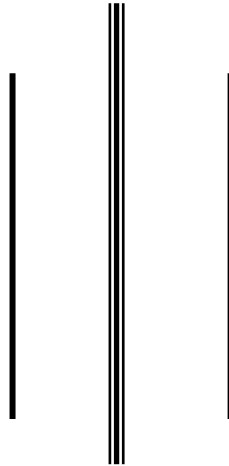


PERATURAN DAN REGULASI CYBER LAW



Di Susunoleh :

ARIF NURROHIM / 41113328

JOSAFATINO MORGANI / 44113683

MUHAMMAD NURSAIFUL A / 46113056



TEKNIK KOMPUTER (D3)

UNIVERSITAS GUNADARMA

2015

DAFTAR ISI

COVER	1
DAFTAR ISI	2
KATA PENGANTAR	3
Peraturan dan regulasi	4
Cyber Law	1
Cyberlaw di Indonesia	5
Tentang UU ITE	6
Computer crime act THAILAND	7
Computer Crime Act Malaysia	9
Council of Europe Convention on Cybercrime (COECCC)	10
DAFTAR PUSTAKA	12

KATA PENGANTAR

Puji syukur saya panjatkan kehadiran Tuhan Yang Maha Esa yang telah memberikan Rahmat serta karunia-Nya kepada saya. Sehingga saya dapat menyelesaikan penulisan makalah ini yang dengan tepat pada waktunya. Yang dimana penulisan ini bernama “PERATURAN dan REGULASI CYBER LAW di BERBAGAI NEGARA”.

Penulisan makalah ini berisikan tentang bagaimana cara suatu negara membuat peraturan tentang kejahatan yang tidak terlihat secara fisik melainkan melalui dunia maya, serta pasal-pasal yang mengatur tentang hukuman apabila melakukan kejahatan di dunia maya.

Diharapkan penulisan makalah ini dapat memberikan informasi kepada kita semua tentang hal-hal yang tidak boleh dilakukan di dunia maya (bersifat kejahatan). Saya menyadari bahwa penulisan makalah ini masih jauh dari sempurna, oleh karena itu kritik dan saran dari semua pihak yang bersifat membangun selalu saya harapkan demi kesempurnaan penulisan makalah ini.

Akhir kata, saya sampaikan terima kasih kepada semua pihak yang telah berperan serta dalam penyusunan makalah ini dari awal sampai akhir. Semoga Tuhan senantiasa melindungi kita semua dari segala usaha kita. Amin.

Bekasi, 10 November 2015

Peraturan dan regulasi

Cyber Law

Peraturan adalah sesuatu yang disepakati dan mengikat sekelompok orang/ lembaga dalam rangka mencapai suatu tujuan dalam hidup bersama. Regulasi adalah “mengendalikan perilaku manusia atau masyarakat dengan aturan atau pembatasan.” Regulasi dapat dilakukan dengan berbagai bentuk, misalnya: pembatasan hukum diumumkan oleh otoritas pemerintah, regulasi pengaturan diri oleh suatu industri seperti melalui asosiasi perdagangan, Regulasi social (misalnya norma), co-regulasi dan pasar. Seseorang dapat, mempertimbangkan regulasi dalam tindakan perilaku misalnya menjatuhkan sanksi (seperti denda). Setelah memahami definisi di atas, mari kita masuk ke pembahasannya.

Perbandingan Cyber Law Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya), yang umumnya diasosiasikan dengan internet. Cyberlaw dibutuhkan karena dasar atau fondasi dari hukum di banyak negara adalah “ruang dan waktu”. Sementara itu, internet dan jaringan komputer mendobrak batas ruang dan waktu ini. Semakin banyak munculnya kasus “CyberCrime” di Indonesia, seperti pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Maka dibuatlah sebuah regulasi konten, yaitu :

