CyberLaw

Cyber Law adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet/elektronik yang dimulai pada saat mulai "online" dan memasuki dunia cyber atau maya. Pada negara yang telah maju dalam penggunaan internet/elektronik sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju.

Berikut ini adalah ruang lingkup atau area yang harus dicover oleh cyberlaw. Ruang lingkup cyberlaw ini akan terus berkembang seiring dengan perkembangan yang terjadi pada pemanfaatan Internet dikemudian hari.

1. Electronic Commerce.

Pada awalnya electronic commerce (E-Commerce) bergerak dalam bidang retail seperti perdagangan CD atau buku lewat situs dalam World Wide Web (www). Tapi saat ini Ecommerce sudah melangkah jauh menjangkau aktivitas-aktivitas di bidang perbankan dan jasa asuransi yang meliputi antara lain ”account inquiries”, ”1oan transaction”, dan sebagainya. Sampai saat ini belum ada pengertian yang tunggal mengenai E-Commerce.

Hal ini disebabkan karena hampir setiap saat muncul bentuk- bentuk baru dari Ecommerce dan tampaknya E-Commerce ini merupakan salah satu aktivitas cyberspace yang berkembang sangat pesat dan agresif. Sebagai pegangan (sementara) kita lihatdefinisi E-Commerce dari ECEG-Australia (Electronic Cornmerce Expert Group) sebagai berikut: “Electronic commerce is a broad concept that covers any commercial transaction that is effected via electronic means and would include such means as facsimile, telex, EDI, Internet and the telephone”.

Secara singkat E-Commerce dapat dipahami sebagai transaksi perdagangan baik barang maupun jasa lewat media elektronik. Dalam operasionalnya E-Commerce ini dapat berbentuk B to B (Business to Business) atau B to C (Business to Consumers). Khusus untuk yang terakhir (B to C), karena pada umumnya posisi konsumen tidak sekuat perusahaan dan dapat menimbulkan beberapa persoalan yang menyebabkan para konsumen agak hati-hati dalam melakukan transaksi lewat Internet.

Persoalan tersebut antara lain menyangkut masalah mekanisme pembayaran (payment mechanism) dan jaminan keamanan dalam bertransaksi (security risk). Mekanisme pembayaran dalam E-Commerce dapat dilakukan dengan cepat oleh konsumen dengan menggunakan ”electronic payment”. Pada umumnya mekanisme pembayaran dalam E-Commerce menggunakan credit card. Karena sifat dari operasi Internet itu sendiri, ada masalah apabila data credit card itu dikirimkan lewat server yang kurang terjamin keamanannya. Selain itu, credit card tidak ”acceptable” untuk semua jenis transaksi. Juga ada masalah apabila melibatkan harga dalam bentuk mata uang asing.

Persoalan jaminan keamanan dalam E-Commerce pada umumnya menyangkut transfer informasi seperti informasi mengenai data-data credit card dan data-data individual konsumen. Dalam area ini ada dua masalah utama yang harus diantisipasi yaitu (1) ”identification integrity” yang menyan gkut identitas si pengirim yang dikuatkan lewat ”digital signature”, dan (2) adalah ”message integrity” yang menyangkut apakah pesan yang dikirimkan oleh si pengirim itu benar-benar diterima oleh si penerima yang dikehendaki (intended recipient). Dalam kaitan ini pula para konsumen memiliki kekhawatiran adanya ”identity theft”’atau ”misuse of information” dari data-data yang diberikan pihak’ konsumen kepada perusahaan.

Persoalan-persoalan/Aspek-aspek hukum terkait.

a. Kontrak Persoalan mengenai kontrak dalam E-Commerce men gemuka karena dalam transaksi ini kesepakatan antara kedua belah pihak dilakukan secara elektronik. Akibatnya, prinsip-prinsip dalam hukum kontrak tradisional seperti waktu dan tempat terjadinya suatu kontrak harus mengalami modifikasi. Sebagai contoh, the UNCITRAL Model Law on Electronic Commerce dalam Pasal 15 memberikan panduan sebagai berikut :
   * Kecuali jika disepakati antara originator dan penerima, pengiriman pesan data terjadi ketika memasuki sistem informasi di luar kendali pencetus atau dari orang yang mengirim pesan data atas nama originator
   * Kecuali disepakati lain antara originator dan penerima, waktu penerimaan pesan data ditentukan sebagai berikut: (a) jika penerima telah menunjuk suatu sistem informasi untuk tujuan menerima pesan data, penerimaan terjadi: (i) saat pesan data memasuki sistem informasi yang ditunjuk, atau "pencetus" dari pesan data berarti seseorang oleh om wh, atau pada yang b ehalf, pesan yang dimaksudkan data telah dikirim atau dihasilkan sebelum penyimpanan, jika ada, tetapi tidak termasuk orang yang bertindak sebagai perantara berkenaan dengan bahwa pesan data "(Art.2c dari UNCITRAL Model Law). "Email" dari pesan data berarti seseorang yang dimaksudkan oleh originator untuk menerima pesan data, tetapi tidak termasuk orang yang bertindak sebagai perantara berkenaan dengan bahwa pesan data (Art.2d dari UNClTRAL Model Law). (ii) jika pesan data dikirim ke sistem informasi dari penerima yang is.not sistem informasi menunjuk, pada saat pesan data diambil oleh si alamat tersebut; (b) jika penerima belum ditentukan sistem informasi , penerimaan terjadi ketika pesan data memasuki sistem informasi si alamat tersebut.

