yang merasa dirugikan baik secara materiil maupun immateriil akibat perbuatan orang lain yang dilakukan melaui internet?
    a. ISP bertanggungjawab
    b. ISP bertanggungjawab apabila ia ikut terlibat
    c. ISP tidak bertanggungjawab, karena tidak mungkin ia melakukan pengawasan terhadap sedemikian banyak pengguna jasa internet
    d. Jelaskan
    e. Tidak mengisi

NOMOR	LOKASI	JENIS PERADILAN																																				JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	1	7	4	1	0	2	6	2	0	0	0	0	0	0	0	1	0	3	1	0	1	4	0	0	0	0	1	3	0	0	1	2	2	0	0	42
2	BANJARMASIN	2	3	6	0	0	4	6	4	0	0	0	0	0	0	0	1	3	3	0	0	0	0	7	0	0	1	0	4	3	0	1	1	0	0	0	46
3	BENGKULU	8	4	2	0	0	3	5	5	0	0	0	0	0	0	0	1	1	3	0	0	3	0	6	0	0	2	5	4	0	0	0	0	0	0	0	52
4	DENPASAR	1	6	7	1	0	0	1	3	0	0	0	0	0	0	0	1	2	2	0	0	0	5	3	0	0	0	6	6	0	0	1	3	1	0	0	49
5	LAMPUNG	0	4	7	0	0	1	11	7	0	0	0	0	0	0	0	0	0	0	0	0	1	0	5	0	0	0	7	2	0	0	0	0	0	0	0	45
6	MAKASSAR	1	6	2	2	0	1	3	5	0	0	3	1	1	0	0	0	3	2	0	0	0	5	3	0	0	1	1	4	0	0	0	1	0	0	0	48
7	MATARAM	4	9	4	0	0	1	1	7	1	0	0	0	0	0	0	1	2	2	0	0	1	0	3	1	0	2	3	5	1	0	0	0	0	0	0	51
8	MEDAN	1	6	4	1	0	0	3	6	0	0	1	1	3	0	0	0	3	1	1	0	0	0	1	0	0	1	2	9	0	0	0	2	2	0	0	50
9	PEKANBARU	2	6	3	3	0	1	8	2	0	0	0	0	0	0	0	0	2	2	1	0	0	5	2	0	0	0	7	4	0	0	0	0	0	0	0	50
10	PALU	2	1	5	0	0	4	2	6	1	0	0	0	0	0	0	0	2	5	0	0	0	3	4	0	0	1	5	2	1	0	0	0	0	0	0	47
11	PONTIANAK	4	10	4	0	0	1	3	4	1	0	0	0	0	0	0	0	2	2	1	0	1	2	3	0	0	1	1	3	0	0	0	1	4	0	0	48
	JUMLAH	26	62	48	8	0	18	49	51	6	0	4	2	4	0	0	5	20	25	4	0	7	27	37	5	0	9	38	46	4	0	3	10	10	0	0	528

JUMLAH (%) A= 13.64% B= 39.39% C= 41.86% D= 5.11% E= 0.00%

15. Menurut saudara perlukah diatur dalam ketentuan hukum mengenai kewajiban-kewajiban ISP terhadap customer maupun pihak lain yang dirugikan dan untuk menyimpan data untuk beberapa jangka waktu?
    a. Perlu
    b. Tidak perlu
    c. Tidak mengisi
    d. Jelaskan pendapat saudara

NOMOR	LOKASI	JENIS PERADILAN																																				JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	0	1	0	0	10	0	0	0	0	0	0	0	0	0	3	1	0	0	0	6	0	0	0	0	4	0	0	0	0	4	0	1	0	0	42
2	BANJARMASIN	11	0	0	0	0	13	1	0	0	0	0	0	0	0	0	7	0	0	0	0	7	0	0	0	0	5	0	0	0	0	2	0	0	0	0	46
3	BENGKULU	13	0	1	0	0	13	0	0	0	0	0	0	0	0	0	5	0	0	0	0	9	0	0	0	0	11	0	0	0	0	0	0	0	0	0	52
4	DENPASAR	15	0	0	0	0	4	0	0	0	0	0	0	0	0	0	5	0	0	0	0	7	1	0	0	0	10	2	0	0	0	4	1	0	0	0	49
5	LAMPUNG	9	2	0	0	0	18	1	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	1	0	0	9	1	0	0	0	0	0	0	0	0	45
6	MAKASSAR	11	0	0	0	0	8	1	0	0	0	5	0	0	0	0	5	0	0	0	0	8	1	1	0	0	5	1	0	0	0	2	0	0	0	0	48
7	MATARAM	17	0	0	0	0	10	0	1	0	0	0	0	0	0	0	5	0	0	0	0	6	1	1	0	0	9	2	1	0	0	0	0	0	0	0	51
8	MEDAN	11	0	1	0	0	8	0	1	0	0	4	1	0	0	0	5	0	0	0	0	1	0	0	0	0	11	2	1	0	0	3	0	0	0	0	50
9	PEKANBARU	11	0	3	0	0	11	0	1	0	0	0	0	0	0	0	4	0	1	0	0	7	1	1	0	0	10	1	0	0	0	0	0	0	0	0	50
10	PALU	8	0	0	0	0	15	0	1	0	0	0	0	0	0	0	7	0	0	0	0	5	2	0	0	0	8	1	0	0	0	0	0	0	0	0	47
11	PONTIANAK	18	0	0	0	0	8	0	1	0	0	0	0	0	0	0	4	0	1	0	0	6	0	0	0	0	5	0	0	0	0	5	0	0	0	0	48
	JUMLAH	136	2	6		0	118	3	3		0	9	1	0		0	50	1	2		0	68	6	3		0	67	8	2		0	20	1	2		0	528

JUMLAH (%) A= 92.42% B= 4.17% C= 3.41% D= 0.00%

16. Apakah memasukkan file-file elektronik kedalam komputer-komputer personal users internet tanpa sepengetahuan users yang bersangkutan, dipandang sebagai pelanggaran hukum (junk mail = e-mail sampah)?
    a. Ya, pelanggaran hukum
    b. Bukan pelanggaran hukum
    c. Tidak mengisi
    d. Jelaskan pendapat saudara

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	1	0	0	0	9	0	1	0	0	0	0	0	0	0	2	0	2	0	0	5	1	0	0	0	4	0	0	0	0	3	1	1	0	0	42
2	BANJARMASIN	9	2	0	0	0	6	8	0	0	0	0	0	0	0	0	5	2	0	0	0	0	7	0	0	0	1	4	0	0	0	2	0	0	0	0	46
3	BENGKULU	14	0	0	0	0	8	5	0	0	0	0	0	0	0	0	0	4	1	0	0	5	4	0	0	0	8	1	2	0	0	0	0	0	0	0	52
4	DENPASAR	10	5	0	0	0	2	2	0	0	0	0	0	0	0	0	2	2	1	0	0	7	1	0	0	0	10	2	0	0	0	4	1	0	0	0	49
5	LAMPUNG	8	2	1	0	0	10	9	0	0	0	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	9	0	0	0	0	1	0	0	0	0	45
6	MAKASSAR	10	0	1	0	0	6	2	1	0	0	5	0	0	0	0	3	2	0	0	0	8	1	1	0	0	4	2	0	0	0	1	1	0	0	0	48
7	MATARAM	12	4	1	0	0	3	5	2	0	0	0	0	0	0	0	4	1	0	0	0	5	2	1	0	0	7	4	0	0	0	0	0	0	0	0	51
8	MEDAN	8	3	1	0	0	8	0	1	0	0	3	1	1	0	0	3	1	1	0	0	6	3	0	0	0	10	3	1	0	0	3	0	0	1	0	50
9	PEKANBARU	8	3	3	0	0	7	4	0	0	0	0	0	0	0	0	4	1	1	0	0	6	1	0	0	0	9	2	0	0	0	0	0	0	0	0	50
10	PALU	5	0	3	0	0	12	0	2	2	0	0	0	0	0	0	5	1	1	0	0	6	1	0	0	0	7	2	0	0	0	0	0	0	0	0	47
11	PONTIANAK	15	3	0	0	0	5	4	0	0	0	0	0	0	0	0	3	1	1	0	0	6	0	0	0	0	4	1	0	0	0	2	3	0	0	0	48
	JUMLAH	111	23	10	0	0	76	39	7	2	0	8	1	1	0	0	31	14	8	0	0	54	21	2	0	0	73	21	3	0	0	15	6	2	0	0	528

JUMLAH (%) A= 69.70% B= 23.67% C= 6.25% D= 0.38%

17. Menurut saudara perlukah diatur mengenai jaminan keamanan bagi para pengguna internet yang berbelanja lewat internet, di dalam melakukan pembayaran dengan kartu kredit, agar kartu kreditnya tidak digunakan orang lain tanpa seijin pemilik kartu kredit tersebut?
    a. Perlu
    b. Tidak perlu
    c. Tidak mengisi
    d. Apa ide/solusi saudara mengena hal ini jelaskan

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	13	0	0	0	0	10	0	0	0	0	0	0	0	0	0	3	1	0	0	0	5	1	0	0	0	4	0	0	0	0	4	0	0	1	0	42
2	BANJARMASIN	9	2	0	0	0	13	1	0	0	0	0	0	0	0	0	7	0	0	0	0	7	0	0	0	0	5	0	0	0	0	2	0	0	0	0	46
3	BENGKULU	13	0	0	1	0	13	0	0	0	0	0	0	0	0	0	4	1	0	0	0	7	2	0	0	0	11	0	0	0	0	0	0	0	0	0	52
4	DENPASAR	15	0	0	0	0	4	0	0	0	0	0	0	0	0	0	4	1	0	0	0	8	0	0	0	0	12	0	0	0	0	5	0	0	0	0	49
5	LAMPUNG	10	1	0	0	0	17	1	1	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	9	0	0	0	0	0	0	0	0	0	45
6	MAKASSAR	10	1	0	0	0	9	0	0	0	0	5	0	0	0	0	5	0	0	0	0	8	0	0	2	0	6	0	0	0	0	2	0	0	0	0	48
7	MATARAM	17	0	0	0	0	10	0	0	0	0	0	0	0	0	0	5	0	0	0	0	6	1	0	1	0	10	0	0	0	0	0	0	0	0	0	51
8	MEDAN	11	1	0	0	0	8	1	0	0	0	4	0	0	1	0	5	0	0	0	0	1	0	0	0	0	14	0	0	0	0	4	0	0	0	0	50
9	PEKANBARU	11	0	0	3	0	9	2	0	0	0	0	0	0	0	0	3	1	0	1	0	8	1	0	0	0	9	2	0	0	0	0	0	0	0	0	50
10	PALU	6	0	1	1	0	15	0	0	1	0	0	0	0	0	0	7	0	0	0	0	6	1	0	0	0	6	3	0	0	0	0	0	0	0	0	47
11	PONTIANAK	18	0	0	0	0	9	0	0	0	0	0	0	0	0	0	3	1	0	1	0	6	0	0	0	0	5	0	0	0	0	5	0	0	0	0	48
	JUMLAH	133	5	1	5	0	117	5	1	1	0	9	0	0	1	0	46	5	0	2	0	68	5	0	4	0	91	5	1	0	0	22	0	0	1	0	528

JUMLAH (%) A= 92.05% B= 4.73% C= 0.57% D= 2.65%

18. Menurut saudara dengan semakin pesatnya perkembangan perdagangan international terutama melaui internet (e-commerce), perlukah sistem pembuktian hukum acara kita baik acara pidana (KUHAP) maupun acara Perdata HIR/RBG, dirubah dan disesuaikan dengan kebutuhan pembuktian sehubungan dengan kontrak melalui internet tersebut?
    a. Perlu
    b Tidak perlu
    c. Tidak mengisi
    d. Jelaskan pendapat saudara

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	10	3	0	0	0	10	0	0	0	0	0	0	0	0	0	4	0	0	0	0	6	0	0	0	0	4	0	0	0	0	4	0	1	0	0	42
2	BANJARMASIN	9	2	0	0	0	11	3	0	0	0	0	0	0	0	0	7	0	0	0	0	0	7	0	0	0	1	4	0	0	0	2	0	0	0	0	46
3	BENGKULU	13	1	0	0	0	11	2	0	0	0	0	0	0	0	0	4	1	0	0	0	9	0	0	0	0	11	0	0	0	0	0	0	0	0	0	52
4	DENPASAR	15	0	0	0	0	2	2	0	0	0	0	0	0	0	0	4	0	1	0	0	8	0	0	0	0	12	0	0	0	0	5	0	0	0	0	49
5	LAMPUNG	7	4	0	0	0	17	2	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	8	1	0	0	0	0	0	0	0	0	45
6	MAKASSAR	10	1	0	0	0	9	0	0	0	0	5	0	0	0	0	3	2	0	0	0	9	1	0	0	0	5	0	1	0	0	2	0	0	0	0	48
7	MATARAM	13	4	0	0	0	9	1	0	0	0	0	0	0	0	0	3	2	0	0	0	7	0	1	0	0	8	3	0	0	0	0	0	0	0	0	51
8	MEDAN	12	0	0	0	0	9	0	0	0	0	5	0	0	0	0	3	2	0	0	0	1	0	0	0	0	13	0	1	0	0	4	0	0	0	0	50
9	PEKANBARU	10	1	3	0	0	10	1	0	0	0	0	0	0	0	0	3	1	1	0	0	8	0	1	0	0	10	1	0	0	0	0	0	0	0	0	50
10	PALU	8	0	0	0	0	13	0	3	0	0	0	0	0	0	0	5	1	1	0	0	6	1	0	0	0	7	2	0	0	0	0	0	0	0	0	47
11	PONTIANAK	17	1	0	0	0	9	0	0	0	0	0	0	0	0	0	3	2	0	0	0	4	2	0	0	0	3	2	0	0	0	5	0	0	0	0	48
	JUMLAH	124	17	3	0	0	110	11	3	0	0	10	0	0	0	0	39	11	3	0	0	64	11	2	0	0	82	13	2	0	0	22	0	1	0	0	528

JUMLAH (%) A= 85.42% B= 11.93% C= 2.65% D= 0.00%

19. Apabila merk dagang milik seseorang atau badan hukum yang telah diaftarkan sebagai mana domein idi internet digunakan oleh orang lain tanpa seijin atau sepengetahuan pemiliknya, dapat dikatagorikan sebagai perbuatan melawan hukum
    a. Merupakan perbuatan melawan hukum
    b. Tidak dapat dikatagorikan sebagai perbuatan melawan hukum
    c. Tidak mengisi
    d. Jelaskan pendapat saudara

