BAB VII

# Cyberlaw : Hukum dan Keamanan

# Pendahuluan

- **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 .
  yuridis, cyber law tidak sama lagi dengan ukuran dan kualifikasi hukum tradisional. Kegiatan cyber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Kegiatan cyber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dari sini lahCyberlaw bukan saja keharusan, melainkan sudah merupakan kebutuhan untuk menghadapi kenyataan yang ada sekarang ini, yaitu dengan banyaknya berlangsung kegiatan cybercrime.

# Tujuan Cyber Law

- Cyberlaw sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana, ataupun penanganan tindak pidana. Cyber law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.

# Ruang Lingkup Cyber Law

- Pembahasan mengenai ruang lingkup ”cyber law” dimaksudkan sebagai inventarisasi atas persoalan-persoalan atau aspek-aspek hukum yang diperkirakan berkaitan dengan pemanfaatan Internet. Secara garis besar ruang lingkup ”cyber law” ini berkaitan dengan persoalan-persoalan atau aspek hukum dari:
  - 1. Hak Cipta (Copy Right)
    2. Hak Merk (Trademark)
    3. Pencemaran nama baik (Defamation)
    4. Hate Speech
    5. Hacking, Viruses, Illegal Access
    6. Regulation Internet Resource
    7. Privacy
    8. Duty Care
    9. Criminal Liability
    10. Procedural Issues (Jurisdiction, Investigation, Evidence, etc)
    11. Electronic Contract
    12. Pornography
    13. Robbery
    14. Consumer Protection E-Commerce, E- Government

# Topik-topik Cyber Law

Secara garis besar ada lima topic dari cyberlaw di setiap negara yaitu:

- *Information security*, menyangkut masalah keotentikan pengirim atau penerima dan integritas dari pesan yang mengalir melalui internet. Dalam hal ini diatur masalah kerahasiaan dan keabsahan tanda tangan elektronik.
- *On-line transaction*, meliputi penawaran, jual-beli, pembayaran sampai pengiriman barang melalui internet.
- *Right in electronic information*, soal hak cipta dan hak-hak yang muncul bagi pengguna maupun penyedia content.
- *Regulation information content*, sejauh mana perangkat hukum mengatur content yang dialirkan melalui internet.
- *Regulation on-line contact*, tata karma dalam berkomunikasi dan berbisnis melalui internet termasuk perpajakan, retriksi eksport-import, kriminalitas dan yurisdiksi hukum.

# Asas-asas Cyber Law

- Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu :
  - *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 jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.
  - *passive nationality* yang menekankan jurisdiksi berdasarkan kewarganegaraan korban.

# Asas-asas Cyber Law

- Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu :
  - ***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*". Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (*crimes against humanity*), misalnya penyiksaan, genosida, pembajakan udara dan lain-lain. Meskipun di masa mendatang asas jurisdiksi universal ini mungkin dikembangkan untuk internet piracy, seperti computer, cracking, carding, hacking and viruses, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.
    Oleh karena itu, untuk ruang cyber dibutuhkan suatu hukum baru yang menggunakan pendekatan yang berbeda dengan hukum yang dibuat berdasarkan batas-batas wilayah. Ruang cyber dapat diibaratkan sebagai suatu tempat yang hanya dibatasi oleh screens and passwords. Secara radikal, ruang cyber telah mengubah hubungan antara legally significant (online) phenomena and physical location.

# Teori-teori cyberlaw

- Berdasarkan karakteristik khusus yang terdapat dalam ruang cyber maka dapat dikemukakan beberapa teori sebagai berikut :
  - *The Theory of the Uploader and the Downloader*, Berdasarkan teori ini, suatu negara dapat melarang dalam wilayahnya, kegiatan uploading dan downloading yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk uploading kegiatan perjudian atau kegiatan perusakan lainnya dalam wilayah negara, dan melarang setiap orang dalam wilayahnya untuk downloading kegiatan perjudian tersebut. Minnesota adalah salah satu negara bagian pertama yang menggunakan jurisdiksi ini.
  - *The Theory of Law of the Server*. Pendekatan ini memperlakukan server dimana webpages secara fisik berlokasi, yaitu di mana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah webpages yang berlokasi di server pada Stanford University tunduk pada hukum California. Namun teori ini akan sulit digunakan apabila uploader berada dalam jurisdiksi asing.
  - *The Theory of InternationalSpaces.* Ruang cyber dianggap sebagai the fourth space. Yang menjadi analogi adalah tidak terletak pada kesamaan fisik, melainkan pada sifat internasional, yakni *sovereignless quality*.