b. Perlindungan konsumen
   Masalah perlindungan konsumen dalam E-Commerce merupakan aspek yang cukup penting untuk diperhatikan, karena beberapa karakteristik khas E-Commerce akan menempatkan pihak konsumen pada posisi yang lemah atau bahkan dirugikan seperti; Perusahaan di Internet (the Internet merchant) tidak memiliki alamat secara fisik di suatu negara tertentu, sehingga hal ini akan menyulitkan konsumen untuk mengembalikan produk yang tidak sesuai dengan pesanan; Konsumen sulit memperoleh jaminan untuk mendapatkan ”local follow up service or repair”;
   Produk yang dibeli konsumen ada kemungkinan tidak sesuai atau tidak kompatibel dengan persyaratan lokal (loca1 requirements);

c. Pajak (Taxation)
   Pengaturan pajak merupakan persoalan yang tidak mudah untuk diterapkan dalam E-Commerce yang beroperasi secara lintas batas. Masing-masing negara akan menemui kesulitan untuk menerapkan ketentuan pajaknya, karena baik perusahaan maupun konsumennya sulit dilacak secara fisik. Dalam masalah ini Amerika telah mengambil sikap bahwa ”no discriminatory taxation against Internet Commerce”. Namun, dalam urusan tarif (bea masuk) Amerika mempertahankan pendirian bahwa Internet harus merupakan ”a tariff free zone”. Sedangkan Australia berpendirian bahwa ”the tariff-free policy” itu tidak boleh diberlakukan untuk ”tangible products” yang dibayar secara on- line tapi dikirimkan secara konvensional.

d. Jurisdiksi (Jurisdiction)
   Peluang yan g diberikan oleh E-Commerce untuk terbukanya satu bentuk baru perdagangan internasional pada saat yang sama melahirkan masalah baru dalam penerapan konsep yurisdiksi yang telah mapan dalam sistern, hukum tradisional. Prinsip-prinsip yurisdiksi seperti tempat terjadinya transaksi (the place of transaction) dan hukum kontrak (the law of contract) menjadi usang (obsolete) karena operasi Internet yang lintas batas. Persoalan ini tidak bisa diatasi hanya dengan upaya-upaya di level nasional, tapi harus melalui kerjasama dan pendekatan internasional.

e. Digital Signature

Digital signature merupakan salah satu isu spesifik dalam E-Commerce. Digital signature ini pada prinsipnya berkenaan dengan jaminan untuk ”message integrity” yang menjamin bahwa si pengirim pesan (sender) itu benar-benar orang yang b erhak dan bertanggung jawab untuk itu (the sender is the person whom they purport to be). Hal ini berbeda dengan ”real signature” yang berfungsi sebagai pangakuan dan penerimaan atas isi pesan/dakumen, Persoalan hukum yang muncul seputar ini antara lain berkenaan dengan fungsi dan kekuatan hukum digital signature. Di Amerika saat ini telah ditetapkan satu undang-undang yang secara formal mengakui keabsahan digital signature.

f. Copy Right.
Internet dipandang sebagai media yang b ersifat ”low-cost distribution channel” untuk penyebaran informasi dan produk-produk entertainment seperti film, musik, dan buku. Produk-produk tersebut saat ini didistribusikan lewat ”physical format” seperti video dan compact disks. Hal ini memungkinkan untuk didownload secara mudah oleh konsumen. Sampai saat ini belum ada perlindungan hak cipta yan g cukup memadai untuk menanggulangi masalah ini.

g. Dispute Settlement
Masalah hukum lain yang tidak kalah pentingnya adalah berkenaan dengan mekanisme penyelesaian sengketa yang .cukup memadai untuk mengantisipasi sengketa yang kemungkinan timbul dari transaksi elektronik ini. Sampai saat ini belum ada satu mekanisme penyelesaian sengketa yang memadai baik di level nasional maupun internasional. Sehingga yang paling mungkin dilakukan oleh para pihak yang bersengketa saat ini adalah menyelesaikan sengketa tersebut secara konvensional.
Hal ini tentunya menimbulkan pertanyaan mengingat transaksi itu terjadi di dunia maya, tapi mengapa penyelesaiannya di dunia nyata. Apakah tidak mungkin untuk dibuat satu mekanisme pen yelesaian sengketa yang juga bersifat virtual (On-line Dispute Resolution).