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	1	0	0	0	10	0	0	0	0	0	0	0	0	0	4	0	0	0	0	5	1	0	0	0	4	0	0	0	0	4	0	1	0	0	42
2	BANJARMASIN	11	0	0	0	0	11	3	0	0	0	0	0	0	0	0	7	0	0	0	0	0	7	0	0	0	1	4	0	0	0	2	0	0	0	0	46
3	BENGKULU	14	0	0	0	0	12	1	0	0	0	0	0	0	0	0	5	0	0	0	0	8	1	0	0	0	11	0	0	0	0	0	0	0	0	0	52
4	DENPASAR	12	3	0	0	0	4	0	0	0	0	0	0	0	0	0	2	3	0	0	0	8	0	0	0	0	12	0	0	0	0	5	0	0	0	0	49
5	LAMPUNG	9	2	0	0	0	18	1	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	9	0	0	0	0	0	0	0	0	0	45
6	MAKASSAR	11	0	0	0	0	8	1	0	0	0	4	0	1	0	0	5	0	0	0	0	9	1	0	0	0	6	0	0	0	0	2	0	0	0	0	48
7	MATARAM	14	3	0	0	0	3	7	0	0	0	0	0	0	0	0	5	0	0	0	0	7	0	1	0	0	10	1	0	0	0	0	0	0	0	0	51
8	MEDAN	12	0	0	0	0	8	1	0	0	0	4	0	1	0	0	5	0	0	0	0	1	0	0	0	0	11	2	1	0	0	4	0	0	0	0	50
9	PEKANBARU	11	2	1	0	0	10	1	0	0	0	0	0	0	0	0	3	1	0	0	0	7	1	0	0	0	11	0	0	0	0	0	0	0	0	0	50
10	PALU	8	0	0	0	0	15	1	0	0	0	0	0	0	0	0	6	1	0	0	0	6	1	0	0	0	9	1	0	0	0	0	0	0	0	0	47
11	PONTIANAK	16	1	1	0	0	9	0	0	0	0	0	0	0	0	0	5	0	0	0	0	5	1	0	0	0	4	1	0	0	0	3	2	0	0	0	48
	JUMLAH	130	12	2	0	0	108	16	0	0	0	6	0	2	0	0	47	5	1	0	0	62	13	2	0	0	88	8	1	0	0	20	2	1	0	0	528

JUMLAH (%) A= 87.69% B= 10.61% C= 1.70% D= 0.00%

20. Bagaimana pendapat saudara persidangan dengan menggunakan teleconference, baik untuk didengar saksi, maupun para pihak yang berperkara (persidangan tidak dihadiri oleh para pihak yang berperkara secara phisik)?
    a. Setuju, dan persidangan tersebut tetap sah
    b. Tidak setuju, dan persidangan tidak sah
    c. Tidak mengisi
    d. Jelaskan pendapat saudara

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	1	0	0	0	9	1	0	0	0	0	0	0	0	0	4	0	0	0	0	3	3	0	0	0	2	0	2	0	0	2	1	1	1	0	42
2	BANJARMASIN	3	8	0	0	0	11	3	0	0	0	0	0	0	0	0	6	1	0	0	0	0	7	0	0	0	1	4	0	0	0	2	0	0	0	0	46
3	BENGKULU	9	5	0	0	0	11	2	0	0	0	0	0	0	0	0	3	1	1	0	0	5	4	0	0	0	5	5	1	0	0	0	0	0	0	0	52
4	DENPASAR	15	0	0	0	0	4	0	0	0	0	0	0	0	0	0	2	3	0	0	0	7	1	0	0	0	10	1	0	1	0	3	2	0	0	0	49
5	LAMPUNG	11	0	0	0	0	15	3	1	0	0	0	0	0	0	0	0	0	0	0	0	2	4	0	0	0	9	0	0	0	0	0	0	0	0	0	45
6	MAKASSAR	10	1	0	0	0	8	1	0	0	0	4	1	0	0	0	5	0	0	0	0	8	2	0	0	0	6	0	0	0	0	0	2	0	0	0	48
7	MATARAM	16	1	0	0	0	9	0	1	0	0	0	0	0	0	0	4	0	1	0	0	4	2	0	2	0	10	0	1	0	0	0	0	0	0	0	51
8	MEDAN	7	3	1	1	0	8	1	0	0	0	5	0	0	0	0	5	0	0	0	0	6	1	0	0	0	11	2	0	1	0	2	0	0	0	0	50
9	PEKANBARU	10	2	1	1	0	9	2	0	0	0	0	0	0	0	0	4	0	0	1	0	6	2	0	1	0	8	3	0	0	0	0	0	0	0	0	50
10	PALU	8	0	0	0	0	9	6	0	1	0	0	0	0	0	0	4	2	0	1	0	2	4	1	0	0	4	5	0	0	0	0	0	0	0	0	47
11	PONTIANAK	14	4	0	0	0	6	3	0	0	0	0	0	0	0	0	4	0	1	0	0	2	2	1	1	0	5	0	0	0	0	5	0	0	0	0	48
	JUMLAH	115	25	2	2	0	99	22	2	1	0	9	1	0	0	0	41	7	3	2	0	39	32	2	4	0	71	20	4	2	0	14	7	1	1	0	528

JUMLAH (%) A= 73.48% B= 21.59% C= 2.65% D= 2.27%

21. Bagaimana pendapat saudara apakah memungkinkan di Indonesia gugatan / permohonan didaftarkan ke Pengadilan melaui komputer/e-mail (e-court)?
    a. Perlu
    b. Tidak perlu
    c. Tidak mengisi
    d. Berikan alasannya

NOMOR	LOKASI	JENIS PERADILAN																																		JUMLAH
		PT					PN					PTTUN					PTUN					PTA					PA					MAHMIL					
		A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	
1	BANDUNG	12	1	0	0	0	9	1	0	0	0	0	0	0	0	0	4	0	0	0	0	4	2	0	0	0	2	2	0	0	0	2	2	1	0	0	42
2	BANJARMASIN	9	2	0	0	0	10	4	0	0	0	0	0	0	0	0	7	0	0	0	0	7	0	0	0	0	5	0	0	0	0	2	0	0	0	0	46
3	BENGKULU	11	3	0	0	0	5	7	1	0	0	0	0	0	0	0	4	1	0	0	0	7	2	0	0	0	8	3	0	0	0	0	1	0	0	0	52
4	DENPASAR	13	2	0	0	0	3	1	0	0	0	0	0	0	0	0	3	2	0	0	0	6	2	0	0	0	8	4	0	0	0	4	1	0	0	0	49
5	LAMPUNG	5	6	0	0	0	11	8	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	0	0	0	8	1	0	0	0	0	0	0	0	0	45
6	MAKASSAR	8	3	0	0	0	5	4	0	0	0	1	1	3	0	0	3	2	0	0	0	7	3	0	0	0	2	4	0	0	0	2	0	0	0	0	48
7	MATARAM	15	2	0	0	0	4	6	0	0	0	0	0	0	0	0	3	2	0	0	0	6	2	0	0	0	8	3	0	0	0	0	0	0	0	0	51
8	MEDAN	4	7	1	0	0	2	7	0	0	0	5	0	0	0	0	5	0	0	0	0	1	0	0	0	0	12	0	2	0	0	3	1	0	0	0	50
9	PEKANBARU	10	2	2	0	0	5	6	0	0	0	0	0	0	0	0	2	2	1	0	0	4	3	0	2	0	7	4	0	0	0	0	0	1	0	0	50
10	PALU	3	2	3	0	0	9	6	1	0	0	0	0	0	0	0	4	3	0	0	0	3	4	0	0	0	5	4	0	0	0	0	0	0	0	0	47
11	PONTIANAK	16	2	0	0	0	4	5	0	0	0	0	0	0	0	0	5	0	0	0	0	5	1	0	0	0	4	1	0	0	0	2	3	0	0	0	48
	JUMLAH	106	32	6	0	0	67	55	2	0	0	6	1	3	0	0	40	12	1	0	0	54	21	2	0	0	69	26	2	0	0	15	7	1	0	0	528

JUMLAH (%) A= 67.61% B= 29.17% C= 3.22% D= 0.00%

BAB VI
E-COMMERCE DAN ASPEK PERDATANYA

Perkembangan tehnologi sekarang ini, telah memungkinkan dilakukannya hubungan bisnis melalui perangkat tehnologi yang disebut dengan *internet.* Perkembangan tehnologi tersebut telah menimbulkan paradigma baru dalam melakukan kontrak di antara pelaku bisnis. Secara konvensional, pelaku bisnis dalam membuat suatu kontrak atau transaksi mangadakan pertemuan secara *face to face* lalu membubuhkan tanda tangan sebagai pertanda penerimaan kesepakatan yang tertuang dalam *contract* tersebut. Namun dengan perkembangan tehnologi, pihak-pihak yang terkait dalam suatu transaksi tidak perlu lagi bertemu secara *face to face,* cukup melalui peralatan komputer dan telekomunikasi, transaksi yang demikian ini lebih dikenal dengan transaksi *e-commerce.*

Disatu sisi tehnologi komputer dan telekomunikasi mempunyai dampak positif dimana para pelaku bisnis lebih mudah dalam menjalankan usahanya, karena dapat menghemat waktu dan tenaga. Namun disisi lain tehnologi ini menimbulkan dampak negatif dimana pihak-pihak tertentu dengan itikad tidak baik mencari keuntungan dengan melawan hukum (cybercrime).

Negara-negara di dunia memberikan istilah yang berbeda-beda untuk perdagangan atau transaksi secara elektronik. Ada yang menggunakan istilah E-Commerce (Electronic Commerce) dan ada juga yang menggunakan istilah Electronic Transaction.

Defenisi E-commmerce atau Electronic Transaction dapat dikatakan secara gampang adalah transaksi atau perdagangan yang dilakukan secara elektronik. Menurut United Nations Commission on International Trade Law (UNCITRAL) yang dimaksud dengan E-Commerce adalah :"... transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information".

Selanjutnya yang dimaksud dengan EDI (Electronic Data Interchange) adalah : [115]"Electronic data interchange (EDI)" means the electronic transfer

[115] Terjemahannya adalah '...transaksi-transaksi dalam perdagangan internasional yang dilakukan dengan cara pertukaran data elektronik yang menyangkut penggunaan alternatif-alternatif atas metode-metode komunikasi dan penyimpanan informasi yang didasarkan pada kertas'

from computer to computer of information using an agreed standard to structure the information",[116]

Dan yang dimaksud dengan data message adalah " information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy"[117] Dari pengertian di atas dapat disimpulkan bahwa transaksi elektronik mencakup informasi yang diperoleh, dikirim, diterima atau disimpan secara eletronic dengan cara yang sama atau hampir sama yang meliputi, namun tidak terbatas pada, e-mail, EDI, telegram, telex atau telecopy.

Transaksi secara elektronik yang melahirkan dokumen elektronik menimbulkan masalah baru dalam sistem hukum karena sistem hukum (konvensional) tidak mengenal dokumen elektronik. Untuk itu telah dibuat peraturan-peraturan hukum yang dapat mengakomodir transaksi elektronik (e-commerce).

Peraturan hukum e-commece adalah phenomena yang sangat baru di tingkat nasional maupun internasional. Semua peraturan e-commerce adalah berkisar pada masalah sahnya transaksi e-commerce. Paling banyak negara-negara berusaha memecahkan masalah ini dengan mengeluarkan peraturan tanda tangan digital *(digital signature legislation)* atau peraturan tanda tangan elektronic (*electronic signature legislation)*

The American Bar Association yang pertama mengembangkan seperangkat pedoman tanda tangan digital (Digital Signature Guidelines) yang berkenaan dengan masalah hukum yang timbul dari tanda tangan digital, pedoman mana dikenal dengan *ABA Guideline 1995*. Kemudian berkembanglah peraturan-peraturan tanda tangan digital dan tanda tangan elektronik. Negara bagian Amerika Serikat Utah memperlakukan peraturan tanda tangan digital pada bulan Mei 1995 yang dikenal dengan *Utah Act*

The ABA Guidelines dan *the Utah Act* menjadi terkenal baik ditingkat nasioanl maupun internasional dan menjadi model peraturan tanda tangan digital yang ditiru oleh negara-negara bagian Amerika Serikat lainnya dan negara-negara lain di dunia. Peraturan-peraturan *Guidelines* dan *the Utah Act* tersebut berfokus pada tanda tangan digital. Namun peraturan-peraturan yang lahir kemudian berkembang dari peraturan yang berfokus tanda tangan digital pada khususnya ke peraturan yang berfokus pada tanda tangan elektronik pada umumnya.

Pada level internasional, *the United Nations Commission on International Trade Law (UNCITRAL)* membuat suatu model hukum electronic

---

[116] Terjemahannya adalah 'Pertukaran Data Elektronik atau Electronic Data Interchange (EDI) berarti pengiriman informasi elektronik dari satu komputer ke komputer yang lainnya yang menggunakan standard yang disetujui untuk menyusun suatu informasi'

[117] Terjemahannya 'informasi yang dihasilkan, yang dikirim, yang diterima atau disimpan secara elektronik, dengan cara yang sama atau hampir sama yang mencakuup, namun tidak terbatas terhadap, pertukaran data elektronik, surat elektronik, telegram, telex atau telecopy'

commerce pada tahun 1996 yang dikenal dengan nama *Model Law on Electronic Commerce (the Model Law)* yang bertujuan untuk mengatasi masalah-masalah hukum dalam penggunaan tanda tangan digital dan tanda tangan elektronik. Di dalam Model Law dinyatakan bahwa bila hukum mensyaratkan tanda tangan seseorang maka tanda tangan tersebut akan menjadi sah berkenaan dengan *data message* jika :

a) suatu metode digunakan untuk mengidentifikasi seseorang dan menunjukan persetujuan seseorang atas suatu informasi yang terkandung didalam *data message;* dan
b) metode tersebut dapat dipercaya sebagai sesuatu yang tepat dan cocok dipandang dari semua keadaan untuk maksud mana *data message* dibuat dan dikomunikasikan, termasuk setiap persetujuan yang relevan.[118]

Berdasar uraian di atas, bahwa *UNCITRAL Model Law* tidak hanya berkenaan dengan tanda tangan digital tetapi mencakup semua bentuk-bentuk tanda tangan elektronik.