- Keamanan nasional : instruksi pada pembuatan bom, produksi obat/racun tidak sah, aktivitas teroris.
- Protection of minors (Perlindungan pelengkap) : abusive forms of marketing, violence, pornography
- Protection of human dignity(Perlindungan martabat manusia) : hasutan kebencian rasial, diskriminasi rasial.
- Keamanan ekonomi : penipuan, instructions on pirating credit cards, scam, cybercrime.
- Keamanan informasi : Cybercrime, Phising
- Protection of Privacy
- Protection of Reputation
- Intellectual Property

Perlunya Peraturan dalam Cyberlaw

Sebagai orang yang sering memanfaatkan internet untuk keperluan sehari-hari sebaiknya kita membaca undang-undang transaksi elektronik yang telah disahkan pada tahun 2008. Undang-undang tersebut dapat didownload dari website www.ri.go.id dan dapat langsung membaca bab VII yang mengatur tentang tindakan yang dilarang. Permasalahan yang sering muncul adalah bagaimana menjerang berbagai kejahatan komputer dikaitkan dengan ketentuan pidana yang berlaku karena ketentuan pidana yang mengatur tentang kejahatan komputer yang berlaku saat ini masih belum lengkap. Hingga saat ini, di negara kita ternyata belum ada pasal yang bisa digunakan untuk menjerat penjahat cybercrime. Untuk kasus carding misalnya, kepolisian baru bisa menjerat pelaku kejahatan komputer dengan pasal 363 soal pencurian karena yang dilakukan tersangka memang mencuri data kartu kredit orang lain.

Cyberlaw di Indonesia

Undang-undang informasi dan transaksi elektronik (UU ITE) atau yang disebut cyberlaw, digunakan untuk mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya, baik transaksi maupun pemanfaatan informasinya. Pada UU ITE ini juga diatur berbagai macam hukuman bagi kejahatan melalui internet. UU ITE mengakomodir kebutuhan para pelaku bisnis diinternet dan masyarakat pada umumnya untuk mendapat kepastian hukum dengan diakuinya bukti elektronik dan tanda tangan elektronik digital sebagai bukti yang sah dipengadilan. UU ITE sendiri baru ada diIndonesia dan telah disahkan oleh DPR pada tanggal 25 Maret 2008. UU ITE terdiri dari 13 Bab dan 54 Pasal yang mengupas secara mendetail bagaimana aturan hidup di dunia maya dan transaksi yang terjadi didalamnya. Perbuatan yang dilarang (cybercrime) dijelaskan pada Bab VII (pasal 27-37),

yaitu:

Pasal 27: Asusila, Perjudian, Penghinaan, Pemerasan.

Pasal 28: Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan.

Pasal 29: Ancaman Kekerasan dan Menakut-nakuti.

Pasal 30: Akses Komputer Pihak Lain Tanpa Izin, Cracking.

Pasal 31: Penyadapan, Perubahan, Penghilangan Informasi.

Tentang UU ITE

UU ITE (Undang-undang Informasi dan Transaksi Elektronik)adalah ketentuan yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia UU ITE mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya, baik transaksi maupun pemanfaatan informasinya. Pada UU ITE ini juga diatur berbagai ancaman hukuman bagi kejahatan melalui internet. UU ITE mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat pada umumnya guna mendapatkan kepastian hukum, dengan diakuinya bukti elektronik dan tanda tangan digital sebagai bukti yang sah di pengadilan. Penyusunan materi UUIITE tidak terlepas dari dua naskah akademis yang disusun oleh dua institusi pendidikan yakni Unpad dan UI.Tim Unpad ditunjuk oleh Departemen Komunikasi dan Informasi sedangkan Tim UI oleh Departemen Perindustrian dan Perdagangan. Pada penyusunannya, Tim Unpad bekerjasama dengan para pakar di ITB yang kemudian menamai naskah akademisnya dengan RUU Pemanfaatan Teknologi Informasi (RUU PTI). Sedangkan Tim UI menamai naskah akademisnya dengan RUU Transaksi Elektronik. Kedua naskah akademis tersebut pada akhirnya digabung dan disesuaikan kembali oleh Tim yang dipimpin Prof. Ahmad M Ramli SH (atas nama pemerintah), sehingga namanya menjadi Undang-Undang Informasi dan Transaksi Elektronik sebagaimana disahkan oleh DPR. Keterbatasan UU Telekomunikasi dalam Mengatur Penggunaan Teknologi Informasi Salah satu UU yang berhubungan dengan pengaturan penggunaan teknologi informasi yaitu UU NO.36. Isi dari UU No.36 adalah apa arti dari telekomunikasi, asas dan tujuan dari telekomunikasi, penyelenggaraan, perizinan, pengamanan, sangsi administrasi dan ketentuan pidana dari penggunaan telekomunikasi, yang dimana semua ketentuan itu telah di setujui oleh DPR RI. Pada UU No.36 tentang telekomunikasi mempunyai salah satu tujuan yang berisikan upaya untuk memperkuat persatuan dan kesatuan bangsa, memperlancar kegiatan pemerintah, mendukung terciptanya tujuan pemerataan pembangunan dan hasil-hasilnya serta meningkatkan hubungan antar bangsa.Dalam pembuatan UU ini dibuat karena ada beberapa alasan,salah satunya