2. Domain Name

Domain name dalam Internet secara sederhana dapat diumpamakan seperti nomor telepon atau sebuah alamat. Contoh, domain name untuk Monash University Law School, Australia adalah ”law.monash.edu.au”. Domain name dibaca dari kanan ke kiri yang menunjukkan tingkat spesifikasinya, dari yang paling umum ke yang paling khusus. Untuk contoh di atas, ”au” menunjuk kepada Australia sebagai geographical region, sedangkan ”edu” artinya pendidikan (education) sebagai Top-level Domain name (TLD) yang menjelaskan mengenai tujuan dari institusi tersebut. Elemen seIanjutnya adalah ”monash” yang merupakan ”the Second-Level Domain name” (SLD) yan g dipilih oleh pendaftar domain name, sedangkan elemen yang terakhir ”law” adalah ”subdomain” dari monash Gabungan antara SLD dan TLD dengan berbagai pilihan subdomain disebut ”domain name”.

Domain names diberikan kepada organisasi, perusahaan atau individu oleh InterNIC (the Internet Network Information Centre) berdasark an kontrak dengan the National Science Foundation (Amerika) melalui Network Solutions, Inc. (NSI). Untuk mendaftarkankan sebuah domain name melalui NSI seseorang cukup membuka situs InterNIC dan mengisi sejumlah form InterNIC akan melayani para pendaftar berdasarkan prinsip *”first come first served”*. InterNIC tidak akan memverifikasi mengenai ’hak’ pendaftar untuk memilih satu nama tertentu, tapi pendaftar harus menyetujui ketentuan-ketentuan yang tercantum dalam *”NSI’s domain name dispute resolution policy”*. Berdasarkan ketentuan tersebut, NSI akan menangguhkan pemakaian sebuah domain name yang diklaim oleh salah satu pihak sebagai telah memakai merk dagang yang sudah terkenal.

Peraturan dan Regulasi (perbedaan cyberlaw diberbagai negara)

Cyber Law adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai "online" dan memasuki dunia cyber atau maya. Cyber Law juga didefinisikan sebagai kumpulan peraturan perundang-undangan yang mengatur tentang berbagai aktivitas manusia di cyberspace (dengan memanfaatkan teknologi informasi).

Ruang lingkup dari Cyber Law meliputi hak cipta, merek dagang, fitnah/penistaan, hacking, virus, akses Ilegal, privasi, kewajiban pidana, isu prosedural (Yurisdiksi, Investigasi, Bukti, dll), kontrak elektronik, pornografi, perampokan, perlindungan konsumen dan lain-lain.

Model Regulasi

Pertama, membuat berbagai jenis peraturan perundang-undangan yang sifatnya sangat spesifik yang merujuk pada pola pembagian hukum secara konservatif, misalnya regulasi yang mengatur hanya aspek-aspek perdata saja seperti transaksi elektronik, masalah pembuktian perdata, tanda tangan elektronik, pengakuan dokumen elektronik sebagai alat bukti, ganti rugi perdata, dll., disamping itu juga dibuat regulasi secara spesifik yang secara terpisah mengatur tindak pidana teknologi informasi (cybercrime) dalam undang-undang tersendiri.

Kedua, model regulasi komprehensif yang materi muatannya mencakup tidak hanya aspek perdata, tetapi juga aspek administrasi dan pidana, terkait dengan dilanggarnya ketentuan yang menyangkut penyalahgunaan teknologi informasi dan komunikasi (TIK).

Pada negara yang telah maju dalam penggunaan internet sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju. Sebagai kiblat dari perkembangan aspek hukum ini, Amerika Serikat merupakan negara yang telah memiliki banyak perangkat hukum yang mengatur dan menentukan perkembangan Cyber Law.

1. Cyber Law di Amerika

Di Amerika, Cyber Law yang mengatur transaksi elektronik dikenal dengan Uniform Electronic Transaction Act (UETA). UETA diadopsi oleh National Conference of Commissioners on Uniform State Laws (NCCUSL) pada tahun 1999.