Menurut *Smith B.W and Tufaro P.S* bahwa Tanda tangan digital mempunyai arti metode-metode otentifikasi yang mempergunakan 'public key cryptography' dan istilah tanda tangan elektronik meliputi tanda tangan digital dan juga metode-metode non-public key authentication.[119]

Dibeberapa negara, pengertian tanda tangan digital adalah tiap simbol atau metode yang dilaksanakan atau dipergunakan secara elektronik dengan suatu maksud agar terikat, sementara pengertian tanda tangan elektronik adalah proses, simbol dan catatan (rekaman) elektronik yang melekat di atau secara logis berhubungan dengan suatu catatan (rekaman) dan dilakukan atau dipergunakan oleh seseorang dengan maksud untuk memberi tanda pada catatan (rekaman) tersebut.[120]

Di beberapa negara lain pengertian tanda tangan elektronik (electronic signature) adalah bahwa tanda tangan elektronik tersebut harus memproses atribut tertentu, atau memenuhi syarat-syarat tertentu sebelum dinyatakan sah dan dapat dilaksanakan. Misalnya di negara *European Union* yang tertera dalam *Directive on Digital Signature*,[121] *electronic sigature* dibedakan pula dengan *anvanced electronic signature*. Kalau *electronic signature* definisinya adalah data dalam bentuk elektronik yang dilekatkan kepada atau secara logis berhubungan dengan data elektronik lainnya yang menggunakan suatu metode otentifikasi. Sebaliknya 'advanced electronic signature' adalah suatu tanda tangan elektronik yang secara unik berhubungan dengan penandaan, dapat

118 Lihat UNCITRAL Model Law, 1996, pasal 7
119 Smith B W and Tufaro P S (1998)'To certify or not to certify: The OCC opens the door to digital signature certification' 24 Ohio Northern University Law Review 813
120 Lihat Uniform Electronic Transactions Act, s2(8)
121 It was adopted on 30th November 1999 at the Council of Telecommunications, European Union.

mengidentifikasi penandaan, yang diciptakan dengan menggunakan cara-cara yang dapat dilakukan oleh penandaan tersebut di bawah kontrolnya sendiri yang dihubungkan dengan data yang berkaitan dengannya, dengan cara demikian bahwa tiap perubahan data yang terjadi dapat dideteksi.[122] Defenisi *advanced electronic signatures* mengilustrasikan pendekatan-pendekatan alternatif terhadap tanda tangan elektronik.

Dibeberapa negara dan negara-negara bagian, mereka hanya memberikan pengakuan hukum terhadap tanda tangan digital, dan tidak mengakui bentuk-bentuk lain tanda tangan elektronik di dalam peraturan perundang-undangan *digital signature* mereka. Sebagai contoh, dalam undang-undang *Utah (Utah Act)* yang hanya memberikan pengakuan hukum terhadap digital signature yang mempunyai defenisi yaitu suatu pengiriman pesan yang menggunakan suatu sistem sandi asimetrik (*asymmetric cryptosystem*)[123]

Hukum atau peraturan sebagai pedoman perdagangan secara e-commerce ini telah dibuat oleh lembaga-lembaga internasional antara lain :[124]

- United Nations Commission on International Trade Law (UNCITRAL) yang mengatur tentang : Kelompok Kerja untuk Perdagangan Elektronik (e-commerce) yang selanjutnya disebut sebagai UNCITRAL, Model Law Perdagangan Elektronik UNCITRAL 1996, Model Law Tanda Tangan Elektronik *(electronic signiture)* UNCITRAL 2001
- European Union yang mengatur tentang Petunjuk 2000/31/EC tentang Petunjuk mengenai Perdagangan Elektronik, Petunjuk 1999/93/EC tentang Petunjuk mengenai Tanda Tangan Elektronik, Petunjuk 95/46EC tentang Petunjuk Perlindungan tanggal
- Organisation for Economic Co-operation and Development (OECD) yang mengatur tentang Rencana Aksi OECD untuk Perdagangan Elektronik 1998, Panduan Kerahasiaan 1980, Panduan Sistem Keamanan Informasi 1992, Panduan Sistem Kriptografi 1997 dan Panduan Perlindungan Konsumen 1999.
- International Chamber of Commerce (ICC) yang mengatur tentang Rencana Aksi untuk perdagangan Elektronik se-dunia, Peraturan Standar mengenai Tata Cara Lalu lintas Data Perdagangan melalui teletransmisi, Penggunaan Umum untuk Perdagangan Internasional yang dijamin secara digital 1997, Model Ketentuan Kerahasiaan untuk lalu lintas data lintas negara.
- Word Trade Organitation (WTO) yang mengatur tentang Program Kerja.
- Asia Pacific Economic Co-operation (APEC) yang mengatur tentang Satuan Tugas Perdagangan Elektronik, Makalah-makalah, Proyek-proyek dan Kelompok kerja Telekomunikasi dan Informasi.

---

122 EU Directive on Digital Signatures, article 2

123 Utah Code Ann (1995), s.46-3-103(10).

124 Makalah, *E-Commerce,* Indonesian Judicial Training Program, 6-10 January 2003, Singapore

Negara-negara asing juga telah mengeluarkan peraturan tentang e-commerce misalnya Australia,[125] Singapore,[126] Hongkong [127] dan juga Malaysia.[128]

Indonesia sampai sekarang ini belum mempunyai Undang-undang yang mengatur tentang e-commerce dan cybercrime meskipun dalam transaksi perdagangan di Indonesia sudah umum dan tidak asing lagi mempergunakan elektronik, dan malah sudah sering menimbulkan perkara di bidang perdata maupun pidana.

Namun secara sektoral sebenarnya hal ini sudah diatur antara lain :

- UU no. 19 tahun 2002 tentang hak cipta,
- UU no. 15 tahun 2001 tentang merk,
- UU no. 14 tahun 2001 tentang paten,
- UU no. 32 tahun 2000 tentang disain tata letak sirkuit terpadu,
- UU no. 31 tahun 2000 tentang disain industri,
- UU no. 30 tahun 2000 tentang rahasia dagang
- UU no. 36 tahun 1999 tentang telekomunikasi,
- Keputusan Menteri Perhubungan no. KM.21 tahun 2001 tentang penyelenggaraan jasa telekomunikasi,
- Keputusan Menteri Perhubungan no. KM 23 tahun 2002 tentang penyelenggaraan jasa internet telepon,
- Bank-bank swasta misalnya BII dan BCA telah menggunakan Internet Banking
- UU no 23 Tahun 1999, disebutkan defenisi kliring yaitu "pertukaran warkat atau data keuangan elektronik antar bank baik atas nama bank maupun nasabah yang hasil perhitungannya diselesaikan pada waktu tertentu..."[129]
- Peraturan Bank Indonesia (PBI) No 1/3/PBI/1999 tanggal 13 Agustus 1999 tentang Penyelenggaraan Kliring Lokal dan Penyelesaian Akhir Transaksi Pembayaran Antar Bank Atas Hasil Kliring Lokal telah diatur lebih lanjut tentang pengakuan atas data elektronik sebagai dasar pembukuan
- Peraturan Bank Indonesia (PBI) No 2/24/PBI/2000 tentang Hubungan Rekening Giro Antar Bank Indonesia Dengan Pihak Ekstern yang dalam Penarikan Rekening Giro Rupiah dengan menggunakan sarana elektronik
- Bursa Efek Jakarta (BEJ) menyelenggarakan sistem komputer dalam jual beli saham yang disebut dengan *Jakarta Automatic Trading System* (JATS)
- Direktorat Jenderal Bea Cukai Indonesia telah memakai sistem Elektronic Data Interchange (EDI). Persatuan Bea Cukai Dunia atau World Custom Organization mewajibkan bagi anggotanya untuk menggunakan Sistem EDI
- .Surat Keputusan Direktur Jenderal Pajak no 122.D/PJ/2000, mengizinkan teknik-teknik baru untuk menggunakan materai dengan sistem komputer.

---

[125] Australia disebut dengan Commonwealth Electronic Transaction Act 1999
[126] Singapore disebut dengan the Electronic Transactions Bill tahun 1998
[127] Hongkong disebut dengan Electronic Transactions Ordinance tahun 2000
[128] Malaysia disebut dengan UU Tanda Tangan Digital tahun 1997
[129] Lihat pasal 16 UU no 23 tahun 1999

Sekarang ini telah dirampungkan beberapa rancangan peraturan misalnya Rancangan UU tentang pidana kejahatan teknologi informasi, Rancangan UU tentang tanda tangan elektronik dan transaksi elektronik, Rancangan Keputusan Dirjen tentang persyaratan teknis perangkat ADSL (Asymetric, Digital, Subscriber Line)

E-Commerce dalam UNCITRAL.

UNCITRAL telah menetapkan suatu *model* law untuk *electronic Commerce* pada tahun 1996 yang kemudian direvisi pada tahun 1998. Model hukum tersebut berisi panduan-panduan yang disarankan diikuti oleh negara-negara anggota saat mereka membuat legislasi untuk e-commerce (atau transaksi elektronik secara umum).

Adapun yang termaktub dalam model law tersebut antara lain adalah masalah :

- keberadaan dan pengakuan hukum transaksi elektronik,
- pengakuan konsep incorperation by reference
- jaminan keamanan atas keaslian transaksi elektronik dengan tanda tangan elektronik ataupun dengan cara lainnya yang dapat dipercaya dan diandalkan.
- Penggunaan salinan transaksi elektronik
- Pengarsipan transaksi elektronik
- Otomasi transaksi elektronik
- Hak dan kewajiban pengiriman transaksi elektronik dan penerima transaksi elektronik.
- Tanda penerimaan tanda bukti (*acknowledgement of receipt*) sebagai tanda untuk mengeksekusi transaksi
- Kapan dikirim, diterima, terjadi dan berlakunya transaksi elektronik.

Karena *model law* untuk *e-commerce* UNCITRAL telah memuat prinsip-prinsip umum yang cukup universal untuk berbagai jenis transaksi elektronik, maka pembahasan kami didasarkan pada transaksi elektronik akan mengacu kepada *model law* tersebut. Namun model transaksi elektronik lainnya yang tidak menggunakan EDI seperti penggunaan *web-wrap contract* dan *e-mail* di internet juga akan disinggung.

Perjanjian elektronik

Perjanjian di era digital akan menggunakan data digital sebagai pengganti kertas sebagai media dari perjanjian tersebut. Penggunaan data digital sebagai media dalam melakukan perjanjian akan memberikan efisiensi yang

sangat besar terutama bagi perusahaan-perusahaan yang setiap bulannya banyak membuat perjanjian, seperti *trading house*, pabrik dan juga bagi perusahaan-perusahaan yang menjalankan bisnisnya di internet. Namun, perjanjian elektronik terutama yang di internet memiliki berbagai permasalahan. Permasalahan itu antara lain adalah apakah suatu kontrak yang dilakukan secara *on-line* adalah *enforceable*, kapankah terjadinya kesepakatan, dan masalah penggunaan tanda tangan dalam perjanjian yang dilakukan secara *on-line*.

Pengakuan Hukum Atas Transaksi Elektronik

Salah satu aspek yang amat penting dalam transaksi elektronik adalah pentingnya pengakuan hukum atas suatu transaksi elektronik. Artinya, hukum tidak bisa menampikkan begitu saja bukti berupa transaksi elektronik dipersidangan. Hal ini dijelaskan dalam *model law* untuk *e-commerce* UNCITRAL di pasal 5. Masalah apakah transaksi elekronik itu terjamin keasliannya atau tidak, itu adalah masalah pembuktian dipengadilan. Transaksi elektronik dalam pasal 6 juga diakui sederajat dengan 'tulisan'. Sekali lagi, masalah apakah transaksi elektronik itu terjamin keasliannyaatau bukan, itu adalah masalah lain. Argumentasinya adalah tulisan biasapun bisa asli, tetapi juga bisa palsu. Demikian pula halnya dengan transaksi elektRonik dimana transaksi elektronik pun bisa terbuktikan keasliannya, atau sebaliknya terbukti palsu.

Konsep Incorporation by Reference

Dalam mengirimkan data-data elektronik, seringkali dilakukan penyederhanaan format data yang dikirimkan. Misalnya antara pabrik dengan supplier sering ada pertukaran data invoice, purchase order, payment instruction dan sebagainya. Kalau setiap pengiriman *message* tersebut harus mengetikan "Payment Instruction", tentu akan memakan *bandwidth* (dengan kata lain, boros), sehingga dibuatlah kode untuk

Tanda Tangan

Pasal 7 dari model law UNCITRAL menjelaskan mengenai pengakuan terhadap tanda tangan pada transaksi elektronik. Hanya saja 'tandatangan' itu harus terjamin keasliannya, sehingga penandatanganan dapat diotentikasi oleh pihak lain.

Keaslian Transaksi Elektronik

Jika ada jaminan bahwa informasi dalam dokumen elektronik itu diciptakan sampai saat ini dilihat kembali di masa depan, informasi itu tidak

berubah, maka artinya kita dapat yakin bahwa dokumen elektronik tersebut terjaga keasliannya (atau keutuhannya, karena tidak berubah-ubah/terkutak katik). Hal ini dapat diimplikasi, jika ada suatu peraturan yang mengharuskan penyerahan suatu dokumen dan dokumen itu harus yang asli, maka transaksi elektronik dapat dianggap sama dengan dokumen asli. Model law dari UNCITRAL memuat masalah ini dalam pasal 8.

Pengarsipan dan Pencatatan Elektronik

Patut diperhatikan bahwa pasal 8 ayat 1b mengindiksikan pengakuan terhadap pengarsipan dan pencatatan secara elektronik (*electronic record*). Meskipun demikian, pasal 10 lebih menegaskan lagi pengakuan terhadap catatan elektronik. Arsip dan catatan elektronik dapat memenuhi persyaratan sebagai objek pengarsipan jika :

- Informasi dalam catatan elektronik dapat diakses. Hal ini jelas, karena tidak ada gunanya suatu catatan kalau tidak bisa diakses/ dibuka untuk dibaca di kemudian hari
- Informasi dalam catatan elektronik itu dapat dijadikan referensi, artinya catatan elektronik tersebut harus bisa dirujuk kembali dengan jelas jika ada pihak lain yang ingin melihatnya kembali.

Sebenarnya ada suatu persyaratan (pasal 8 ayat 1b) berkenan dengan catatan elektronik, tetapi kami berpendapat bahwa persyaratan tersebut sangat terpaut dengan EDI jadi tidak bisa digeneralisasikan. Sebuah rekomendasi lain (pasal 8 ayat 1c), menyarankan agar sebaiknya transaksi elektronik yang direkam tersebut juga mendeskripsikan informasi pengirim, penerima, beserta waktu pengiriman dan waktu penerimaan diterima.