# Cyber Crime

- sebuah bentuk kriminal yang mana menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan kriminal. Masalah yang berkaitan dengan kejahatan jenis ini misalnya hacking, pelanggaran hak cipta, pornografi anak, eksploitasi anak, carding dan masih bnyak kejahatan dengan cara internet. Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.
- Dalam definisi lain, **kejahatan dunia maya adalah** istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, confidence fraud, penipuan identitas, pornografi anak, dll.

# Cyber Crime

- Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. Umumnya, kejahatan ini dibagi menjadi dua kategori: (1) kejahatan yang menjadikan jaringan komputer dan divais secara langsung menjadi target;

- (2) Kejahatan yang terfasilitasi jaringan komputer atau divais, dan target utamanya adalah jaringan komputer independen atau divais.

# Cyber Crime

- Malware (malicious software / code)
- Malware (berasal dari singkatan kata malicious dan software) adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, server atau jaringan komputer tanpa izin (informed consent) dari pemilik. Istilah ini adalah istilah umum yang dipakai oleh pakar komputer untuk mengartikan berbagai macam perangkat lunak atau kode perangkat lunak yang mengganggu atau mengusik. Istilah 'virus computer' terkadang dipakai sebagai frasa pemikat (catch phrase) untuk mencakup semua jenis perangkat perusak, termasuk virus murni (true virus).
- Denial-of-service (DOS) attacks
- Denial of service attack atau serangan DoS adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

# Cyber Crime

- Computer viruses
- Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus murni hanya dapat menyebar dari sebuah komputer ke komputer lainnya (dalam sebuah bentuk kode yang bisa dieksekusi) ketika inangnya diambil ke komputer target, contohnya ketika user mengirimnya melalui jaringan atau internet, atau membawanya dengan media lepas (floppy disk, cd, dvd, atau usb drive). Virus bisa bertambah dengan menyebar ke komputer lain dengan mnginfeksi file pada network file system (sistem file jaringan) atau sistem file yang diakses oleh komputer lain.
- Phishing scam
- Dalam sekuriti komputer, phising (Indonesia: pengelabuan) adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. Istilah phishing dalam bahasa Inggris berasal dari kata fishing (= memancing), dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna.

# Cyber Crime

- Cyber stalking (Pencurian dunia maya)
- Cyberstalking adalah penggunaan internet atau alat elektronik lainnya untuk menghina atau melecehkan seseorang, sekelompok orang, atau organisasi. Hal ini termasuk tuduhan palsu, memata-matai, membuat ancaman, pencurian identitas, pengerusakan data atau peralatan, penghasutan anak di bawah umur untuk seks, atau mengumpulkan informasi untuk mengganggu. Definisi dari “pelecehan” harus memenuhi kriteria bahwa seseorang secara wajar, dalam kepemilikan informasi yang sama, akan menganggap itu cukup untuk menyebabkan kesulitan orang lain secara masuk akal.
- Penipuan dan pencurian identitas
- Pencurian identitas adalah menggunakan identitas orang lain seperti KTP, SIM, atau paspor untuk kepentingan pribadinya, dan biasanya digunakan untuk tujuan penipuan. Umumnya penipuan ini berhubungan dengan Internet, namun sering huga terjadi di kehidupan sehari-hari. Misalnya penggunaan data yang ada dalam kartu identitas orang lain untuk melakukan suatu kejahatan. Pencuri identitas dapat menggunakan identitas orang lain untuk suatu transaksi atau kegiatan, sehingga pemilik identitas yang aslilah yang kemudian dianggap melakukan kegiatan atau transaksi tersebut.