Secara lengkap Cyber Law di Amerika adalah sebagai berikut:

– Electronic Signatures in Global and National Commerce Act
– Uniform Electronic Transaction Act
– Uniform Computer Information Transaction Act
– Government Paperwork Elimination Act
– Electronic Communication Privacy Act
– Privacy Protection Act
– Fair Credit Reporting Act
– Right to Financial Privacy Act
– Computer Fraud and Abuse Act

– Anti-cyber squatting consumer protection Act
– Child online protection Act
– Children's online privacy protection Act
– Economic espionage Act
– "No Electronic Theft" Act

Cyber Law yang mengatur transaksi elektronik dikenal dengan Uniform Electronic Transaction Act (UETA). UETA adalah salah satu dari beberapa Peraturan Perundang-undangan Amerika Serikat yang diusulkan oleh National Conference of Commissioners on Uniform State Laws (NCCUSL). Sejak itu 47 negara bagian, Kolombia, Puerto Rico, dan Pulau Virgin US telah mengadopsinya ke dalam hukum mereka sendiri. Tujuan menyeluruhnya adalah untuk membawa ke jalur hukum negara bagian yag berbeda atas bidang-bidang seperti retensi dokumen kertas, dan keabsahan tanda tangan elektronik sehingga mendukung keabsahan kontrak elektronik sebagai media perjanjian yang layak. UETA 1999 membahas diantaranya mengenai :

Pasal 5 : mengatur penggunaan dokumen elektronik dan tanda tangan elektronik
Pasal 7 : memberikan pengakuan legal untuk dokumen elektronik, tanda tangan elektronik, dan kontrak elektronik.
Pasal 8 : mengatur informasi dan dokumen yang disajikan untuk semua pihak.
Pasal 9 : membahas atribusi dan pengaruh dokumen elektronik dan tanda tangan elektronik.
Pasal 10 : menentukan kondisi-kondisi jika perubahan atau kesalahan dalam dokumen elektronik terjadi dalam transmisi data antara pihak yang bertransaksi.
Pasal 11 : memungkinkan notaris publik dan pejabat lainnya yang berwenang untuk bertindak secara elektronik, secara efektif menghilangkan persyaratan cap/segel.
Pasal 12 : menyatakan bahwa kebutuhan "retensi dokumen" dipenuhi dengan mempertahankan dokumen elektronik.
Pasal 13 : "Dalam penindakan, bukti dari dokumen atau tanda tangan tidak dapat dikecualikan hanya karena dalam bentuk elektronik"
Pasal 14 : mengatur mengenai transaksi otomatis.
Pasal 15 : mendefinisikan waktu dan tempat pengiriman dan penerimaan dokumen elektronik.
Pasal 16 : mengatur mengenai dokumen yang dipindahtangankan.

2. Cyber Law di Singapore

Cyber Law di Singapore, antara lain:

- Electronic Transaction Act
- IPR Act
- Computer Misuse Act
- Broadcasting Authority Act
- Public Entertainment Act
- Banking Act
- Internet Code of Practice
- Evidence Act (Amendment)
- Unfair Contract Terms Act

The Electronic Transactions Act (ETA) 1998

ETA sebagai pengatur otoritas sertifikasi. Singapore mempunyai misi untuk menjadi poros / pusat kegiatan perdagangan elektronik internasional, di mana transaksi perdagangan yang elektronik dari daerah dan di seluruh bumi diproses.

The Electronic Transactions Act telah ditetapkan tgl.10 Juli 1998 untuk menciptakan kerangka yang sah tentang undang-undang untuk transaksi perdagangan elektronik di Singapore yang memungkinkan bagi Menteri Komunikasi Informasi dan Kesenian untuk membuat peraturan mengenai perijinan dan peraturan otoritas sertifikasi di Singapura.

Tujuan dibuatnya ETA :

• Memudahkan komunikasi elektronik atas pertolongan arsip elektronik yang dapat dipercaya;

• Memudahkan perdagangan elektronik, yaitu menghapuskan penghalang perdagangan elektronik yang tidak sah atas penulisan dan persyaratan tandatangan, dan untuk mempromosikan pengembangan dari undang-undang dan infrastruktur bisnis diperlukan untuk menerapkan menjamin / mengamankan perdagangan elektronik;

• Memudahkan penyimpanan secara elektronik tentang dokumen pemerintah dan perusahaan menurut undang-undang, dan untuk mempromosikan penyerahan yang efisien pada kantor pemerintah atas bantuan arsip elektronik yang dapat dipercaya;

• Meminimalkan timbulnya arsip alektronik yang sama (double), perubahan yang tidak disengaja dan disengaja tentang arsip, dan penipuan dalam perdagangan elektronik, dll;

• Membantu menuju keseragaman aturan, peraturan dan mengenai pengesahan dan integritas dari arsip elektronik; dan

• Mempromosikan kepercayaan, integritas dan keandalan dari arsip elektronik dan perdagangan elektronik, dan untuk membantu perkembangan dan pengembangan dari perdagangan elektronik melalui penggunaan tandatangan yang elektronik untuk menjamin keaslian dan integritas surat menyurat yang menggunakan media elektronik.