Komunikasi Transaksi Elektronik dan Terjadinya Kesepakatan

Secara umum, agar pengiriman pesan elektronik dari pengirim (*originator*) kepada penerima (*addessee*) dapat terjamin sampai kepada penerima, maka sang penerima sebaiknya mengirimkan pesan balasan (*acknowledgement*) yang memberitahukan kepada pengirim bahwa sang penerima sudah menerima pesan tersebut. Jadi kalau tidak dibalas, maka pengirim akan menganggap bahwa pesan tersebut belum sampai dan akan mengirimkan pesan pemberitahuan kepada penerima bahwa belum ada pesan balasan (*acknowledgement*) yang sampai kepada pengirim kembali. Pemberitahuan ini akan dilakukan terus menerus sampai ada balasan dari penerima, atau sampai *time-out* (berhenti karena terlalu lama menunggu balasan).

Suatu perjanjian lahir pada detik tercapainya kesepakatan, maka perjanjian itu lahir pada detik diterimanya suatu penawaran (*offerte*). Artinya dengan diterimanya suatu penawaran maka dapat disimpulkan bahwa kedua

belah pihak telah mengetahui tentang adanya penawaran tersebut. Dan pihak penerima penawaran melakukan penerimaan terhadap penawar tersebut sehingga lahirlah suatu perjanjian. Dengan tidak bertemunya antara orang yang memberikan penawaran dan orang yang menerima penawaran dalam suatu transaksi elektronik, maka penawaran baru dianggap disepakati jika diterimanya jawaban atas penawaran (*acknowledgement*) oleh pemberi penawaran. Sehingga tampak jelas bagi kita bahwa kedua belah pihak tersebut dianggap telah sama-sama mengetahui adanya kesepakatan atas penawaran yang dijadikan patokan saat lahirnya suatu perjanjian.

Pendelegasian wewenang kepada komputer atau orang lain.

Sangat sulit dibayangkan apabila seorang pejabat menandatangani ribuan dokumen export/import setiap bulannya. Namun kenyataannya, hal itu bisa terjadi. Untungnya dengan menggunakan komputer, proses pemeriksaan dokumen-dokumen acap kali bisa dipercepat. Dokumen export/import yang disetujui dapat segera dikirim kepada adressee. Karena sesungguhnya bukan pejabat itu yang melakukan persetujuan (karena diotomatisasi oleh komputer), maka secara hukum perlu ada aturan yang memperbolehkan pendelegasian wewenang kepada komputer. Tentunya komputer tersebut harus diprogram terlebih dahulu sesuai dengan 'kehendak' pemberi wewenang (dalam hal ini sang pejabat). Sang pejabat harus memiliki kontrol terhadap komputer yang melakukan pemeriksaan dan penyetujuan dokumen-dokumen export import yang seharusnya ditandatangani oleh pejabat tersebut. Pendelegasian wewenang juga dapat diperluas kepada orang lain (bukan komputer).

Jaminan Keamanan

Model law UNCITRAL untuk e-commerce banyak menuntut adanya suatu jaminan atas kehandalan sistem, jaminan atas keaslian transaksi elektronik, atau metode pembuktian yang handal. Semua itu sebenarnya terkait dengan masalah keamanan (security) dari transaksi elektronik. Untuk keamanan transaksi elektronik pada dasarnya menggunakan prinsip kriptografi.

Konsep Dasar Kriptografi

Kriptografi, sebagai batu bata utama untuk keamanan e-commerce adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman. Isu-isu dalam kriptografi meliputi :

1. Kerahasiaan (confidential) dari pesan dijamin dengan melakukan enkripsi (penyandian), sehingga pesan yang telah disandikan itu tidak dapat dibaca oleh orang-orang yang tidak berhak.

2. Keutuhan (integrity) dari pesan, sehingga saat pesan itu dikirimkan tidak ada yang bisa mengutak atik ditengah jalan. Sebagai contoh, dalam suatu transaksi pembayaran, sang pengirim pesan berkepentingan agar nilai cek digital tidak diubah orang lain menjadi ditengah jalan.
3. Jaminan atas identitas dan keabsahan (authenticity) jati diri dari pihak-pihak yang melakukan transaksi.
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (non-repudiation) jika terjadi sengketa atau perselisihan pada transaksi elektronik yang telah terjadi.

Dalam kriptografi, ada dua proses utama :
1. Enkripsi (encryption) : yakni proses untuk mengubah pesan asli (plaintext) menjadi pesan yang tersandikan atau pesan yang terahasiakan (ciphertext)
2. Dekripsi (decryption) : yakni proses mengubah pesan yang tersandikan (ciphertext) kembali menjadi pesan pada bentuk aslinya (plaintext).

Kriptografi Kunci Simetrik

Ini adalah jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pengirim pesan dan penerima pesan harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia ciphertext .

Kriptografi kunci publik / kunci asimetrik

Teknik kriptografi kunci publik mencoba menjawab permasalahan pendistribusian kunci pada teknologi kriptografi kunci simetrik. Dalam kriptografi kunci publik, setiap pihak memiliki sepasang kunci :
1. Sebuah kunci publik yang didistribusikan kepada umum/ khalayak ramai.
2. Sebuah kunci privat yang harus disimpan dengan rahasia dan tidak boleh diketahui orang lain.

Fungsi Hash Satu Arah

Fungsi *hash* berguna untuk menjaga keutuhan (integrity) dari pesan yang dikirimkan Bagaimana jika Anto mengirimkan surat pembayaran kepada Badu sebesar 1 juta rupiah, namun ditengah jalan Maman (yang ternyata berhasil membobol sandi entah dengan cara apa) membubuhkan angka 0 lagi dibelakangnya sehingga menjadi 10 juta rupiah ? Dimata Tari, pesan tersebut harus utuh, tidak diubah-ubah oleh siapapun, bahkan bukan hanya oleh Maman, namun juga termasuk oleh Anto, Badu dan gangguan pada transmisi pesan

(*noise*). Hal ini dapat dilakukan dengan fungsi hash satu arah (*one way hash function*), yang terkadang disebut sidik jari (*fingerprint*), *hash, message integrity check*, atau *manipulation detection code*

Fungsi *hash* untuk membuat sidik jari tersebut dapat diketahui oleh siapapun, tak terkecuali, sehingga siapapun dapat memeriksa keutuhan dokumen atau pesan tertentu. Tak ada algoritma rahasia dan umumnya takada pula kunci rahasia.Jaminan dari keamanan sidik jari berangkat dari kenyataan bahwa hampir tidak ada dua pre-image yang memiliki *hash value* yang sama. Inilah yang disebut dengan sifat *collision free* dari suatu fungsi *hash* yang baik. Selain itu, sangat sulit untuk membuat suatu pre-image jika hanya diketahui *hash* valuenya saja. Contoh algoritma fungsi *hash* satu arah adalah MD-4, MD-5 dan SHA. *Message authentication code* (MAC) adalah satu variasi dari fungsi hash satu arah, hanya saja selain *pre-image*, sebuah kunci rahasia juga menjadi input bagi fungsi MAC.

Tanda Tangan digital

Sifat yang diinginkan dari tanda tangan digital diantaranya adalah :

1. Tanda tangan asli (otentik), tidak mudah ditulis/ ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti sehingga penandatangan tidak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya,
2. Tanda tangan itu hanya sah untuk dokumen (pesan) itu saja. Tanda tangan itu tidak bisa dipindahkan dari suatu dokumen ke dokumen lainnya. Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak sah lagi.
3. Tanda tangan itu dapat diperiksa dengan mudah.
4. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
5. Tanda tangan itu juga sah untuk kopi dari dokumen yang sama persis.

Meskipun ada banyak skenario, ada baiknya kita perhatikan salah satu skenario yang cukup umum dalam penggunaan tanda tangan digital. Tanda tangan digital memanfaatkan fungsi hash satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Bukan dokumen tersebut secara keseluruhan yang ditandatangani, namun biasanya yang ditandatangani adalah sidik jari dari dokumen itu beserta ***time stamp***-nya dengan menggunakan kunci privat. *Time stamp* berguna untuk berguna untuk menentukan waktu pengesahan dokumen.

Sertifikat digital

Kriptografi kunci publik bukan tanpa masalah. Masalah utama adalah bagaimana orang-orang bisa yakin bahwa kunci publik yang di 'duga' milik Badu adalah benar-benar milik Badu? Bukankah bisa saja Chandra membohongi Anto bahwa kunci publiknya adalah kunci publik milik Badu ? Untuk mengamankan kunci publik, setiap kunci publik beserta keterangannya "disegel" dengan tanda tangan digital agar kunci publik dan keterangannya tidak bisa "dikutak-katik" oleh hacker. Ingat bahwa dengan menandatangani kunci publik dan keterangannya,berarti tidak ada yang bisa" memanipulasinya" lagi. Kalaupun ada yang mengubah-ubah, pasti akan ketahuan, karena tanda tangannya tidak akan valid lagi (lihat sifat tanda tangan digital). Kunci publik beserta keterangan yang menyertainya yang sudah ditanda tangani disebut dengan istilah sertifikat digital. Lembaga yang menandatangani sertifikat digital disebut dengan istilah *Certification Authority* (CA). Kita boleh membayangkan sertifikat digital berupa "tanda pengenal digital" Keterangan yang ada dalam standar sertifikat digital X.509 versi 3 dan di RFC 2459 meliputi:

1. Versi sertifikat
2. Nomor seri sertifikat
3. Algoritma yang dipergunakan
4. Nama pemilik sertifikat digital, atau istilah lainnya adalah subject atau subscriber. Dilengkapi pula dengan keterangan mengenai pemilik, seperti negara asal, organisasi, unit dalam organisasi itu, provinsi, dsb. Pada identitas "digital" dari pemilik sertifikat digital juga dicantumkan e-mail atau *domain name* websitenya (oleh karena itu untuk membuat sertifikat digital, sebuah perusahaan juga harus melampirkan surat keterangan yang menyatakan bahwa dirinya berhak menggunakan *domain name* tersebut)
5. Issuer, yakni lembaga yang menerbitkan sertifikat digital.
6. Validitas, yakni masa berlakunya sertifikat digital tersebut
7. *Extension* lainnya (sesuai kebutuhan penggunaan yang spesifik pada bidang tertentu).

Panjang kunci dan keamanannya

Pembobolan kunci mungkin saja terjadi. Besar kecilnya kemungkinan ini ditentukan oleh panjangnya kunci. Semakin panjang kunci semakin sulit

Certification Authority

Certification Authority (CA) adalah sebuah lembaga yang bertugas mensertifikasi jati diri *subscriber / subject* agar *subscriber* itu bisa dikenali di

dunia digital, dengan menerbitkan sertifikat digital untuk tiap *subscribernya.* Jika dianalogikan dengan penerbitan KTP di kelurahan, mungkin CA dapat disamakan posisinya dengan lurah yang menandatangani setiap KTP di kelurahannya. Hanya saja CA menandatangani 'KTP digital'. Tentunya CA harus merupakan entitas yang independen dan terpercaya (*trusted third party*). Untuk memberikan gambaran bagaimana CA bekerja kita ambil contoh bagaimana cara sebuah perusahaan meminta SSL. Perusahan itu perlu menunjukan kepada CA dua lembar surat, yakni surat ijin usaha dan surat izin penggunaan suatu *domain name* tertentu. Barulah setelah memeriksa keabsahan kedua dokumen tersebut, CA menerbitkan sertifikat digital SSL untuk perusahan yang bersangkutan. Sebenarnya tidak harus pihak ketiga diluar organisasi sang *subscriber,* terutama untuk PKI yang tidak berhubungan dengan kepentingan publik. Misalnya, CA – internal disebuah perusahaan bisa saja mengeluarkan *digital ID* buat pegawainya, untuk keluar masuk ruangan (*accses control card)*

Registration Authority

Registration Authority (RA) bertanggung jawab untuk melakukan proses identifikasi dan otentikasi terhadap subscriber digital, tetapi tidak menandatangani sertifikat itu. Dalam kehidupan sehari-hari, banyak sekali dokumen yang diperiksa namun ditandatangani oleh orang yang berbeda. Kembali ke contoh dikelurahan, saat kita mendaftarkan diri untuk membuat KTP baru, maka akta kelahiran, surat keluarga, dan surat keterangan RT akan diperiksa oleh pegawai tata usaha kelurahan. Nah, pegawai tata usaha kelurahan inilah yang dapat dianalogikan sebagai RA, karena yang menandatangani KTP tetap lurahnya (diibaratkan CA).

Adanya sebuah RA dalam PKI memang sifatnya *optional* (tidak harus ada) karena memang RA hanya menjalankan beberapa tugas yang didelegasikan oleh CA jika CA tidak sanggup melakukannya. Artinya, bisa saja dalam suatu skenario tertentu, seluruh tugas RA berada dalam CA. Menurut *Adams dan Lloyd*, tugas-tugas RA dapat mencakup :

- Otentikasi calon subscriber secara fisik
- ≠ Registrasi calon subscriber
- Membuat pasangan key untuk subsriber (jika subscriber tidak sanggup membuat sendiri pasangan kuncinya.
- ≠ Membuat backup dari kunci privat yang dipergunakan untuk enkripsi (key recovery)
- Pelaporan kalau ada sertifikat yang dicabut (revocation reporting)

Certificate Repository

Jika sebuah CA sudah menandatangani sebuah sertifikat digital, bukan berarti lantas seluruh permasalahan beres. Seorang subscriber, katakanlah Anto, bisa saja memegang sertifikat digital, dan Anto dapat menyerahkan sertifikat digitalnya kepada orang lain yang ingin berkomunikasi dengan aman dengan Anto. Teknik penyerahan sertifikat digital oleh pribadi ini disebut dengan istilah *private dessemination.* Tapi, teknik ini memiliki beberapa kekurangan :

1. Teknik ini hanya bisa untuk PKI dengan user dalam jumlah kecil. Artinya *scalability*-nya rendah, karena penyebaran informasinya tidak meluas.
2. Umumnya tidak sesuai dengan struktur perusahaan pada umumnya, yang cenderung sifatnya *centralized hierarchia*, ketimbang *user – centris*

Namun dalam suatu skenario lain, Badu yang belum pernah berkomunikasi dengan Anto, hendak mengirimkan pesan rahasia kepada Anto. Nah, untuk itu, Badu perlu mendapatkan sertifikat digital Anto. Tetapi dari mana Badu mendapatkan sertifikat digital Anto? Oleh karena itu, sebuah tempat penyimpanan (*repository*) on-line untuk sertifikat digital dibutuhkan dalam PKI. *Repository* ini juga berguna untuk menyimpan daftar sertifikat yang dibatalkan/CRL (yang tidak berlaku sebelum masa berlakunya habis). Jadi yang disimpan dalam repository bukan hanya sertifikat digital saja, namun informasi-informasi penting yang berkaitan dengan operasi sebuah PKI. *Repository* untuk sertifikat digital boleh diibaratkan seperti daftar alamat atau buku telepon. Beberapa contoh yang masuk kategori *repository* mencakup : LDAP, X500, OCSP responder, database, dsb

Relying Party

Relying party adalah pihak yang mempercayai keberadaan dan keabsahan suatu sertifikat digital. Dalam kasus pengiriman data rahasia (dengan amplop digital) dari Anto ke Badu, Anto mempercayai keberadaan sertifikat digital Badu. Dalam kasus ini, relying party-nya adalah Anto. Sedangkan dalam kasus penandatanganan surat oleh Anto, Badu memeriksa keabsahan tanda tangan Anto, adalah *relying-party*-nya.

