



**SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI**

ETIKA PROFESI

Krisna Panji, S.Kom | panji@nurulfikri.ac.id | 0857-1414-1089

TEKNIK INFORMATIKA | SISTEM INFORMASI



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

PERTEMUAN KE 12

CYBERLAW



PEMBAHASAN

1. Pengertian Cyberlaw
2. Tindakan-tindakan terhadap Cyberlaw
3. Undang-undang Cyberlaw Indonesia



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Cyber Law dalam arti Luas

- ✓ Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik
- ✓ Artinya semua tindak pidana konvensional dalam Kitab Undang-undang Hukum Pidana (“KUHP”) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas
- ✓ Demikian juga tindak pidana dalam Undang-undang Nomer 3 Tahun 2011 tentang Transfer Dana maupun tindak pidana perbankan serta tindak pidana pencucian uang



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Cyber Law dalam arti Sempit

Dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU ITE”) UU ITE juga memberikan definisi mengenai cybercrimes, melalui beberapa pengelompokan yang mengacu pada Convention on Cybercrimes (Sitompul, 2012), meliputi:



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

ASAS-ASAS CYBERLAW

- • **Subjective territoriality**, yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.
- **Objective territoriality**, yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
- **Nationality** yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.
- **Passive nationality** yang menekankan yurisdiksi berdasarkan kewarganegaraan korban.
- **Protective principle** yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah,
- **Universality**. Asas ini selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus cyber. Asas ini disebut juga sebagai “universal interest jurisdiction”.

Pengelompokan Tindak Pidana Cyber (UU ITE)

1. Tindak pidana yang berhubungan dengan aktivitas illegal

a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari:

- Kesusilaan (Pasal 27 ayat [1] UU ITE);
- Perjudian (Pasal 27 ayat [2] UU ITE);
- Penghinaan atau pencemaran nama baik (Pasal 27 ayat [3] UU ITE);
- Pemerasan atau pengancaman (Pasal 27 ayat [4] UU ITE);



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Sanksi Pelanggaran (Pasal 45 ayat 1):

Hukum Pasal 27 ayat 1, 2, 3, 4 : Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp ,1.000.000.000,- (satu miliar rupiah)

PENGELOMPOKAN TINDAK PIDANA CYBER (UU ITE)

- a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal (lanjut)
- Berita bohong yang menyesatkan dan merugikan konsumen(**Pasal 28 ayat [1] UU ITE**);
 - Menimbulkan rasa kebencian berdasarkan SARA (**Pasal 28 ayat [2] UU ITE**);
 - Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (**Pasal 29 UU ITE**);



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- ❖ Hukuman pada Pasal 28: Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1000.000.000. (satu miliar rupiah).
- ❖ Hukuman pada Pasal 29: Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah)



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Pengelompokan Tindak Pidana Cyber (UU ITE)

- b. Dengan cara apapun melakukan akses ilegal (**Pasal 30 UU ITE**);
- c. Intersepsi ilegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (**Pasal 31 UU ITE**);

PENGELOMPOKAN TINDAK PIDANA CYBER (UU ITE)

2. Tindakpidana yang berhubungan dengan gangguan (interferensi)
 - a. Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* – **Pasal 32 UU ITE**);
 - b. Gangguan terhadap Sistem Elektronik (*system interference* – **Pasal 33 UU**)

PENGELOMPOKAN TINDAK PIDANA CYBER (UU ITE)

3. Tindak pidana memfasilitasi perbuatan yang dilarang (**Pasal 34 UU ITE**)
4. Tindak pidana pemalsuan informasi atau dokumen elektronik (**Pasal 35 UU ITE**)



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

CYBERLAW

Cyber Law adalah aspek hukum 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 dunia maya. Cyber Law sendiri merupakan istilah yang berasal dari Cyberspace Law.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Jonathan Rosenoer dalam Cyber law, the law of internet mengingatkan tentang ruang lingkup

dari cyber law diantaranya :

- ✓ Hak Cipta (Copy Right)
- ✓ Hak Merk (Trademark)
- ✓ Pencemaran nama baik (Defamation)
- ✓ Fitnah, Penistaan, Penghinaan (Hate Speech)
- ✓ Serangan terhadap fasilitas komputer (Hacking, Viruses, Illegal Access)
- ✓ Pengaturan sumber daya internet seperti IP-Address, domain name
- ✓ Kenyamanan Individu (Privacy)



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Ruang Lingkup Cyber Law (Cont)

- ☐ Prinsip kehati-hatian (Duty care)
- ☐ Tindakan kriminal biasa yang menggunakan TI sebagai alat
- ☐ Isu prosedural seperti yuridiksi, pembuktian, penyelidikan dll
- ☐ Kontrak / transaksi elektronik dan tanda tangan digital
- ☐ Pornografi
- ☐ Pencurian melalui Internet
- ☐ Perlindungan Konsumen
- ☐ Pemanfaatan internet dalam aktivitas keseharian seperti e-commerce, e-government, e-education dll