Pada dasarnya Muatan ETA mencakup, sbb:

• Kontrak Elektronik

Kontrak elektronik ini didasarkan pada hukum dagang online yang dilakukan secara wajar dan cepat serta untuk memastikan bahwa kontrak elektronik memiliki kepastian hukum.

• Kewajiban Penyedia Jasa Jaringan

Mengatur mengenai potensi / kesempatan yang dimiliki oleh network service provider untuk melakukan hal-hal yang tidak diinginkan, seperti mengambil, membawa, menghancurkan material atau informasi pihak ketiga yang menggunakan jasa jaringan tersebut. Pemerintah Singapore merasa perlu untuk mewaspadai hal tersebut.

• Tandatangan dan Arsip elektronik

Bagaimanapun hukum memerlukan arsip/bukti arsip elektronik untuk menangani kasus-kasus elektronik, karena itu tandatangan dan arsip elektronik tersebut harus sah menurut hukum, namun tidak semua hal/bukti dapat berupa arsip elektronik sesuai yang telah ditetapkan oleh Pemerintah Singapore.

Langkah yang diambil oleh Singapore untuk membuat ETA inilah yang mungkin menjadi pendukung majunya bisnis e-commerce di Singapore dan terlihat jelas alasan mengapa di Indonesia bisnis e-

commerce tidak berkembang karena belum adanya suatu kekuatan hukum yang dapat meyakinkan masyarakat bahwa bisnis e-commerce di Indonesia aman seperi di negara Singapore.

3. Cyber Law di Malaysia

komputer sebagai diekstrak dari "penjelasan Pernyataan" dari CCA 1997 :

a) Berusaha untuk membuat suatu pelanggaran hukum bagi setiap orang untuk menyebabkan komputer untuk melakukan apapun fungsi dengan maksud untuk mendapatkan akses tidak sah ke komputer mana materi.

b) Berusaha untuk membuatnya menjadi pelanggaran lebih lanjut jika ada orang yang melakukan pelanggaran sebagaimana dimaksud dalam item (a) dengan maksud untuk melakukan penipuan, ketidakjujuran atau menyebabkan cedera seperti yang didefinisikan dalam KUHP Kode.

c) Berusaha untuk membuat suatu pelanggaran bagi setiap orang untuk menyebabkan modifikasi yang tidak sah dari isi dari komputer manapun.

d) Berusaha untuk menyediakan bagi pelanggaran dan hukuman bagi komunikasi yang salah nomor, kode, sandi atau cara lain untuk akses ke komputer.

e) Berusaha untuk menyediakan untuk pelanggaran-pelanggaran dan hukuman bagi abetments dan upaya dalam komisi pelanggaran sebagaimana dimaksud pada butir (a), (b), (c) dan (d) di atas.

f) Berusaha untuk membuat undang-undang anggapan bahwa setiap orang memiliki hak asuh atau kontrol apa pun program, data atau informasi lain ketika ia tidak diizinkan untuk memilikinya akan dianggap telah memperoleh akses yang tidak sah kecuali jika dibuktikan sebaliknya

Lima cyberlaws telah berlaku pada tahun 1997 tercatat di kronologis ketertiban. Digital Signature Act 1997 merupakan Cyberlaw pertama yang disahkan oleh parlemen Malaysia. Tujuan Cyberlaw ini, adalah untuk memungkinkan perusahaan dan konsumen untuk menggunakan tanda tangan elektronik (bukan tanda tangan tulisan tangan) dalam hukum dan transaksi bisnis. Computer Crimes Act 1997 menyediakan penegakan hukum dengan kerangka hukum yang mencakup akses yang tidak sah dan penggunaan komputer dan informasi dan menyatakan berbagai hukuman untuk pelanggaran yang berbeda komitmen.

Para Cyberlaw berikutnya yang akan berlaku adalah Telemedicine Act 1997. Cyberlaw ini praktisi medis untuk memberdayakan memberikan pelayanan medis / konsultasi dari lokasi jauh melalui menggunakan fasilitas komunikasi elektronik seperti konferensi video. Berikut pada adalah Undang-Undang Komunikasi dan Multimedia 1998 yang mengatur konvergensi komunikasi dan industri multimedia dan untuk mendukung kebijakan nasional ditetapkan untuk tujuan komunikasi dan multimedia industri. The Malaysia Komunikasi dan Undang-Undang Komisi Multimedia 1998 kemudian disahkan oleh parlemen untuk membentuk Malaysia Komisi Komunikasi dan Multimedia yang merupakan peraturan dan badan pengawas untuk mengawasi pembangunan dan hal-hal terkait dengan komunikasi dan industri multimedia.