Shrink Wrap (breaking the seal) dan WebWrap (clicking the button) dan Standard Form Agreement

Shrink wrap contract dan Webwrap contract mempunyai prinsip yang sama yaitu sama-sama perjanjian berupa standard form contract. Shrink Wrap Agreement biasanya digunakan dalam pembelian suatu *software* (program komputer) yang dibungkus dalam suatu kotak yang disegel (seal) sedemikian rupa dan ada tertera tulisan pada kemasannya apabila kemasan (seal) dirobek

(breaking the seal)ap menyetujui perjanjian lisensi software. Dari hal di atas sebenarnya seorang pembeli tidak ada menandatangani suatu kontrak lisensi dengan *licensor*. Namun begitu pembeli merobek kemasan sofware saat itu pula, pembeli terikat perjanjian lisensi atas penggunaan program komputer tersebut.

Konsep dari *shrink wrap* contract ini adalah juga diadopsi didalam suatu perjanjian yang dilakukan secara on-line. Misalnya seorang penjual barang atau jasa hendak menawarkan barang atau jasanya kepada para pelanggan. Penjual tersebut kemudian menampilkan ketentuan –ketentuan mengenai barang / jasa tersebut di dalam homepagenya. Dan apabila ketentuan tersebut disetujui oleh calon pembeli, maka tinggal menekan tombol 'setuju' saja (clicking button) Penggunaan perjanjian dengan model webwrap ini merupakan suatu hal yang umum di internet namun masalah hukum sehubungan dengan sahnya perjanjian di Web wrap telah menjadi pembicaraan di kalangan ahli hukum, dan juga telah ada beberapa kasus yang masuk ke pengadilan.

Transaksi E-Commerce

Tentang E Commerce ini, telah ada aturan yang dapat digunakan sebagai model yang berlaku secara internasional yaitu UNCITRAL *(United Nations on International Trade Law)* yang telah menetapkan peraturan peraturan yang dapat mengesahkan kontrak-kontrak yang terjadi pada alat elektronik, karakteristik tulisan-tulisan elektronis dan dokumen dokumen asli yang valid, memberikan tandatangan elektronis yang dapat diterima untuk melakukan perdagangan serta mendukung pengakuan bukti-bukti dari komputer dalam proses di persidangan dan proses pengambilan keputusan.

Transaksi E Commerce sendiri tidak hanya terbatas pada perdagangan saja tapi juga untuk perjanjian agensi, pemberian dana, investasi, asuransi dan sebagainya. Dalam UNCITRAL pasal 2 dikatakan bahwa data message adalah informasi yang dibuat, dikirim, diterima, atau disimpan dengan peralatan peralatan elektronik, optic atau semacamnya, termasuk, tapi tidak terbatas pada pertukaran data elektronik (EDI / Elektronik Data Interchange), e-mail, telegram teleks dan telekopi.

Dari ketentuan tersebut diatas nampak bahwa e-commerce bukanlah perdagangan yang menggunakan internet saja, tetapi juga media elektronik lainnya, walaupun yang paling popular adalah internet.

Dibawah ini akan dibahas aspek perdata dari E-Commerce sesuai dengan hukum positif yang berlaku di Indonesia, agar dapat diketahui kekosongan kekosongan hukum yang perlu diatur lebih lanjut, baik dengan menggunakan model UNCITRAL ataukah dengan penafsiran / interprestasi.

E-Commerce dan Hukum Kontrak.

Sebagai suatu bentuk perdagangan , E-Commerce tidak bisa dipisahkan dengan hukum kontrak atau hukum perikatan (verbintenis), sebab dalam e-commerce tersebut ada pihak-pihak yang mengikatkan diri untuk memberikan prestasi dan pihak lain yang berhak menerima prestasi.

Hukum kontrak merupakan salah satu istilah yang banyak digunakan oleh kalangan praktisi hukum di Indonesia, selain istilah perikatan , perjanjian atau persetujuan, yang pada prinsipnya mengatur hak dan kewajiban dari kreditur (si berpiutang) dan debitur (si berutang). Ada pula yang membedakan perjanjian (dari istilah Belanda *Overeenkomst*) sebagai suatu peristiwa dimana seseorang berjanji kepada orang lain atau dua orang yang saling berjanji untuk melaksanakan sesuatu hal.

Dalam *Black Law Dictionary*, kontrak didefinisikan sebagai sebuah kesepakatan antara dua orang atau lebih yang menciptakan sebuah kewajiban untuk melakukan sesuatu hal yang tertentu. Unsur unsur intinya adalah pihak pihak yang kompeten (cakap), subyek kesepakatan, sebuah konsideransi hukum, mutualis kesepakatan dan mutualis kewajiban[130]

Uniform Comercial Code mendefinisikan kontrak sebagai suatu perjanjian atau kontrak yang merujuk kepada kewajiban hukum secara penuh yang terlahir dari kesepakatan para pihak yang dilakukan sesuai dengan undang undang.

Dalam hukum positif kita, yaitu pasal 1313 KUH Perdata dikatakan bahwa yang dimaksud dengan suatu perjanjian adalah suatu perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang atau lebih. Lebih lanjut dalam pasal 1320 KUH Perdata disebutkan bahwa untuk sahnya suatu perjanjian harus dipenuhi syarat-syarat sebagai berikut :

- Adanya kesepakatan para pihak ;
- Adanya kecakapan bertindak dari para pihak ;
- Sifat dan luas obyek perjanjian dapat ditentukan ;
- Klausula yang halal ;

Dari definisi-definisi tersebut diatas, nampak bahwa kesepakatan para pihak merupakan unsur yang sangat esensial bagi terjadinya suatu kontrak.

Tentang kesepakatan para pihak ;

Secara konvensional kesepakatan para pihak dibuktikan adanya tandatangan dari para pihak dimana para pihak yang membuat perjanjian atau kontrak tersebut membubuhkan tandatangannya diatas surat perjanjian yang

[130] *M.Arsyad Sanusi,E Commerce, Hukum dan Solusinya,Juni 2001,PT.Mizan Grafika Sarana,halaman 36*

mereka buat untuk membuktikan telah terjadinya suatu persetujuan, dan juga hal-hal apa saja yang mereka setujui ;

Bahwa dalam pembuatan perjanjian inipun bisa dibuat dibawah tangan ataupun dihadapan pejabat yang berwenang, dalam hal ini adalah Notaris, dimana cara pembuatan perjanjian inipun akan menentukan kekuatan pembuktian dari perjanjian tersebut ; Dalam hal perjanjian tersebut dibuat oleh para pihak sendiri dan tidak dihadapan Notaris, maka perjanjian tersebut termasuk dalam kategori akta dibawah tangan sehingga dapat dilumpuhkan oleh alat bukti lain yang lebih kuat, sedangkan perjanjian yang dibuat dihadapan Notaris termasuk dalam kategori akta authentik dan mempunyai kekuatan pembuktian yang sempurna.

Bagaimana dengan perjanjian ataupun kontrak on line ?

Kontrak atau perjanjian melaui internet (on line) tentu saja tidak membutuhkan tandatangan para pihak, sebab dalam kontrak melalui internet (on line) salah satu pihak memberikan penawaran melalui internet, dan apabila calon konsumen yang melihat penawaran tersebut menyetujui, maka ia hanya tinggal memencet tombol yang menyatakan persetujuannya (click and point agrrement) dan terjadilan kesepakatan .Masalah timbul apabila salah satu pihak wanprestasi atau ingkar janji bagaimana membuktikan adanya persetujuan tersebut? Apakah mungkin dibuktikan dengan print out yang menunjukkan bahwa konsumen telah memencet tombol persetujuan ? Apabila dapat dibuktikan dengan hasil print out, termasuk dalam kategori alat bukti yang mana ?

Tentang kecakapan bertindak bagi para pihak

Bahwa kecakapan bertindak sesuai dengan ketentuan dalam Kitab Undang-Undang Hukum Perdata (BW) adalah orang dewasa, tidak berada dibawah pengampuan. Ukuran dewasa sesuai dengan BW adalah berusia berusia 21 tahun atau sudah pernah kawin dan dalam ketentuan lainnya yaitu Undang-Undang Kesejahteraan Anak ,usia dewasa adalah 21 tahun, demikian pula dalam yurisprudensi adalah 21 tahun;

Dalam transaksi e-commerce kita tidak dapat mengetahui dengan jelas apakah pihak-pihak yang terlibat dalam perjanjian tersebut mempunyai kecakapan untuk melakukan perbuatan hukum sebab pihak-pihak tersebut tidak pernah bertemu untuk membicarakan isi transaksi yang akan dilakukan. Dalam hal ini pembuat kontrak, baik pihak yang menawarkan ataupun konsumen bisa saja masih di bawah umur, sebab kemampuan seseorang untuk dapat menggunakan internet sudah sangat luas sehingga anak anakpun tidak mengalami kesulitan untuk menggunakannya;

Bila kita kaitkan dengan ketentuan mengenai persyaratan sahnya perjanjian menurut BW akan berakibat perjanjian tersebut tidak sah.

Apabila orang yang menawarkan tersebut tinggal di negara lain sedangkan konsumen ada di Indonesia, apakah ketentuan mengenai batas usia tersebut dapat diterapkan mengingat penawaran yang dilakukan bisa diakses dari seluruh penjuru dunia ?

Tentang obyek perjanjian

Dalam pasal 1334 BW dinyatakan bahwa obyek perjanjian haruslah konkrit yaitu berupa benda yang ada atau benda yang yang akan ada dan obyek perjanjian tersebut tidak boleh bertentangan hukum, kesusilaan, dan kepatutan. Bila kita membuka situs situs (world website) yang ada dalam internet, banyak sekali penawaran / iklan yang tidak sesuai dengan kesusilaan dan kepatutan yang kita anut, contohnya penawaran membeli video porno dengan kartu kredit. Kita tidak mengetahui dimana keberadaan pihak pihak yang menawarkan tersebut dan hukum apa yang berlaku bagi mereka . Apabila perjanjian seperti itu dilakukan , apakah lalu secara otomatis batal demi hukum ? Padahal hukum yang berlaku di Negara penjual mungkin tidak mengatur atau bahkan memperbolehkan transaksi semacam itu. Bila kemudian terjadi wanprestasi, hukum siapa yang digunakan ?

Dalam BW (Kitab Undang Undang Hukum Perdata) disebutkan bahwa perjanjian atau kontrak lahir karena persetujuan atau undang undang .Dalam hal kontrak lahir karena persetujuan dibutuhkan *konsensus* dari para pihak , baik yang menawarkan maupun konsumen yang menerima penawaran tersebut .

Penawaran melalui internet yang bersifat digital tidak banyak memberikan penjelasan atas hal-hal yang ditawarkan sehingga konsumen sering kurang memperoleh informasi mengenai barang yang ditawarkan, dan bila kemudian terjadi ketidakcocokkan atas prestasi yang diberikan penjual, dapatkah konsumen meminta pertanggungjawaban kepada penjual dengan alasan tidak tersedianya cukup informasi mengenai hal hal yang ditawarkan , sehingga persetujuan yang diberikan konsumen tidak sah / batal.

Pada asasnya persetujuan dianggap telah ada apabila konsumen menerima atau menyatakan persetujuannya atas penawaran seseorang, hal mana mengikat orang yang menyatakan persetujuannya untuk menaati isi perjanjian atau kontrak yang dilakukan.

Oleh karena adanya konsekuensi sebagaimana tersebut dalam pasal 1338 BW, maka orang yang menawarkan dituntut untuk memberikan informasi yang sejelas jelasnya atas barang yang ditawarkannya kepada konsumen, dan persetujuan yang diberikan harus bersifat konkrit, dimana hal itu dibuktikan dengan adanya tandatangan dari pihak yang menerima penawaran.

Kewajiban untuk memberikan informasi yang sejelas-jelasnya tersebut tidak dapat diterapkan terhadap penawaran-penawaran yang dilakukan melalui internet yang mungkin dilakukan oleh orang dari Negara lain karena penawaran melalui internet tidak mengenal tapal batas negara (Without Boundary),

demikian juga bukti tanda tangan dari orang yang menerima penawaran tidak dapat dilakukan melalui internet ;

Dengan demikian dapatkah ketentuan pasal 1338 BW diterapkan ?

Sehubungan dengan semakin banyaknya penawaran-penawaran yang dilakukan melalui internet, karena selain murah, cepat juga dapat menjangkau seluruh dunia akan timbul banyaknya kontrak-kontrak melalui internet (kontrak on line) yang berpotensi menimbulkan konflik baik karena wanprestasi yang dilakukan pihak yang menawarkan ataupun yang menerima penawaran. Terhadap hal ini apakah akan diatur lebih lanjut dalam aturan tersendiri ataukah cukup dengan aturan dalam BW tersebut dengan lebih memperluas penafsiran sehingga dapat ditentukan apakah dalam kontrak on line tersebut ada persetujuan / konsensus para pihak, kapan konsensus dianggap ada dan sebagainya; Hal ini tidak lain karena persetujuan persetujuan ataupun penawaran yang semula hanya ada diatas kertas sekarang sudah berubah menjadi digital dan seseorang tidak perlu lagi harus membubuhkan tandatangannya untuk dapat menyatakan persetujuannya .

E- Commerce dan Yurisdiksi Pengadilan

Pada prinsipnya baik instrumen hukum nasional maupun internasional (*Brussels Convention dan the Hague Convention*) menyatakan bahwa gugatan harus diajukan di pengadilan dimana tergugat berdomisili.

