Cyberlaw

Pengertian cyberlaw

Cyberlaw adalah Aspek hukum yang istilahnya berasal dari cyberspace law yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki cyberspace atau dunia maya.

Berikut merupakan beberapa istilah yang dimaksudkan sebagai terjemahan dari ”cyber law”, misalnya, Hukum Sistem Informasi, Hukum Informasi, dan Hukum Telematika (Telekomunikasi dan Informatika).

Menurut Girasa (2002) mendefinisikan Cybercrime sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama.Menurut Tavani (2000) memberikan definisi Cybercrime yang lebih menarik, yaitu kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi cyber dan terjadi di dunia cyber.

Cyberlaw merupakan salah satu solusi dalam menangani kejahatan di dunia maya yang demikian meningkat jumlahnya.Cyberlaw bukan saja keharusan, melainkan sudah merupakan suatu kebutuhan untuk menghadapi kenyataan yang ada sekarang ini, yaitu banyaknya berlangsung kegiatan cybercrime.Tetapi Cyberlaw tidak akan terlaksana dengan baik tanpa didukung oleh Sumber Daya Manusia yang berkualitas dan ahli dalam bidangnya. Tingkat kerugian yang ditimbulkan dari adanya kejahatan dunia maya ini sangatlah besar dan tidak dapat dinilai secara pasti berapa tingkat kerugiannya.

Tetapi perkembangan cyberlaw di Indonesia ini belum bisa dikatakan maju. Oleh karena itu, pada tanggal 25 Maret 2008 Dewan Perwakilan Rakyat (DPR) mengesahkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE ini mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya, baik transaksi maupun pemanfaatan informasinya. Sejak dikeluarkannya UU ITE ini, maka segala aktivitas didalamnya diatur dalam undang-undang tersebut. Cyberlaw ini sudah terlebih dahulu diterapkan di Negara seperti Amerika Serikat, Eropa,Indonesia, Australia, dan lain sebagainya.

Ruang lingkup cyberlaw

Pembahasan mengenai ruang lingkup ”cyber law” dimaksudkan sebagai inventarisasi atas persoalan-persoalan atau aspek-aspek hukum yang diperkirakan berkaitan dengan pemanfaatan Internet.

Menurut Jonathan Rosenoer dalam Cyber Law – The Law Of Internet (BSI pert 5, 2013:6) menyebutkan ruang lingkup cyber law adalah

1. Copy Right (Hak Cipta)
2. Trademark (Hak Merk)
3. Defamation (Pencemaran Nama Baik)

4. Hate Speech (Fitnah, Penghinaan,Penistaan)
5. Hacking, Viruses, Illegal Access (Serangan terhadap fasilitas computer)
6. Regulation Internet Resource
7. Privacy
8. Duty Care (Prinsip Kehati-hatian)
9. Criminal Liability
10. Procedural Issues (yuridiksi, pembuktian, penyelidikan dll)
11. Electronic Contract (kontrak elektronik dan di tanda tangan digital)
12. Pornography
13. Robbery (Pencurian)
14. Consumer Protection (Perlindungan konsumen)
15. E-Commerce, E- Government

1. Copy Right (Hak Cipta)

Hak Cipta adalah hak khusus bagi pencipta maupun penerima hak untuk mengumumkan atau memperbanyak ciptaannya maupun memberi izin untuk itu dengan tidak mengurangi pembatasan-pembatasan menurut peraturan perundang-undangan yang berlaku.

2. Trademark (Hak Merk)

Berdasarkan Pasal 1 Undang-Undang Nomor 15 Tahun 2001 tentang Merek, merek adalah tanda yang berupa gambar, nama, kata, huruf-huruf, angka-angka, susunan warna, atau kombinasi dari unsur-unsur tersebut yang memiliki daya pembeda dan digunakan dalam kegiatan perdagangan barang atau jasa.

Hak atas merek adalah hak eksklusif yang diberikan oleh Negara kepada pemilik merek yang terdaftar dalam daftar umum merek untuk jangka waktu tertentu dengan menggunakan sendiri merek atau memberikan izin kepada pihak lain untuk menggunakannya.

3. Defamation (Pencemaran Nama Baik)

Defamation diartikan sebagi pencemaran nama baik dan bisa juga dengan istilah slander (lisan), libel (tertulis) yang dalam Bahasa Indonesia (Indonesian translation) diterjemahkan menjadi pencemaran nama baik, fitnah (lisan), fitnah (tertulis). Slander adalah oral defamation (fitnah secara lisan) sedangkan Libel adalah written defamation (fitnah secara tertulis). Dalam bahasa Indonesia belum ada istilah untuk membedakan antara slander dan libel. Penghinaan atau defamation secara harfiah diartikan sebagai sebuah tindakan yang merugikan nama baik dan kehormatan seseorang.

4. Hate Speech (Fitnah, Penghinaan,Penistaan)

Hate Speech dalam arti hukum, Hate speech adalah perkataan, perilaku, tulisan, ataupun pertunjukan yang dilarang karena dapat memicu terjadinya tindakan kekerasan dan sikap prasangka entah dari pihak pelaku pernyataan tersebut ataupun korban dari tindakan tersebut.

5. Hacking, Viruses, Illegal Access (Serangan terhadap fasilitas computer)

Hacking adalah suatu aktifitas dari hacker yaitu orang yang tertarik dan mendalami sistem operasi komputer sehingga mengetahui kelemahan yang ada pada suatu sistem tetapi tidak memanfaatkan

kelemahan suatu sistem atau situs kemudian dengan kemampuannya itu kelemahan tersebut untuk hal kejahatan.

Virus adalah program yang dibuat oleh seorang programmer yang bersifat mengganggu dan merusak proses-proses yang dikerjakan komputer. Virus menginfeksi file dengan eksetensi tertentu. Misalnya exe, txt, jpg dan lain sebagainya.

Illegal access merupakan kejahatan dunia maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer. Illegal access terjadi ketika seseorang memasuki atau menyusup kedalam suatu system jaringan komputer dengan tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain.

7. Privacy

Kerahasiaan pribadi (Bahasa Inggris: privacy) adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka. Privasi kadang dihubungkan dengan anonimitas walaupun anonimitas terutama lebih dihargai oleh orang yang dikenal publik. Privasi dapat dianggap sebagai suatu aspek dari keamanan.

8. Duty Care (Prinsip Kehati-hatian)

Duty Care adalah Dimana seseorang atau suatu instansi harus berhati-hati dalam menggunakan media internet. karena media internet sangat banyak sekali cybercrime sehingga duty care (prinsip kehati-hatian) itu sangat diperlukan.

Sumber

http://www.academia.edu/8572146/CYBER_LAW_dan_UNDANG-UNDANG_ITE