# Cyber Crime

- Perang informasi (Information warfare)
- Perang Informasi adalah penggunaan dan pengelolaan informasi dalam mengejar keunggulan kompetitif atas lawan. perang Informasi dapat melibatkan pengumpulan informasi taktis, jaminan bahwa informasi sendiri adalah sah, penyebaran propaganda atau disinformasi untuk menurunkan moral musuh dan masyarakat, merusak kualitas yang menentang kekuatan informasi dan penolakan peluang pengumpulan-informasi untuk menentang kekuatan. Informasi perang berhubungan erat dengan perang psikologis.
- Contohnya ketika seseorang mencuri informasi dari situs, atau menyebabkan kerusakan computer atau jaringan komputer. Semua tindakan ini adalah virtual (tidak nyata) terhadap informasi tersebut -hanya ada dalam dunia digital, dan kerusakannya -dalam kenyataan, tidak ada kerusakan fisik nyata kecuali hanya fungsi mesin yang bermasalah.
- Komputer dapat dijadikan sumber bukti. Bahkan ketika komputer tidak secara langsung digunakan untuk kegiatan kriminal, komputer merupakan alat yang sempurna untuk menjaga record atau catatan, khususnya ketika diberikan tenaga untuk mengenkripsi data. Jika bukti ini bisa diambil dan didekripsi, ini bisa menjadi nilai bagi para investigator kriminal.

# Cyber Crime Hacker dan Cracker

- Menurut Mansfield, hacker didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya, tetapi tidak melakukan tindakan pengrusakan apapun, tidak mencuri uang atau informasi. Sedangkan cracker adalah sisi gelap dari hacker dan memiliki kertertarikan untuk mencuri informasi, melakukan berbagai macam kerusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer.

  - **Recreational Hackers**, kejahatan yang dilakukan oleh netter tingkat pemula untuk sekedar mencoba kekurang handalan sistem sekuritas suatu perusahaan
  - **Crackers/Criminal Minded hackers**, pelaku memiliki motivasi untuk mendapat keuntungan finansial, sabotase dan pengerusakan data. Tipe kejahatan ini dapat dilakukan Penggolongan Hacker dan Cracker dengan bantuan orang dalam.
  - **Political Hackers,** aktifis politis (hacktivist) melakukan pengrusakan terhadap ratusan situs web untuk mengkampanyekan programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendiskreditkan lawannya.

# 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 : Melibatkan unsur yang terkait (pemerintah, swasta, profesional).
  - Menggunakan pendekatan moderat untuk mensintesiskan prinsip hukum konvensional dan norma hukum baru yang akan terbentuk
  - Memperhatikan keunikan dari dunia maya
  - Mendorong adanya kerjasama internasional mengingat sifat internet yang global
  - Menempatkan sektor swasta sebagai leader dalam persoalan yang menyangkut industri dan perdagangan.
  - Pemerintah harus mengambil peran dan tanggung jawab yang jelas untuk persoalan yang menyangkut kepentingan publik
  - Aturan hukum yang akan dibentuk tidak bersifat restriktif melainkan harus direktif dan futuristik
  - 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 Informasi dan transaksi elektronik, UU perlindungan konsumen, UU Penyiaran dan Telekomunikasi,
    UU Perseroan Terbatas, UU Penanaman Modal Asing, UU Perpajakan, Hukum Kontrak, Hukum Pidana dll.

# Undang – undang Informasi dan Transaksi Elektronik

- Rancangan Undang-undang Informasi dan transaksi elektronik (RUU ITE) yang telah disahkan menjadi undang - undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Mulai dirancang sejak Maret 2003 oleh kementrian Negara Komunikasi dan Informasi dengan nama rancangan undang undang informasi elektronik dan transaksi elektronik (RUU- ITE)
- Melalui serangkaian pembahasan sebelumnya, UU ITE ditetapkan menjadi undang-undang pada Rapat Paripurna Dewan tanggal 25 Maret 2008
  - UU ITE terdiri dari 13 Bab dan 54 Pasal dengan cakupan materi antara lain :
  - Pengakuan informasi dan atau dokumen elektronik sebagai alat bukti hukum yang sah
  - Pengakuan atas tanda tangan elektronik
  - Penyelenggaraan sertifikasi elektronik dan sistem elektronik
  - Hak kekayaan intelektual dan perlindungan hak pribadi
  - Perbuatan yang dilarang serta ketentuan pidananya

Merci bien
ありがとう
Matur Nuwun
Hatur Nuhun
Obrigado
Dank
Thanks
Matur se Kelangkong
Syukron
Kheili Mamnun
ευχαριστιες
Danke
Grazias
谢谢
Terima Kasih



Irawan_afrianto@yahoo.com

Irawan.afrianto

@Irawan_afrianto

+628170223513