The Brussels Convention dan the Hague Convention membuat pengecualian terhadap prinsip ini yaitu khusus untuk konsumer, dimana konsumer dapat mengajukan gugatan di pengadilan dimana ia berdomisili.

Hukum yang disebut dengan the Brussels I regulation menyatakan bila ada perselisihan diantara konsumer di dalam satu negara UE (uni eropa) dan suatu retailer yang online di suatu negara lain (uni eropa), konsumer tersebut dapat mengajukan gugatan ke pengadilan di negaranya sendiri.[131] Menteri kehakiman komisi eropa yang membuat draft peraturan ini, memberi argumentasinya bahwa peraturan tersebut memberi fokos kepada konsumer yang dianggap sangat penting dalam pengembangan e-commerce di Eropa. Dan the Hague Convention juga bertujuan untuk memberi perlindungan terhadap konsumer. Selanjutnya ditambahkan oleh *Leonello Gabrici*, juru bicara masalah-masalah hukum dari komisi tersebut bahwa kurangnya kepercayaan konsumer adalah hal yang paling signifikan dalam menjaga pertumbuhan e-commerce di Eropa, sehingga dengan keluarnya peraturan tersebut akan mendorong konsumer untuk melakukan pembelian/belanja melalui online. Namun perwakilan perusahaan industri mengajukan debat argumentasi dan

[131] Paul Meller, *E-commerce Law* (internet)

menyatakan bahwa peraturan tersebut akan menimbulkan ketidakpastian hukum bagi perusahaan kecil yang menggunakan internet. Berbeda dengan perusahaan besar yang menganggap peraturan tersebut tidak menimbulkan masalah bagi mereka karena perusahaan mereka yang besar itu mempunyai kantor perwakilan hampir di setiap negara di Eropa. Versi terakhir pasal 7 The Haguae Convention pada bulan April 2001 pada pokoknya menyatakan bahwa consumer boleh menggugat penjual online di pengadilan di tempat mana ia berdomisili.[132] Hal tersebut di atas oleh beberapa ahli hukum masih diperdebatkan, namun pada akhirnya pendapat yang lebih argumentatif menyatakan bahwa perlu diberikan perlindungan terhadap konsumer dengan alasan bahwa konsumer itu lebih lemah posisinya dari pelaku bisnis.

Contoh kasus:

> *On 20 November last year, a Paris court directed Yahoo! to stop French visitors from accessing auctions of Nazi memorabilia. Yahoo! has an operation in France and a website directed at French visitors: www.yahoo.fr. However, the French court's order was directed at the US website operated in the US: www.yahoo.com. If Yahoo! fails to comply within three months of service of the court order, it is liable to a daily fine of FF100,000. Rather than challenge the French ruling, on 21 December, Yahoo! issued proceedings in a California District Court seeking a declaration that the French court ruling could not be enforced in the US.*[133]

Selanjutnya untuk kontrak yang mempuyai unsur asing (conflic of jurisdictions), sampai sekarang ini, masih tetap berlaku hukum perdata internasional antara lain yang menyangkut :

- ***Lex Forum atau Choice of law***, yaitu dalam suatu perjanjian tertulis para pihak memilih dan menentukan hukum apa yang berlaku dan domisi hukumnya apabila terjadi perselisihan di antara mereka. Dan apabila mereka tidak menentukan pilihan hukumnya, maka akan berlaku azas-azas hukum sebagai berikut:

  - ***Lex Loci Contractus***, yakni hukum yang digunakan adalah hukum dimana
    kontrak tersebut dibuat, dan
  - ***Lex Loci Solutionis***, bahwa hukum yang berlaku adalah tempat dimana perjanjian dilaksanakan. Azas-azas tersebut diatas kemudian

[132] Bygrave and Svantesson (2001) 'Jurisdictional issues and consumer protection in cyberspace: the view from down under' [2001] CyberLRes 12
[133] Robbie Downing, IT/Telecoms Partner, Baker & McKenzie, Baker & McKenzie, *Conflics in Cyberspace*

berkembang, sehingga yang paling populer sekarang ini menggunakan azas-azas sebagai berikut :

- ***The Proper Law of the Contract dan***
- ***The Most Characteristic of the Conection.***

Pembuktian dalam E-Commerce

Secara konvensional transaksi atau kontrak atau perjajian dibuat dalam suatu tulisan diatas media kertas lalu dibubuhi tanda tangan oleh para pihak dan ditempelkan meterai secukupnya dimana para pihak bertemu langsung secara phisik atau *face to face*. Sangat berbeda dengan transaksi secara elektronik dimana tulisannya dibuat di media elektronik dengan atau tanpa tanda tangan elektronik dengan atau tanpa meterai yang dilakukan secara maya dimana para pihak tidak bertemu secara phisik.

Transaksi elektronik ini menimbulkan masalah baru dalam hukum pembuktian karena dalam sistem pembuktian tidak dikenal dokumen elektronik. Namun meskipun dokumen elektronik tidak dikenal dalam sistem pembuktian, dalam hal terjadi sengketa di pengadilan dimana para pihak mengajukan bukti berupa dokumen elektronik, maka hakim, sesuai dengan Undang-Undang no. 14 tahun 1970 tentang Kekuasaan Kehakiman yang telah dirubah dengan UU no 35 tahun 1999, tidak boleh menolak perkara dengan alasan tidak ada hukum yang mengaturnya, Hakim dituntut untuk menggali dan menemukan hukum.

Pembuktian Dalam Acara Peradilan

Prof Subekti berpendapat bahwa " membuktikan ialah meyakinkan hakim tentang kebenaran dalil atau dalil-dalil yang dikemukakan dalam satu persengketaan"[134] Dalam hukum acara peradilan di Indonesia bahwa keyakinan hakim tersebut harus diperoleh berdasarkan alat bukti yang sudah ditentukan secara limitatif dalam perundang-undangan yang berlaku.

Prinsip Pembuktian Dalam Acara Perdata

HIR (*Herzien Indonesisch Reglement*) pasal 164 dan kitab Undang-undang Hukum Perdata (KUHP) pada pasal 1866 yang berbunyi: Alat-alat bukti terdiri atas :

1. bukti tulisan
2. bukti dengan saksi-saksi
3. persangkaan-persangkaan
4. pengakuan
5. sumpah

[134] Subekti Prof.SH. Hukum Pembuktian,cetakan ke-3, Pradnya Paramita. Jakarta, 1975, hal 5

HIR juga mengatur pembuktian lain yaitu hasil pemeriksaan setempat, sebagaimana diatur dalam pasal-pasal sebagai berikut:

- Pasal 153 (1) HIR yang berbunyi:" *jika ditimbang perlu atau ada faedahnya, maka ketua boleh mengangkat satu atau dua orang komisaris daripada dewan itu yang dengan bantuan penitera pengadilan akan melihat keadaan setempat atau menjalankan pemeriksaan di tempat itu, yang dapat menjadi keterangan kepada hakim.* "
- Pasal 154 HIR (hasil penyelidikan seorang ahli) yang berbunyi : "jika pengadilan negeri menimbang, bahwa perkara itu dapat lebih terang, jika diperiksa atau dilihat oleh orang ahli maka dapatlah ia mengangkat ahli itu, baik atas permintaan kedua pihak, maupun karena jabatannya."

Timbul pertanyaan, dokumen elektronik dimasukan ke pembuktian mana, dapatkah dokumen elektronik dianggap sama dengan kekuatan hukum salah satu alat bukti di atas, atau apakah dokumen elektronik tidak dapat diajukan sebagai alat bukti.

Kalau disimak, dokumen elektronik adalah tulisan (surat) dalam media elektronik, berbeda dengan tulisan biasa yang dituangkan dalam media kertas. Alat bukti tulisan (surat) ini menurut doktrin ilmu hukum dan undang-undang secara garis besar di bagi menjadi 2 macam :

- Alat bukti tulisan (surat) biasa : yaitu surat yang sejak semula tidak dibuat sebagai alat bukti tetapi kemudian dijadikan bukti, misalnya surat cinta, surat-surat korespondensi dagang [135]
- Tulisan (surat) yang berupa akta
  Tulisan (surat) yang berupa akta ini di bagi menjadi 2 yaitu :
  - Akta di bawah tangan : yaitu akta ini dibuat untuk pembuktian juga, tetapi tidak dibuat dihadapan Pejabat yang berwenang. Contoh akta dibawah tangan adalah kwitansi , surat perjanjian sewa menyewa, jual beli dan sebagainya yang dibuat oleh para pihak sendiri
  - Akta otentik yaitu surat yang dibuat oleh dan dihadapan Pejabat yang berwenang seperti Hakim, Notaris, Pegawai Catatan Sipil dan sebagainya. Akta Otentik merupakan bukti yang sempurna kecuali dapat dibuktikan bahwa akta tersebut tidak benar

Sesuai dengan ketentuan pasal 1868 Kitab Undang-Undang Hukum Perdata (KUH Perdata) yang berbunyi :

"*Suatu akta otentik adalah suatu akta yang didalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau dihadapan pegawai-pegawai umum yang berkuasa untuk itu di tempat dimana akta di buat .* "

[135] Hukum Acara Perdata Dalam Teori dan Praktek , Retno Wulan,SH halaman 64)

Perbedaan akta otentik dan akta dibawah tangan dilihat dari terbentuknya akta tersebut, apabila akta tersebut dibuat dihadapan atau dibuatkan oleh pejabat yang berwenang maka akta tersebut adalah akta otentik dan apabila akta tersebut tidak dibuat dihadapan atau oleh pejabat yang berwenang maka akta itu adalah akta di bawah tangan.

Pembuatan Akta Otentik

1. **Konsep Akta Otentik**

   Pasal 1868 KUHper berbunyi :

   > *Suatu akta otentik ialah suatu akta yang, didalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau dihadapan pegawai-pegawai umum yang berkuasa untuk itu, ditempat mana akte dibuat.*

   Mengacu pada pasal 1868 KUHPerdata (BW), persyaratan suatu dokumen dikatakan otentik, maka dokumen tersebut harus dibuat;

   a. oleh pegawai umum atau pejabat yang berwenang
   b. dihadapan pegawai umum atau pejabat yang berwenang
   c. ditentukan oleh Undang-undang.

   Sebagai pegawai umum yang dimaksudkan di atas berlaku seorang notaris, seorang hakim, seorang jurusita pada suatu pengadilan, seorang pegawai catatan sipil, dan sebagainya. Dengan demikian, maka suatu akte notaris, suatu-surat putusan hakim, suatu surat proses verbal yang dibuat oleh seorang jurusita pengadilan dan suatu surat perkawinan yang dibuat oleh Pegawai Catatan Sipil adalah akta-akta otentik.[136]

2. **Pengesahan Transaksi Elektronik**

   Bagaimana peranan notaris didalam transaksi elektronik bertanda tangan elektronik. Dalam transaksi elektronik dengan menggunakan tanda tangan digital, apakah dokumen yang dihasilkan dapat dinyatakan sebagai akta otentik.

   Di Indonesia belum ada suatu lembaga yang fungsinya sama dengan notaris dalam hal dokumen elektronik. Di beberapa ketentuan internasional sudah ada mengatur tentang CA *(Certification Authority)* yang fungsinya adalah untuk autentifikasi tanda tangan dalam suatu dokumen elektronik. Diisyaratkan bahwa apabila CA tersebut mendapatkan *lisensi* dari pemerintah, maka CA tersebut dapat bertindak sebagai pejabat umum. Jika kita asumsikan bahwa pejabat umum disini mempunyai tanggung jawab yang sama dengan notaris, maka CA yang berlisensi dari pemerintah dapat dipersamakan dengan notaris.

---

[136] Subekti, Hukum pembuktian PT Pradnya Paramita, cet ke-8, 1987, hal 28

3. **Bea Materai Elektronik**

Undang-undang nomor 13 tahun 1985 mengenai bea materai, pasal 2 ayat 1 menyatakan bahwa bea materai wajib dikenakan pada semua dokumen yang hendak dijadikan alat bukti di pengadilan perdata. Selanjutnya ditegaskan lagi di dalam pasal 2 ayat 3 bahwa dokumen yang tidak wajib dikenakan bea materai, maka saat dokumen itu dijadikan bukti surat di pengadilan, maka dokumen itu akan dikenakan bea materai. Surat Keputusan Direktur Jenderal Pajak no. 122.D/PJ/2000, mengizinkan teknik-teknik baru untuk menggunakan materai dengan sistem komputer yang terbatas pada transaksi-transaksi yang mengandung nilai uang sesuai dengan pasal 10 Peraturan no. 24 tahun 2000.

E-Commerce dan Perlindungan Konsumen

Dalam E Commerce, perusahaan perusahaan di internet (internet merchant) pada umumnya tidak memiliki alamat secara fisik di negara tertentu, hal mana akan menimbulkan masalah bagi konsumen untuk mengembalikan produk yang dipesan bila barang yang dikirim tidak sesuai dengan pesanan. Selain itu konsumen juga akan mengalami kesulitan memperoleh jaminan servis atas kerusakan barang yang dipesan dari perusahaan di internet tersebut, juga tidak ada perlindungan atas keamanan dan kerahasiaan data data individual konsumen yang diberikan kepada perusahaan tersebut. Bisa saja terjadi data-data tersebut dicopy dan digunakan untuk tujuan yang merugikan konsumen pemilik data, sebab walaupun kita memiliki Undang-undang Perlindungan Konsumen, akan tetapi tidak cukup mampu mengatasi hal ini .

E-Commerce dan Internet Banking

Dalam E-Commerce, dimungkinkan untuk melakukan pembayaran melalui Bank yang juga dilakukan secara on line / melalui internet . Saat ini sudah banyak bank bank di Indonesia yang menyediakan layanan internet banking, antara lain misalnya www.klik.bca.com. Internet banking biasanya memberikan pelayanan kepada nasabahnya berupa :

- Informasi, dimana Bank menyediakan informasi jasa keuangan saja melalui website nya kepada nasabah.
- Komunikasi, dimana dalam websitenya tersebut bank menyediakan layanan agar nasabah dapat berkomunikasi dengan Bank.
- Transaksi, dimana nasabah dapat melakukan transaksi keuangan seperti pengecekan saldo, transfer dana dan juga berbagai jenis pembayaran melalui internet.

Dalam beberapa kasus transaksi yang terjadi, ada nasabah yang menulis dalam pikiran pembaca Kompas bahwa transaksi yang dilakukan melalui internet ternyata tidak aman, karena setelah melakukan transaksi melalui internet ternyata saldo tabungannya berkurang cukup banyak. Pakar internet RM Roy Suryo mengatakan agar berhati hati bila melakukan transaksi melalui internet di warnet, karena data data transaksi tersebut bisa diketahui orang lain yang menggunakan komputer yang sama, dan dengan data data tersebut orang yang bersangkutan dapat juga melakukan transaksi yang merugikan pengguna jasa layanan internet banking.