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Perangkat Hukum Cyber Law

Agar pembentukan perangkat perundangan tentang teknologi informasi mampu mengarahkan segala aktivitas dan transaksi didunia cyber sesuai dengan standar etik dan hukum yang disepakati maka proses pembuatannya diupayakan sebagai berikut:

❑ Menetapkan prinsip – prinsip dan pengembangan teknologi informasi antara lain :

1. Melibatkan unsur yang terkait (pemerintah, swasta, profesional).
2. Menggunakan pendekatan moderat untuk mensintesis prinsip hukum konvensional dan norma hukum baru yang akan terbentuk
3. Memperhatikan keunikan dari dunia maya



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Perangkat Hukum Cyber Law (Cont)

4. Mendorong adanya kerjasama internasional mengingat sifat internet yang global
5. Menempatkan sektor swasta sebagai leader dalam persoalan yang menyangkut industri dan perdagangan.
6. Pemerintah harus mengambil peran dan tanggung jawab yang jelas untuk persoalan yang menyangkut kepentingan public
7. Aturan hukum yang akan dibentuk tidak bersifat restriktif melainkan harus direktif dan futuristik



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Perangkat Hukum Cyber Law (Cont)

- ❑ Melakukan pengkajian terhadap perundangan nasional yang memiliki kaitan langsung maupun tidak langsung dengan munculnya persoalan hukum akibat transaksi di internet seperti : UU hak cipta, UU merk, UU perlindungan konsumen, UU Penyiaran dan Telekomunikasi, UU Perseroan Terbatas, UU Penanaman Modal Asing, UU Perpajakan, Hukum Kontrak, Hukum Pidana dll.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Perangkat Hukum Internasional

Dalam rangka upaya menanggulangi cyber crime Resolusi Kongres PBB VII/1990 mengenai “Computer related crime” mengajukan beberapa kebijakan antara lain :

1. Menghimbau negara anggota untuk mengintensifkan upaya – upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah – langkah berikut :
 - a. Melakukan moderinasi hukum pidana material dan hukum acara pidana.
 - b. Mengembangkan tindakan pencegahan dan pengamanan komputer.
 - c. Melakukan langkah untuk membuat peka warga masyarakat, aparat terhadap pentingnya pencegahan kejahatan.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- d. Melakukan training bagi para hakim, pejabat dan aparat hukum tentang cyber crime.
- e. Memperluas rules of ethics dalam penggunaan komputer melalui kurikulum informasi,
- f. Mengadopsi kebijakan perlindungan korban cyber crime sesuai deklarasi PBB.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

2. Menghimbau negara anggota meningkatkan upaya Penanggulangan cyber crime
3. Merekomendasikan kepada komite pengendalian dan pencegahan kejahatan PBB (Committee on Crime Prevention and Control) untuk :
Menyebarkan pedoman dan standar untuk membantu negara anggota menghadapi cyber crime, mengembangkan penelitian dan analisis untuk menemukan cara baru menghadapi cyber crime dimasa datang.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Kebijakan IT di Indonesia

Ada dua model yang diusulkan oleh Mieke untuk mengatur kegiatan di cyber space, yaitu :

1. Model ketentuan Payung (Umbrella Provisions), Model ini dapat memuat materi pokok saja dengan memperhatikan semua kepentingan (seperti pelaku usaha, konsumen, pemerintah dan pemegak hukum), Juga keterkaitan hubungan dengan peraturan perundang – undangan.
2. Model Triangle Regulations sebagai upaya mengantisipasi pesatnya laju kegiatan di cyber space. Upaya yang menitikberatkan permasalahan prioritas yaitu pengaturan sehubungan transaksi online, pengaturan sehubungan privacy protection terhadap pelaku bisnis dan konsumen, pengaturan sehubungan cyber crime yang memuat yuridiksi dan kompetensi dari badan peradilan terhadap kasus cyber space.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Kebijakan IT di Indonesia (Cont)

Dalam modernisasi hukum pidana, Mas Wigrantoro Roes Setiyadi dalam seminar cyber crime 19 maret 2003 mengusulkan alternatif :

1. Menghapus pasal – pasal dalam UU terkait yang tidak dipakai lagi
2. Mengamandemen KUHP
3. Menyisipkan hasil kajian dalam RUU yang ada
4. Membuat RUU sendiri misalnya RUU Teknologi Informasi

Upaya tersebut tampaknya telah dilakukan terbukti dengan mulai disusunnya RUU KUHP yang baru (konsep tahun 2000). Di samping pembaharuan KHUP di Indonesia juga telah ditawarkan alternatif menyusun RUU sendiri, antara lain RUU yang disusun oleh tim dari pusat kajian cyber law UNPAD yang diberi title RUU TI draft III.

Tujuan dari dibentuknya cyber law sendiri menurut Sunarto (2006:42) adalah :

1. Melindungi data pribadi.
2. Menjamin kepastian hukum.
3. Mengatur tindak pidana cyber crime.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

TERIMA KASIH