adalah bahwa pengaruh globalisasi dan perkembangan teknologi telekomunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi dan untuk menjaga keamanan bagi para pengguna teknologi informasi. Teknologi informasi sangatlah berpengaruh besar untuk negara kita, di lihat dari segi kebudayaan, kita bisa memperkenalkan budaya – budaya yang kita miliki dengan bebas kepada negara-negara luar untuk menarik minat para turis asing. Kalau dilihat dari segi bisnis keuntungannya adalah kita dengan bebas dan leluasa memasarkan bisnis yang kita jalankan dengan waktu yang singkat. Jadi menurut saya UU ini belum sepenuhnya dapat mengatur penggunaan teknologi informasi karena kebebasan yang dimiliki dari setiap individu yang tidak bisa dikontrol dan juga tidak bisa dilihat dari segi negatifnya saja banyak juga segi positif dari penggunaan teknologi informasi seperti dapatnya memperkenalkan kebudayaan kita kepada negara-negara luar untuk menarik minat para turis asing.

Pasal 32: Pemindahan, Perusakan dan Membuka Informasi Rahasia.

Pasal 33: Virus, Membuat Sistem Tidak Bekerja (DOS).

Pasal 35: Menjadikan Seolah Dokumen Otentik (phising).

Pelanggaran UU ITE ini akan dikenakan denda 1 Milliar rupiah. Di Indonesia, masalah tentang perlindungan konsumen, privasi, cybercrime, muatan online, digital copyright, penggunaan nama domain dan kontrak elektronik sudah ditetapkan oleh pemerintah Indonesia. Namun, masalah spam dan online dispute resolution belum mendapat tanggapan dari pemerintah sehingga belum ada rancangannya.

Computer crime act THAILAND

Cybercrime dan kontrak elektronik di Negara Thailand sudah ditetapkan oleh pemerintahnya, walaupun yang sudah ditetapkannya hanya 2 tetapi yang lainnya seperti privasi, spam, digital copyright dan ODR sudah dalam tahap rancangan. Cyberlaw di Amerika Serikat Di Amerika, 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 yang 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. Undang-Undang Lainnya :

- Electronic Signatures in Global and National Commerce 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 Undang-Undang Khusus :
- Computer Fraud and Abuse Act (CFAA)
- Credit Card Fraud Act
- Electronic Communication Privacy Act (ECPA)

- Digital Performance Right in Sound Recording Act
- Electronic Fund Transfer Act
- Uniform Commercial Code Governance of Electronic Funds Transfer
- Federal Cable Communication Policy
- Video Privacy Protection Act Undang-Undang Sisipan :
 - Arms Export Control Act
 - Copyright Act, 1909, 1976
 - Code of Federal Regulations of Indecent Telephone Message Services
 - Privacy Act of 1974
 - Statute of Frauds
 - Federal Trade Commission Act
 - Uniform Deceptive Trade Practices Act