Departemen Energi, Komunikasi dan Multimedia sedang dalam proses penyusunan baru undang-undang tentang Perlindungan Data Pribadi untuk mengatur pengumpulan, kepemilikan, pengolahan dan penggunaan data pribadi oleh organisasi apapun untuk memberikan perlindungan untuk data

pribadi seseorang dan dengan demikian melindungi hak-hak privasinya. Ini to-be-undang yang berlaku didasarkan pada sembilan prinsip-prinsip perlindungan data yaitu :

- Cara pengumpulan data pribadi
- Tujuan pengumpulan data pribadi
- Penggunaan data pribadi
- Pengungkapan data pribadi
- Akurasi dari data pribadi
- Jangka waktu penyimpanan data pribadi
- Akses ke dan koreksi data pribadi
- Keamanan data pribadi
- Informasi yang tersedia secara umum.

Cyber Law di Malaysia, antara lain:

– Digital Signature Act
– Computer Crimes Act
– Communications and Multimedia Act
– Telemedicine Act
– Copyright Amendment Act
– Personal Data Protection Legislation (Proposed)
– Internal security Act (ISA)
– Films censorship Act

The Computer Crime Act 1997

Sebagai negara pembanding terdekat secara sosiologis, Malaysia sejak tahun 1997 telah mengesahkan dan mengimplementasikan beberapa perundang-undangan yang mengatur berbagai aspek dalam cyberlaw seperti UU Kejahatan Komputer, UU Tandatangan Digital, UU Komunikasi dan Multimedia, juga perlindungan hak cipta dalam internet melalui amandemen UU Hak Ciptanya. Sementara, RUU Perlindungan Data Personal kini masih digodok di parlemen Malaysia.

The Computer Crime Act itu sendiri mencakup mengenai kejahatan yang dilakukan melalui komputer, karena cybercrime yang dimaksud di negara Malaysia tidak hanya mencakup segala aspek kejahatan/pelanggaran yang berhubungan dengan internet. Akses secara tak terotorisasi pada material komputer, adalah termasuk cybercrime. Hal ini berarti, jika saya memiliki komputer dan anda adalah orang yang tidak berhak untuk mengakses komputer saya, karena saya memang tidak mengizinkan anda untuk mengaksesnya, tetapi anda mengakses tanpa seizin saya, maka hal tersebut termasuk cybercrime, walaupun pada kenyataannya komputer saya tidak terhubung dengan internet.

Lebih lanjut, akses yang termasuk pelanggaran tadi (cybercrime) mencakup segala usaha untuk membuat komputer melakukan/menjalankan program (kumpulan instruksi yang membuat komputer untuk melakukan satu atau sejumlah aksi sesuai dengan yang diharapkan pembuat instruksi-instruksi tersebut) atau data dari komputer lainnya (milik pelaku pelanggar) secara aman, tak terotorisasi, juga termasuk membuat komputer korban untuk menjalankan fungsi-fungsi tertentu sesuai dengan waktu yang telah ditentukan oleh pelaku pelanggar tadi.

Hukuman atas pelanggaran The computer Crime Act :

Denda sebesar lima puluh ribu ringgit (RM50,000) dan atau hukuman kurungan/penjara dengan lama waktu tidak melebihi lima tahun sesuai dengan hukum yang berlaku di negara tersebut (Malaysia).

The Computer Crime Act mencakup, sbb:
•Mengakses material komputer tanpa ijin
•Menggunakan komputer untuk fungsi yang lain
•Memasuki program rahasia orang lain melalui komputernya
•Mengubah / menghapus program atau data orang lain
•Menyalahgunakan program / data orang lain demi kepentingan pribadi

4. Cyber Law di Indonesia

Indonesia telah resmi mempunyai undang-undang untuk mengatur orang-orang yang tidak bertanggung jawab dalam dunia maya. Cyber Law-nya Indonesia yaitu undang–undang tentang Informasi dan Transaksi Elektronik (UU ITE).

Di berlakukannya undang-undang ini, membuat oknum-oknum nakal ketakutan karena denda yang diberikan apabila melanggar tidak sedikit kira-kira 1 miliar rupiah karena melanggar pasal 27 ayat 1 tentang muatan yang melanggar kesusilaan. sebenarnya UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) tidak hanya membahas situs porno atau masalah asusila. Total ada 13 Bab dan 54 Pasal yang mengupas secara mendetail bagaimana aturan hidup di dunia maya dan transaksi yang terjadi didalamnya. Sebagian orang menolak adanya undang-undang ini, tapi tidak sedikit yang mendukung undang-undang ini.