BAB VII
KESIMPULAN DAN SARAN

A. KESIMPULAN

Berdasarkan pada penelitian atas sejumlah pasal-pasal dalam Kitab Undang-Undang Hukum Pidana, dan setelah membandingkan dengan ketentuan pidana dan yurisprudensi yang berlaku di beberapa negara, penulis berpendapat bahwa Kitab Undang-Undang Hukum Pidana dan peraturan perundang-undangan yang berlaku sekarang ini belum bisa menjangkau seluruh bentuk 'kejahatan komputer' oleh karena itu perlu disempurnakan, sebagai berikut:

1. Pencurian dan penggelapan

Pasal-pasal mengenai pencurian dan penggelapan hanya dapat diperlakukan terhadap 'barang' sebagai 'tangible object' dan tidak dapat diperlakukan terhadap 'data komputer', oleh karena itu perlu disusun pengaturan yang khusus yang mengatur pencurian dan penggelapan 'data komputer'.

Pengambilan uang melalui 'Automatic Teller Machine" seringkali menimbulkan permasalahan hukum oleh karena tidak jelas apakah mengambil uang tanpa dana yang cukup atau mengambil uang padahal rekening sipelaku telah ditutup termasuk pencurian atau bukan. Untuk itu perlu dibuat ketentuan yang baru mengenai penggunaan 'cash-card'.

2. Pemalsuan

Dilihat dari sejarah perundang-undangan pemalsuan hanya dilakukan terhadap 'instrument' yang bisa dilihat ('visual readibility') seperti kertas yang berupa 'tangible object'. Beberapa pakar hukum lainnya berpendapat bahwa pemalsuan dapat dilakukan juga terhadap bahan yang secara langsung tidak dapat dibaca seperti 'data komputer', namun dapat dibaca oleh alat yang khusus untuk itu seperti komputer, asal saja 'data komputer' itu bersifat permanen, misalnya 'program komputer'. Oleh karena itu ketentuan mengenai pemalsuan dapat diperlakukan terhadap hal tersebut.

Namun beberapa pakar lainnya berpendapat bahwa oleh karena 'data komputer' bukan merupakan 'tangible object' maka ketentuan mengenai pemalsuan tidak dapat diterapkan terhadap 'data komputer', oleh karena perlu disusun ketentuan baru yang memperluas pengertian pemalsuan juga meliputi data komputer'. Untuk menghilangkan keragu-raguan

seyogyanya disusun ketentuan baru yang memperjelas ketentuan pemalsuan sehingga dapat dilakukan juga terhadap 'data komputer'.

3. **Penipuan – Internet fraud**

Ketentuan pidana mengenai hal ini mensyaratkan adanya orang tertentu yang ditipu, tidak cukup apabila hanya mesin yang ditipu. Beberapa negara telah menyempurnaan pengertian penipuan sehingga meliputi juga mesin. Namun beberapa yurisprudensi telah memperluas penerapan ketentuan mengenai 'orang' sehingga meliputi juga 'pemerintah'. Agar tidak menimbulkan keragu-raguan mengenai hal ini seyogyanya dibuat ketentuan baru yang memperjelas pengertian penipuan.

Dengan munculnya Internet fraud perlu dipikirkan pula agar kejahatan ini dapat dijangkau oleh amandemen undang-undang.

4. **Perusakan, sabotase dan digital vandalism**

Menurut sejarahnya ketentuan mengenai perusakan dan sabotase ditujukan terhadap barang sebagai objek, oleh karena itu perbuatan yang dilarang ialah 'physical damage'. Ketentuan dalam KUHP mengenai hal ini tidak dapat diterapkan terhadap perusakan terhadap 'data komputer' yang merupakan 'logical damage', kecuali apabila 'data komputer' mempunyai hubungan yang sangat erat dengan 'data carrier', sehingga kerusakan yang dialami oleh 'data komputer' dapat mengganggu berfungsinya komputer tersebut. Beberapa yurisprudensi memutuskan bahwa 'perbuatan merubah kode untuk memasuki sistim komputer secara melawan hukum yang menyebabkan sipemilik komputer tidak dapat memasuki sistim komputer, atau perbuatan 'merubah atau merusak data komputer sehingga mengganggu berfungsinya sistim komputer' tersebut dianggap sebagai perbuatan merusak. Untuk menghilangkan keragu-raguan diperlukan ketentuan baru mengenai hal itu.

5. **Tanpa hak menggunakan komputer**

Ketentuan pidana dalam Kitab Undang-Undang Hukum Pidana tidak dapat menjangkau perbuatan 'tanpa hak menggunakan komputer'. Perbuatan 'furtum usus' hanya diperlakukan terhadap 'joyriding'. Oleh karena itu diperlukan suatu ketentuan baru yang mengatur 'computer-trespass atau 'joycomputing'.

6. **Tanpa hak menggunakan fasilitas dan waktu komputer**

Yurisprudensi beberapa negara menunjukkan bahwa ketentuan pidana mengenai 'tanpa hak menggunakan komputer' tidak dapat diperluas

terhadap perbuatan 'tanpa hak menggunakan fasilitas dan waktu komputer', oleh karena itu perlu diatur ketentuan baru mengenai hal tersebut dalam KUHP.

7. Tanpa hak memasuki sistim komputer

Ketentuan dalam Kitab Undang-Undang Hukum Pidana tidak dapat menjangkau perbuatan ini. Untuk ini diperlukan ketentuan baru. Penal Code di Amerika Serikat mewajibkan semua perguruan tinggi mengeluarkan peraturan disiplin intern yang melarang para mahasiswa untuk melakukan hacking atas sistem komputer orang/lembaga lain.

8. Perbuatan memata-matai (spionase)

Ketentuan yang berlaku mengenai membocorkan rahasia negara dapat diperlakukan terhadap perbuatan membocorkan rahasia yang terkandung dalam data komputer yang dilakukan oleh siapa saja.

Perlindungan terhadap pembocoran rahasia perusahaan atau rahasia industri hanya dapat diperlakukan terhadap perbuatan pegawai yang diberi tugas untuk merahasiakannya, namun tidak dapat diperluas terhadap orang luar, oleh karena itu diperlukan ketentuan baru mengenai hal ini.

B. SARAN

Dalam menyusun KUHPNasional perlu dipertimbangkan pendapat para pakar hukum pidana yang memperingatkan agar berhati-hati dalam memidana suatu perbuatan penyalahgunaan komputer, sehingga akan menghindari timbulnya 'over criminalization'. Piragoff, misalnya memberi 10 nasehat sebagai berikut:

1. Pastikan perilaku computer apa yang sering dikeluhkan oleh masyarakat, kelompok industri, pemerintah dan lainnya yang berkepentingan
2. Pelajari tingkatan sejauh mana hukum tradisional dapat diperlakukan terhadap "penyalahgunaan komputer tersebut (computer abuses) dan tingkatan dimana penyalahgunaan itu hanya merupakan kejahatan komputer biasa yang dilakukan dengan cara baru. Apabila undang-undang yang berlaku tidak dapat diterapkan, pastikan mengapa. Apabila undang-undang dapat diterapkan persoalkan mengapa, berdasarkan kebijaksanaan, undang-undang itu dapat diterapkan
3. Untuk penyalahgunaan komputer yang tidak dapat dijangkau secara penuh oleh undang-undang yang berlaku, persoalan yang timbul ialah apakah, dan

sejauh mana, perbuatan-perbuatan itu harus dilarang oleh hukum pidana, hukum administrasi, hukum perdata, atau tidak dilarang sama sekali. Untuk penyalahgunaan itu, identifikasi kepentingan masyarakat yang dituduhkan telah dilanggar.

4. Pelanggaran komputer dapat melanggar lebih dari satu kepentingan, atau dapat dikonseptualisasikan dengan cara lain. (Misalnya membaca atau mengkopi data arsip orang lain capat dikonseptualisasikan sebagai pelanggaran hak cipta, pembajakan atau tanpa hak memiliki data atau informasi. Identifikasi semua kepentingan dan cara-cara.
5. Setelah mempelajari semua kepentingan, tentukan apakah pelanggaran yang sama atau hampir bersamaan dalam suasana diatur oleh undang-undang. (Misalnya, apakah ada pelangaran atas hukum yang berlakui selaras dengan perusakan data komputer). data).
6. Sebaliknya, pastikan apakah pelanggaran itu dan kepentingan dalam suasana "non-computer" mempunyai kesamaan (pararel) dengan pelanggaran yang ada, seperti perusakan barang atau penyadapan komunikasi.
7. Apabila jawaban terhadap pertanyaan 6 benar, pastikan apakah dapat dibenarkan untuk melindungi kepentingan-kepentingan tersebut hanya dengan suasana non-computer ataukah kepentingan itu harus dilindungi secara sama dalam suasana komputer. (misalnya pencurian terhadap barang yang berupa "tangible property" dan kepemilikan yang tidak syah atas informasi tidak boleh dipersamakan, perusakan barang dan perusakan data dapat dipersamakan)
8. Apabila jawaban atas pertanyaan 6 negatif, pastikan apakah dapat dibenarkan untuk melindungi kepentingan dalam suasana komputer yang tidak dilindungi dalam suasana non-computer (seperti misalnya perubahan atau penambahan data).
9. Setelah mengidentifikasi pelanggaran dan kepentingan-kepentingan, dan bagaimana hukum yang berlaku dapat diterapkan, apabila dapat diperlakukan, pastikan apakah penerapan secara legislative dan peradilan atau perluasan undang-undang terhadap pelanggaran dapat menciptakan akibat hukum atau social ekonomi yang tidak dapat dijamin.
10. Pastikan batasan apa diperlukan untuk mendefinisikan pelanggaran agar supaya tepat pada yang bersangkutan (To Whom It MayConcern). To Whom It May Concern membedakan perilaku penjahat dengan yang bukan dan menghalangi pemidanaan yang berkelebihan (over-criminalization)[137]

Bagi Indonesia perlu penyempurnaan/pengaturan dalam Kitab Undang-undang Hukum Pidana untuk dapat menjangkau segala jenis kejahatan komputer, antara lain dengan mengatur perbuatan-perbuatan:

[137] Piragoff (1986), hal. 128-129.

1. Secara melawan hukum merubah /menghapus/membuat tidak berguna data yang dipergunakan untuk proses otomatis.
2. Secara melawan hukum mengambil data yang disimpan dalam tempat penyimpanan data pribadi.
3. Secara melawan hukum menyadap (mengintersepsi) dengan alat teknis data yang dikirimkan melalui sarana telekomunikasi umum.
4. Tanpa hak menggunakan fasilitas komputer dengan maksud untuk memperoleh keuntungan yang tidak syah.
5. Memperluas pengertian barang sehingga meliputi data komputer, jaringan komputer, system komputer, dan penggunaan komputer tanpa ijin.
6. Memperluas pengertian barang dalam perusakan/sabotase sehingga meliputi "digital goods".
7. Mengundangkan ketentuan mengenai Electronic Commerce dengan mempertimbangkan model Indian Electronoc Commerce Act 1998.
8. Money laundering
   Kewajiban memberikan batas uang yang disimpan di bank tanpa memberikan informasi asal-usul uang dalam praktek seringkali dapat diterobos dengan menggunakan kurir-kurir (couriers) yang banyak atas perintah mereka yang memperoleh uang haram. Perlu pembuatan undang-undang sehingga perbuatan money laundering yang dilakukan antar bank dan di "cyberspace" dapat juga dituntut, oleh karena dengan semakin ketatnya pengawasan terhadap peredaran "cash money", para sindikat kejahatan sudah memulai operasinya dengan menggunakan "electronic cash-E-cash)" yang dengan cara yang canggih ditransfer keberbagai bank di seluruh dunia sehingga menghilangkan jejak asal-usul uang tersebut.
9. Penipuan dan Internet-fraud
   Internet-fraud seringkali menimbulkan kerugian dan sulit untuk dilacak, oleh karena sipembeli seringkali tidak mengetahui apakah sipenjual barang yang ditawarkan melalui Internet betul-betul sipenjual dengan itikad baik dan bukan penipu. Oleh karena itu pembayaran lebih dahulu dengan menggunakan credit-card atau lainnya sebaiknya tidak dilakukan dan identitas sipenjual harus jelas.
   Dengan demikian perlu diundangkan amandemen undang-undang tentang penipuan yang menjangkau penipuan melalui Internet (Internet fraud).[138]
10 Pemberatan sanki pidana
   Mengingat bahaya yang bisa ditimbulkan oleh kejahatan komputer terhadap harta benda maupun jiwa manusia sangat besar, maka selain

[138] Federal Court telah mengadili pelaku kejahatan penipuan melalui Internet (Internet fraud) oleh karena ia memasarkan obat HIV tanpa disetujui Drug Office.
Dalam kasus lainnya seorang pelaku diadili oleh karena menjual obat viagra melalui Internet tanpa pemeriksaan fisik sipembeli sesuai dengan persyaratan kedokteran yang berlaku.

menyempurnakan peraturan perundang-undangan yang ada, perlu dipertimbangkan pemberatan ancaman pidana terhadap kejahatan komputer antara lain mengenai:

1). pencurian,
2). penggelapan,
3). pemalsuan,
4). penipuan termasuk Internet fraud,
5). perusakan/sabotase/digital vandalism,
6). membocorkan rahasia perusahaan,
7). money laundering.

Sesuai dengan kewajiban yang ditugaskan oleh Undang-Undang Pokok Kekuasaan Kehakiman, hakim harus selalu siap memeriksa dan mengadili berbagai jenis kejahatan komputer. Sebelum undang-undang baru mengenai kejahatan komputer diundangkan, hakim di luar negeri, dan peraturan perundang-undangan mengenai kejahatan komputer dari berbagai negara kiranya perlu dikaji lebih lanjut dan diadaptasi sepanjang berkesesuaian dengan perundang-undangan yang berlaku di Indonesia.