Kesimpulan Dalam hal ini Thailand masih lebih baik dari pada Negara Vietnam karena Negara Vietnam hanya mempunyai 3 cyberlaw sedangkan yang lainnya belum ada bahkan belum ada rancangannya. Kesimpulan dari 5 negara yang dibandingkan adalah Negara yang memiliki cyberlaw paling banyak untuk saat ini adalah Indonesia, tetapi yang memiliki cyberlaw yang terlengkap nantinya adalah Malaysia karena walaupun untuk saat ini baru ada 6 hukum tetapi yang lainnya sudah dalam tahap perencanaan sedangkan Indonesia yang lainnya belum ada tahap perencanaan. Untuk Thailand dan Vietnam, Vietnam masih lebih unggul dalam penanganan cyberlaw karena untuk saat ini saja terdapat 3 hukum yang sudah ditetapkan tetapi di Thailand saat ini baru terdapat 2 hukum yang ditetapkan tetapi untuk kedepannya Thailand memiliki 4 hukum yang saat ini sedang dirancang.

Computer Crime Act Malaysia

Computer Crime Act (Akta Kejahatan Komputer) merupakan Cyber Law (Undang-Undang) yang digunakan untuk memberikan dan mengatur bentuk pelanggaran-pelanggaran yang berkaitan dengan penyalahgunaan komputer. Computer Crime Act (Akta Kejahatan Komputer) yang dikeluarkan oleh Malaysia adalah peraturan Undang-Undang (UU) TI yang sudah dimiliki dan dikeluarkan negara Jiran Malaysia sejak tahun 1997 bersamaan dengan

dikeluarkannya Digital Signature Act 1997 (Akta Tandatangan Digital), serta Communication and Multimedia Act 1998 (Akta Komunikasi dan Multimedia). Di Malaysia, sesuai akta kesepakatan tentang kejahatan komputer yang dibuat tahun 1997, proses komunikasi yang termasuk kategori Cyber Crime adalah komunikasi secara langsung ataupun tidak langsung dengan menggunakan suatu kode atau password atau sejenisnya untuk mengakses komputer yang memungkinkan penyalahgunaan komputer pada proses komunikasi terjadi.

Council of Europe Convention on Cybercrime (COECCC)

Merupakan salah satu contoh organisasi internasional yang bertujuan untuk melindungi masyarakat dari kejahatan di dunia maya, dengan mengadopsikan aturan yang tepat dan untuk meningkatkan kerja sama internasional dalam mewujudkan hal ini.

COECCC telah diselenggarakan pada tanggal 23 November 2001 di kota Budapest, Hongaria. Konvensi ini telah menyepakati bahwa Convention on Cybercrime dimasukkan dalam European Treaty Series dengan nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal lima Negara, termasuk paling tidak ratifikasi yang dilakukan oleh tiga Negara anggota Council of Europe. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan criminal yang bertujuan untuk melindungi masyarakat dari cybercrime, baik melalui undang-undang maupun kerja sama internasional. Konvensi ini dibentuk dengan pertimbangan-pertimbangan antara lain sebagai berikut:

Bahwa masyarakat internasional menyadari perlunya kerjasama antar Negara dan Industri dalam memerangi kejahatan cyber dan adanya kebutuhan untuk melindungi kepentingan yang sah dalam penggunaan dan pengembangan teknologi informasi.

Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Hal lain yang diperlukan adalah adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.

Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik Dan sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi/pendapat.

Konvensi ini telah disepakati oleh masyarakat Uni Eropa sebagai konvensi yang terbuka untuk diakses oleh Negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrument Hukum Internasional dalam mengatasi kejahatan cyber, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi.

DAFTAR PUSTAKA

- <http://sitihalimahfight.blogspot.co.id/2015/05/peraturan-regulasi-cyberlaw-berbagai.html>
- <https://furqonubd.wordpress.com/2015/10/28/peraturan-dan-regulasi-it/>