Dibandingkan dengan negara-negara di atas, indonesia termasuk negara yang tertinggal dalam hal pengaturan undang-undang ite. Secara garis besar UU ITE mengatur hal-hal sebagai berikut :

•Tanda tangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (tinta basah dan bermaterai). Sesuai dengan e-ASEAN Framework Guidelines (pengakuan tanda tangan digital lintas batas).

• Alat bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHP.
• UU ITE berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar Indonesia yang memiliki akibat hukum di Indonesia.

• Pengaturan Nama domain dan Hak Kekayaan Intelektual.

• Perbuatan yang dilarang (cybercrime) dijelaskan pada Bab VII (pasal 27-37):

o Pasal 27 (Asusila, Perjudian, Penghinaan, Pemerasan)

o Pasal 28 (Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan)

o Pasal 29 (Ancaman Kekerasan dan Menakut-nakuti)

o Pasal 30 (Akses Komputer Pihak Lain Tanpa Izin, Cracking)

o Pasal 31 (Penyadapan, Perubahan, Penghilangan Informasi)

o Pasal 32 (Pemindahan, Perusakan dan Membuka Informasi Rahasia)

o Pasal 33 (Virus?, Membuat Sistem Tidak Bekerja (DOS?))

o Pasal 35 (Menjadikan Seolah Dokumen Otentik (phising?))

5. Cyber Law di Negara lainnya

• Hongkong:
– Electronic Transaction Ordinance
– Anti-Spam Code of Practices
– Code of Practices on the Identity Card Number and Other Personal Identifiers
– Computer information systems internet secrecy administrative regulations
– Personal data (privacy) ordinance
– Control of obscene and indecent article ordinance

• Philipina:
– Electronic Commerce Act
– Cyber Promotion Act
– Anti-Wiretapping Act

• Australia:
– Digital Transaction Act
– Privacy Act
– Crimes Act
– Broadcasting Services Amendment (online services) Ac

• UK:
– Computer Misuse Act
– Defamation Act
– Unfair contract terms Act
– IPR (Trademarks, Copyright, Design and Patents Act)

• South Korea:
– Act on the protection of personal information managed by public agencies
– Communications privacy act
– Electronic commerce basic law
– Electronic communications business law
– Law on computer network expansion and use promotion
– Law on trade administration automation
– Law on use and protection of credit card
– Telecommunication security protection act
– National security law

• Jepang:
– Act for the protection of computer processed personal data held by administrative organs
– Certification authority guidelines
– Code of ethics of the information processing society
– General ethical guidelines for running online services
– Guidelines concerning the protection of computer processed personal data in the private sector
– Guidelines for protecting personal data in electronic network management
– Recommended etiquette for online service users
– Guidelines for transactions between virtual merchants and consumers

6. Cyber Law di beberapa negara khususnya yang berhubungan dengan e-commerce antara lain:

1. Perlindungan hukum terhadap konsumen.
• Indonesia
UU ITE menerangkan bahwa konsumen berhak untuk mendapatkan informasi yang lengkap berkaitan dengan detail produk, produsen dan syarat kontrak.

• Malaysia
Communications and Multimedia Act 1998 menyebutkan bahwa setiap penyedia jasa layanan harus menerima dan menanggapi keluhan konsumen.

• Filipina
Electronic Commerce Act 2000 dan Consumer Act 1991 menyebutkan bahwa siapa saja yang menggunakan transaksi secara elektronik tunduk terhadap hukum yang berlaku.

2. Perlindungan terhadap data pribadi serta privasi.

• Singapura
Sebagai pelopor negara ASEAN yang memberlakukan cyberlaw yang mengatur e-commerce code untuk melindungi data pribadi dan komunikasi konsumen dalam perniagaan di internet.

• Indonesia
Sudah diatur dalam UU ITE.

• Malaysia & Thailand
Masih berupa rancangan.

3. Cybercrime
Sampai dengan saat ini ada delapan negara ASEAN yang telah memiliki Cyber Law yang mengatur tentang cybercrime atau kejahatan di internet yaitu Brunei, Malaysia, Myanmar, Filipina, Singapura, Thailand, Vietnam dan termasuk Indonesia melalui UU ITE yang disahkan Maret 2008 lalu.
4. Spam

Spam dapat diartikan sebagai pengiriman informasi atau iklan suatu produk yang tidak pada tempatnya dan hal ini sangat mengganggu.
• Singapura
Merupakan satu-satunya negara di ASEAN yang memberlakukan hukum secara tegas terhadap spammers (Spam Control Act 2007).