DAFTAR KEPUSTAKAAN

1. Barret, Neil, "Digital Crimes: Policing Cybernation", Kohan Page, 1997.
2. Budi Agus Riswandi , Hukum dan Internet di Indonesia, UII Press, April 2003.
3. Bernard Arif Sidharta.Refleksi tentang struktur Ilmu Hukum, Mandar Maju Bandung 2000;
4. Cyber laundering: Anonymous Digital Cash and Money Laundering,1996 R. Mark Bortner, Presented as final paper requirement for Law & the Internet (LAW 745).A seminar at the University of Miami School of Law.
5. Centrale Recherche Informatie Bulletin, "Computer Criminaliteit", 1990, The Hague.
6. Clare Sullivan, "The Response of the Criminal Law in Australia to Electronic Funds, 1990.
7. Colin Tapper, Computer Law, Longman, London-New York, 1989 (Fourth Edition).
8. D.K. Piragoff, "Combatting Computer Crime with Criminal Law", dalam Strafrecht in de Informatiemaatschappij, Symposium, Vrije Universiteit Amsterdam, 22 April 1986.
9. Eddy D. Karnasudirdja, "Memberantas Kejahatan Komputer dengan Hukum Pidana", Suatu Syllabus, Leiden, 1991.
10. Gordon Hughes, Essays on Computer Law, Longman Professional, 1990.
11. H.W.K. Kaspersen, "Standards for Computer Crime Legislation: A Comparative Analysis", dalam Computer Law Series No.3, 1987.
12. ------Strafbaarstelling van Computermisbruik, Kluwer, 1990.
13. H.W.K. Kaspersen en N. Keijzer, "Het Nederlandse Strafrecht en Computermisbruik", dalam Strafrecht in de Informatiemaatschappij, Symposium, Vrije Universiteit Amsterdam, 22 April 1986
14. Hans Franken, Report of the Dutch Committee on Computer Crime, Ministry of Jutice, the Hague, 1988.
15. -----"Computing and Security", dalam Amongst Friends in Computer Law, Computer Law Series No.8, 1990.
16. Harvard International Law Journal I, Volume 30, 1989.
17. Hilary E. Pearson, "Recent Developments in Computer Law in the United States of America, dalam buku Gordon Hughes Essays on Computer Law, Longman Professional, 1990.
18. Hugo Cornwall, Data Theft, Mandarin, 1990.
19. Indian Electronic Commerce Act - 1998
20. International Herald Tribune, "When Law Allows Computer Raids", 22 March 1991, pp.1 dan 4.

21. M.Arsyad Sanusi , Makalah Dasar Dasar E Commerce ;
22. M.Arsyad Sanusi , E Commerce , Hukum dan Solusinya , PT.Mizan Grafika Sarana Juni 2001 ,
23. Martin Wasik, "Computer Crime": Recent Developments, Yearbook of Law Computer and Technology, Volume Three,1987
24. Crime and the Computer, Oxford University Press.
25. Minkenhof A,De Nederlandse Strafvordering, Vierde herziene druk, 1981.
26. Paul Marett Information Law and Practice, Gower, 1991.
27. Peter Blume, "Computer Crime Legislation in Denmark", Yearbook of Law Computer and Technology, Volume Three, 1987.
28. R.A. Brown, "Computer-related Crime in Australia", dalam buku Gordon Hughes Essays on Computer Law, Longman Professional, 1990.
29. Rostoker, M.D. et al Computer Jurisprudence, Oceana, 1986.
30. Scott, Michael D, Computer Law, John Wiley & Sons, 1989.
31. Stein Schjolberg, Computers and Penal Legislation, A Study of the Legal Politics of a New Technologyplex-Norwegian Research Centre for Computers and Law, Universitetsforlaget, 1983.
32. Stephen Saxby, "The Role of Law in the Development of the Information Society", Computer Law Series No.8, 1990.
33. "Transfer Abuse", dalam buku Gordon Hughes, Essays in Computer Law, Longman Professional, 1990, hal.248-280.
34. Ulrich Sieber, "New Legislative Responses to Computer-Related Economic Crimes and Infringements of Privacy, A Comparative Analysis of Major Western Legislations and International Solutions", dalam Strafrecht in de Informatie Maatschappij, Symposium, Vrije Universiteit Amsterdam, 22 April 1986.
35. -----"The Emergence of Criminal Information Law", dalam Amongst Friends in Computer Law, Computer Series 8.
36. -----The International Handbook on Computer Crime, 1986.
37. Undang-undang No. 19 Tahun 2002 tentang Hak Cipta
38. Kitab Himpunan Perundang-undangan Republik Indonesia (Disusun menurut sistem Engelbrecht), 1989.
39. Kitab Undang-Undang Hukum Acara Pidana, 1981
40. Model State Computer Penal Code
41. U.S. Federal Computer Crimes Law: Chapter 33. Computer Crimes (Last amendment September 2001)
42. Report of The British Law Commission on Computer Misuse, 1989
43. Texas Computer Crimes Statute
44. The American Journal of Comparative Law, Volume 37, 1989.
45. Yves Poullet, "The Law and New Information Technology: A Comparative Approach to the Laws of Continental Europe", dalam buku Gordon Hughes Essays on Computer Law, Longman Professional, 1990.

46. O.Bidara dan Martin P.Bidara , Hukum Acara Perdata , PT.Pradnya Paramita, Jakarta 1987
47. Retno Wulan Sutantio, Hukum Acara Perdata, dalam Teori dan Praktek, Mandar Maju Bandung , 1997;
48. Subekti, SH, Prof , Hukum Perjanjian
49. SubektiSH, Prof : Kitab Undang-Undang Hukum Perdata, Pratnya Paramita1980
50. http://www.cyberlaw.lkht.org.
51. http://www.hukum.online.com
52. http://www.austlii.com

LAMPIRAN I
TEXAS COMPUTER CRIMES LAW

In 1985, a computer crimes law for the state of Texas took effect. Under this state law, it is a crime to make unauthorized use of protected computer systems or data files on computers, or to make intentionally harmful use of such computers or data files. The seriousness of such a crime ranges from Class B misdemeanor to third-degree felony.

The complete text of the computer crimes chapter of the Penal Code appears below. Since this is a state law, ignorance is not a defense. Thus, it is in your own best interest to be familiar with it. Notice that sharing passwords without the system administrator's permission is a Class A misdemeanor.

Texas Computer Crimes Statute

SECTION 1. Title 7, Chapter 33, Texas Penal Code
"Section 33.01. DEFINITIONS.
In this chapter:

(1) 'Communications common carrier' means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.
(2) 'Computer' means an electronic device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communications facilities that are connected or related to the device. 'Computer' includes a network of two or more computers that are interconnected to function or communicate together.
(3) 'Computer program' means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.
(4) 'Computer security system' means the design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.

(5) Data' means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, and punchcards, or may be stored internally in the memory of the computer.

(6) 'Electric utility' has the meaning assigned by Subsection (c), Section 3, Public Utility Regulatory Act (Article 1446c, Vernon's Texas Civil Statutes).

Section 33.02. BREACH OF COMPUTER SECURITY.

(a) A person commits an offense if the person:

(1) uses a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer and the actor knows that there exists a computer security system intended to prevent him from making that use of the computer; or

(2) gains access to data stored or maintained by a computer without the effective consent of the owner or licensee of the data and the actor knows that there exists a computer security system intended to prevent him from gaining access to that data.

(b) A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict the use of acomputer or to restrict access to data stored or maintained by a computer.

(c) An offense under this section is a Class A misdemeanor.

Section 33.03. HARMFUL ACCESS.

(a) A person commits an offense if the person intentionally or knowingly:

(1) causes a computer to malfunction or interrupts the operation of a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer; or

(2) alters, damages, or destroys data or a computer program stored, maintained, or produced by a computer, without the effective consent of the owner or licensee of the data or computer program.

(b) An offense under this section is:

(1) a Class B misdemeanor if the conduct did not cause any loss or damage or if the value of the loss or damage caused by the conduct is less than $200;

(2) a Class A misdemeanor if the value of the loss or damage caused by the conduct is $200 or more but less than $2,500; or

(3) a felony of the third degree if the value of the loss or damage caused by the conduct is $2,500 or more.

Section 33.04. DEFENSES.
It is an affirmative defense to prosecution under Sections 33.02 and 33.03 of this code that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is necessary incident to the condition of service or to the protection of the rights or property of the communications common carrier or electric utility.

"Section 33.05. ASSISTANCE BY ATTORNEY GENERAL.
The attorney general, if requested to do so by a Prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer."

LAMPIRAN II
US FEDERAL COMPUTER CRIMES LAW

CHAPTER 33. COMPUTER CRIMES

§ 33.01. Definitions
In this chapter:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.

(2) "Aggregate amount" means the amount of:
   (a) any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen or rendered unrecoverable by the offense; or
   (b) any expenditure required by the victim to verify that a computer, computer network, computer program, or computer system was not altered, acquired, damaged, deleted, or disrupted by the offense.

(3) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(4) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(5) "Computer network" means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(6) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(7) "Computer services" means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(8) "Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

(9) "Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

(10) "Computer virus" means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punchcards, or may be stored internally in the memory of the computer.

(12) "Effective consent" includes consent by a person legally authorized to act for the owner. Consent is not effective if:

(a) induced by deception, as defined by Section 31.01, or induced by coercion;

(b) given by a person the actor knows is not legally authorized to act for the owner;

(c) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;

(d) given solely to detect the commission of an offense; or

(e) used for a purpose other than that for which the consent was given.

(13) "Electric utility" has the meaning assigned by Section 31.002, Utilities Code.

(14) "Harm" includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(15) "Owner" means a person who:

(a) has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;

(b) has the right to restrict access to the property; or

(c) is the licensee of data or computer software.

(16) "Property" means:

(a) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or

(b) the use of a computer, computer system, computer network, computer software, or data.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, § 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

Amended by Acts 1997, 75th Leg., ch. 306, § 1, eff. Sept. 1, 1997; Acts 1999, 76th Leg., ch. 62, § 18.44, eff. Sept. 1, 1999.

§ 33.02. Breach of Computer Security

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:

(1) a Class A misdemeanor if the aggregate amount involved is less than $1,500;

(2) a state jail felony if:

(a) the aggregate amount involved is $1,500 or more but less than $20,000; or

(b) the aggregate amount involved is less than $1,500 and the defendant has been previously convicted two or more times of an offense under this chapter;

(3) a felony of the third degree if the aggregate amount involved is $20,000 or more but less than $100,000;

(4) a felony of the second degree if the aggregate amount involved is $100,000 or more but less than $200,000; or

(5) a felony of the first degree if the aggregate amount involved is $200,000 or more.

(c) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or deletion of property may be aggregated in determining the grade of the offense.

(d) A person who his subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, § 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

Amended by Acts 1997, 75th Leg., ch. 306, § 2, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 1411, § 1, eff. Sept. 1, 2001.

§ 33.03. Defenses

It is an affirmative defense to prosecution under Section 33.02 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Renumbered from § 33.04 and amended by Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

§ 33.04. Assistance by Attorney General

The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Renumbered from § 33.05 by Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

LAMPIRAN IV

*Indian Electronic Commerce Act - **1998***

Part XII – Computer Crime

49. Computer Crime.

For the purpose of this Act, any person who commits any of the following acts is guilty of an offense of computer crime:

(a) Intentionally accesses, damages or conceals, or attempts to access, damage or conceal, temporarily or permanently, any computer data base, computer, information system or computer network, without permission from the owner, in order to either:
   (i) wrongfully control, obtain, make use of or prevent others from deriving the benefits of money, property, data or electronic records;
   (ii) copy or destroy any data or electronic records;
   (iii) use or disrupt any functions of computers, computer networks or information systems; or
   (iv) commit any act that is an offense under the Indian Penal Code.

(b) Knowingly, and with the intent to defraud, obtains or attempts to obtain any computer services by false representation, false statement or unauthorized charging to the account of another, by installing or tampering with any facilities or equipment, or by any other means.

(c) Intentionally or recklessly introduces or allows the introduction of any computer virus into any computer, computer system or computer network without permission of the owner.

Comments:

This section provides for the enumeration of various acts that shall be considered computer crimes. Fundamental to the approach taken in this section is the recognition that the Indian Penal Code, 1860 already enumerates a wide variety of crimes that include acts committed through or in connection with computers. For, example, the Indian Penal Code covers all acts of larceny, without any limitations regarding the means by which the larceny is committed. If the larceny takes the form of manually stealing goods from a store or stealing money from a remote bank account through use of a computer, the law treats either act as the same for purposes of classification as larceny. Thus, the fact that a crime is committed by computer does not limit the applicability of the Indian Penal Code in most instances. This section, therefore, does not attempt to identify all criminal acts involving computers, at least in instances where such acts already would be considered crimes under the Indian Penal Code. Instead, this section merely acknowledges that any act that is considered criminal under

the Penal Code may also be called a computer crime when computers are involved.

In addition, this section specifies certain acts as computer crimes when the Indian Penal Code appears not to apply. In particular, the introduction of viruses into computers and the appropriation or disruption of computer services are unique to the computer environment and do not appear to be covered by the Penal Code. It can be years, or by both.

(d) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, all offenses under this Act shall be bailable, nonrecognizable, and triable exclusively by the Chief Metropolitan Magistrate, Additional Chief Metropolitan Magistrate, Chief Judicial Magistrate or Additional Chief Judicial Magistrate.

Comments:

This section provides criminal penalties for the offenses enumerated in Section 49. Some leniency was provided in cases of first offenses where no damage occurred as a result of the criminal act. On the other hand, additional fines were imposed in cases where governmental or public property is damaged. As indicated in the commentary to Section 49, the Indian Penal Code already provides for penalties in the case of many criminal acts without regard to whether a computer is involved. Therefore, this section specifies that nothing in this Act should be construed to abrogate any penalties that may be applicable under the Penal Code.

51. Forfeiture.

(a) Any person who commits the offense of computer crime as set forth in Section 49 of this Act shall forfeit, according to the provisions of this section, any monies, profits or proceeds, and any interest or property which the sentencing court determines he has acquired or maintained, directly or indirectly, in whole or in part, as a result of such offense. Such person shall also forfeit any interest in, security, claim against or contractual right of any kind which affords him a source of influence over any enterprise which he has established, operated, controlled, conducted or participated in conducting, where his relationship to or connection with any such thing or activity directly or indirectly, in whole or in part, is traceable to any item or benefit which he has obtained or acquired through computer fraud.

(b) Any computer, computer system, computer network or any software or data, owned by such person, which is used during the commission of any public offense described in Section 49 or any computer, owned by the person, which is used as a repository for the storage of software or data illegally obtained in violation of Section 49 shall be subject to forfeiture under orders of the Court ordering his conviction.

Comments:
This section provides for the forfeiture of any benefits derived by any criminal offended as a result of the commission of any computer crime, as well as the forfeiture of any computers or related apparatus used in the commission of such crime.