• Malaysia & Thailand
Masih berupa rancangan.

• Indonesia
UU ITE belum menyinggung masalah spam.

5. Peraturan Materi Online / Muatan dalam suatu situs

Lima negara ASEAN yaitu Brunei, Malaysia, Myanmar, Singapura serta Indonesia telah menetapkan cyberlaw yang mengatur pemuatan materi online yang mengontrol publikasi online berdasarkan norma sosial, politik, moral, dan keagamaan yang berlaku di negara masing-masing.

6. Hak Cipta Intelektual atau Digital Copyright

Di ASEAN saat ini ada enam negara yaitu Brunei, Kamboja, Indonesia, Filipina, Malaysia dan Singapura yang telah mengatur regulasi tentang hak cipta intelektual.
Sementara negara lainnya masih berupa rancangan.

7. Penggunaan Nama Domain

Saat ini ada lima negara yaitu Brunei, Kamboja, Malayasia, Vietnam termasuk Indonesia yang telah memiliki hukum yang mengatur penggunaan nama domain. Detail aturan dalam setiap negara berbeda-beda dan hanya Kamboja yang secara khusus menetapkan aturan tentang penggunaan nama domain dalam Regulation on Registration of Domain Names for Internet under the Top Level 'kh' 1999.

8. Electronic Contracting

Saat ini hampir semua negara ASEAN telah memiliki regulasi mengenai Electronic contracting dan tanda tangan elektronik atau electronik signatures termasuk Indonesia melalui UU ITE.
Sementara Laos dan Kamboja masih berupa rancangan.
ASEAN sendiri memberi deadline Desember 2009 sebagai batas waktu bagi setiap negara untuk memfasilitasi penggunaan kontrak elektronik dan tanda tangan elektonik untuk mengembangkan perniagaan intenet atau e-commerce di ASEAN.

9. Online Dispute resolution (ODR)

ODR adalah resolusi yang mengatur perselisihan di internet.
• Filipina
Merupakan satu-satunya negara ASEAN yang telah memiliki aturan tersebut dengan adanya Philippines Multi Door Courthouse.
• Singapura
Mulai mendirikan ODR facilities.
• Thailand
Masih dalam bentuk rancangan.
• Malaysia
Masih dalam tahap rancangan mendirikan International Cybercourt of Justice.
• Indonesia

Dalam UU ITE belum ada aturan yang khusus mengatur mengenai perselisihan di internet. Sementara di negara ASEAN lainnya masih belum ada. ODR sangat penting menyangkut implementasinya dalam perkembangan teknologi informasi dan e-commerce.

7. Council of Europe Convention on Cyber crime (Eropa)

Saat ini berbagai upaya telah dipersiapkan untuk memerangi cybercrime. The Organization for Economic Co-operation and Development (OECD) telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan computer-related crime, di mana pada tahun 1986 OECD telah mempublikasikan laporannya yang berjudul Computer-Related Crime: Analysis of Legal Policy. Laporan ini berisi hasil survey terhadap peraturan perundang-undangan Negara-negara Anggota beserta rekomendasi perubahannya dalam menanggulangi computer-related crime tersebut, yang mana diakui bahwa sistem telekomunikasi juga memiliki peran penting dalam kejahatan tersebut.

Melengkapi laporan OECD, The Council of Europe (CE) berinisiatif melakukan studi mengenai kejahatan tersebut. Studi ini memberikan guidelines lanjutan bagi para pengambil kebijakan untuk menentukan tindakan-tindakan apa yang seharusnya dilarang berdasarkan hukum pidana Negara-negara Anggota, dengan tetap memperhatikan keseimbangan antara hak-hak sipil warga negara dan kebutuhan untuk melakukan proteksi terhadap computer-related crime tersebut. Pada perkembangannya, CE membentuk Committee of Experts on Crime in Cyberspace of the Committee

on Crime Problems, yang pada tanggal 25 April 2000 telah mempublikasikan Draft Convention on Cyber-crime sebagai hasil kerjanya (http://www.cybercrimes.net), yang menurut Prof.

Susan Brenner (brenner@cybercrimes.net) dari University of Daytona School of Law, merupakan perjanjian internasional pertama yang mengatur hukum pidana dan aspek proseduralnya untuk berbagai tipe tindak pidana yang berkaitan erat dengan penggunaan komputer, jaringan atau data, serta berbagai penyalahgunaan sejenis.

Dari berbagai upaya yang dilakukan tersebut, telah jelas bahwa cybercrime membutuhkan global action dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah:

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut
2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime
4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi

Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties