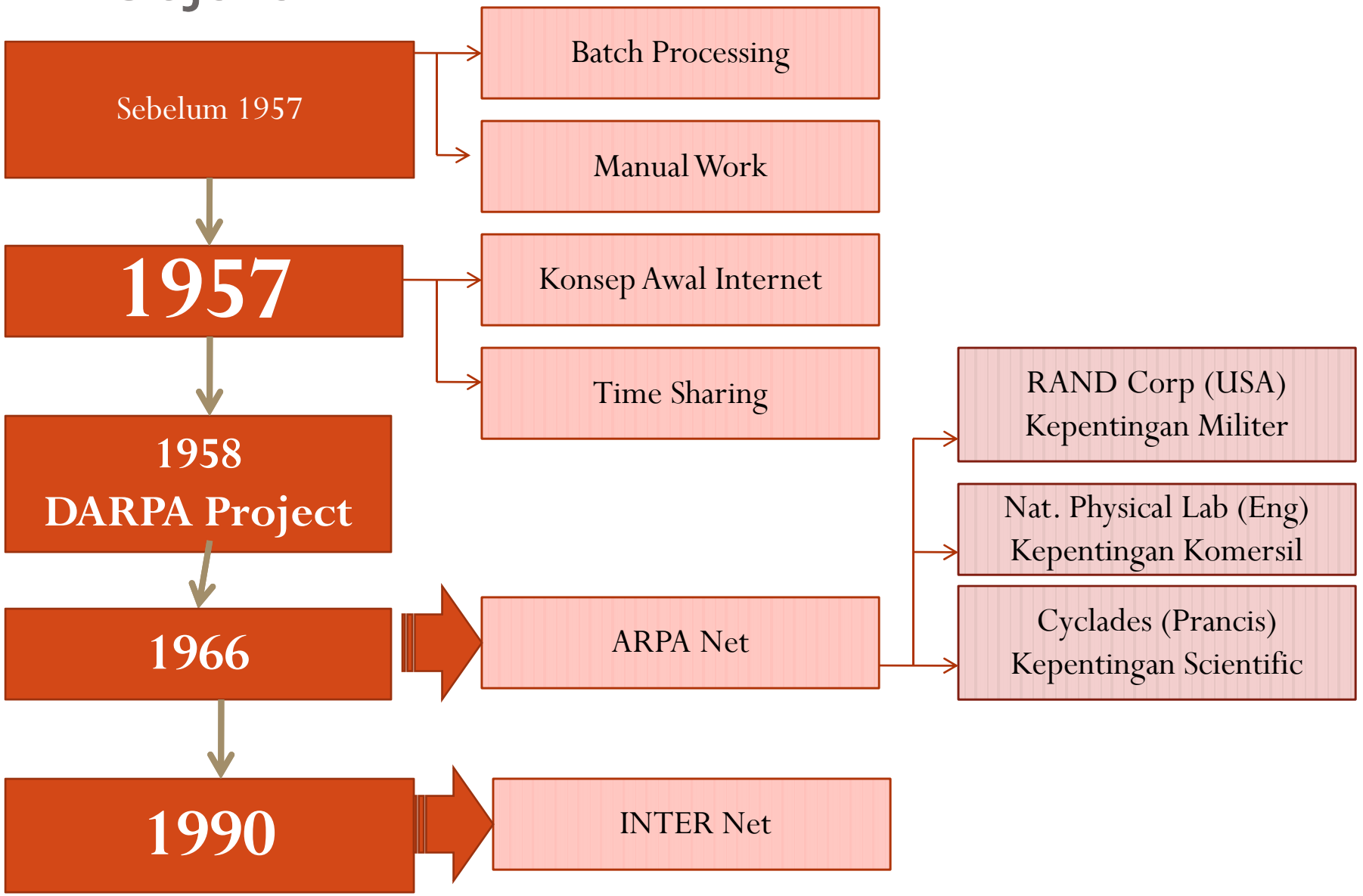
PRAKTEK HUKUM TELEMATIKA

Rencana Perkuliahan

Sesi	Materi
1	Pengantar
2	Perkembangan Pemanfaatan Teknologi Informasi dan Telekomunikasi
3	Problematika Hukum Internet
4	Aspek Hukum Perlindungan Data dan Hak Pribadi
5	Aspek Hukum Media di Internet
6	Kajian Aspek Pidana
7	Kajian Aspek Hukum Internasional
8	UTS
9	Aspek Hukum HKI
10	Evolusi Hukum dan Regulasi Telekomunikasi di Indonesia
11	Kajian Aspek Hukum Telekomuniasi UU No.36/1999 dan UU No.11/2008
12	Perkembangan Sistem Pembuktian dan Alat Bukti Elektronik
13	Unifikasi dan Upaya Harmonisasi Hukum
14	UAS

Sejarah


Sebelum 1957
Batch Processing
Manual Work
1957
Konsep Awal Internet
Time Sharing
1958
DARPA Project
RAND Corp (USA)
Kepentingan Militer
Nat. Physical Lab (Eng)
Kepentingan Komersil
1966
ARPA Net
Cyclades (Prancis)
Kepentingan Scientific
1990
INTER Net

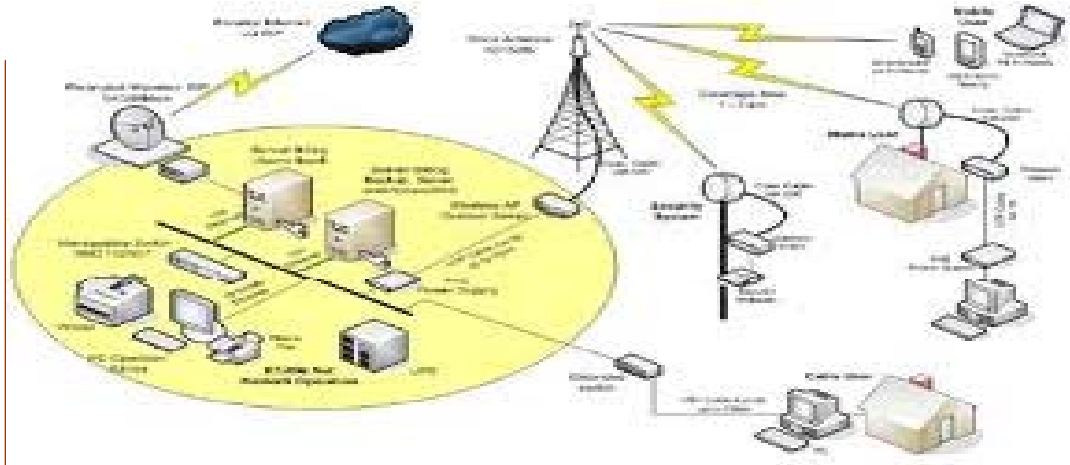
Definisi

- Telematika
- Multi Media
- *Cyber Space*

TELEMATIKA

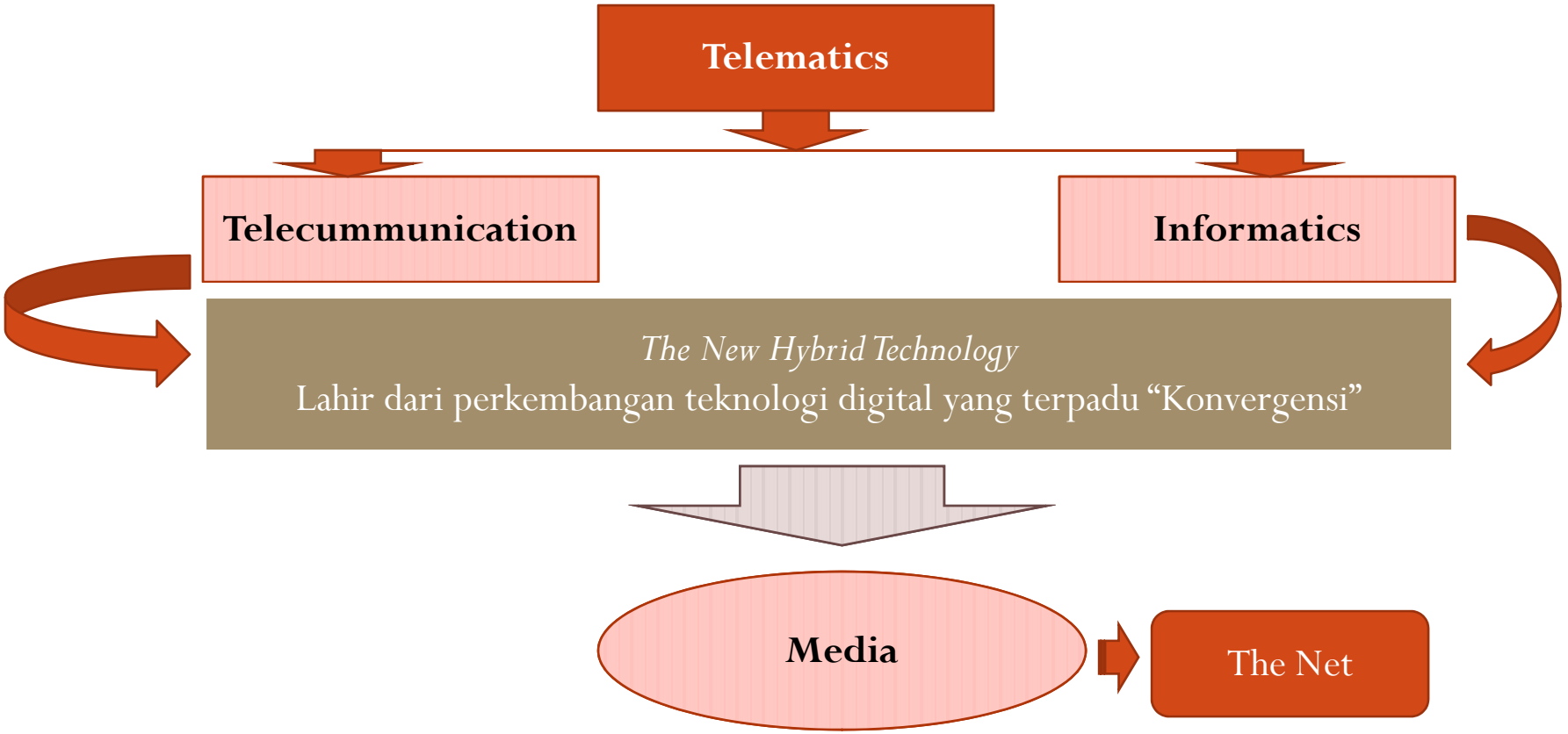
Asal Kata : "TELEMATIQUE" (Bahasa Prancis)

Istilah Umum Di Eropa



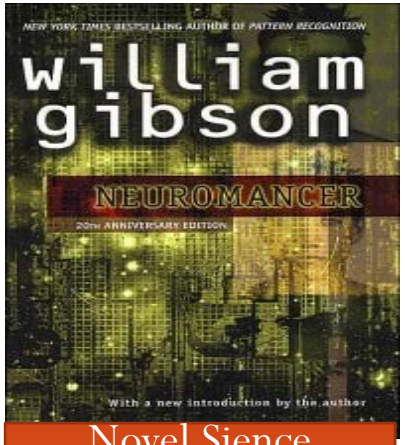
Menggambarkan Pertemuan Sistem Jaringan Komunikasi dengan Teknologi Informasi

PERKEMBANGAN KONSEPSI TELEMATIKA



Cyber Space

Penggunaan Internet Meningkat



Novel Sience Fiction 1984

Cyber Space

Merupakan suatu bentuk halusinasi virtual yang di gambarkan seakan-akan adanya suatu ruang baru (space) yang lahir akibat terhubungnya medium kawat penghantar listrik (cyber) yang mempertemukan sistem komputer dengan sistem telekomunikasi virtual dalam penyelenggaraan sistem elektronik.

Keterkaitan Dengan Hukum

Sist HK

Sist HK

Sist HK

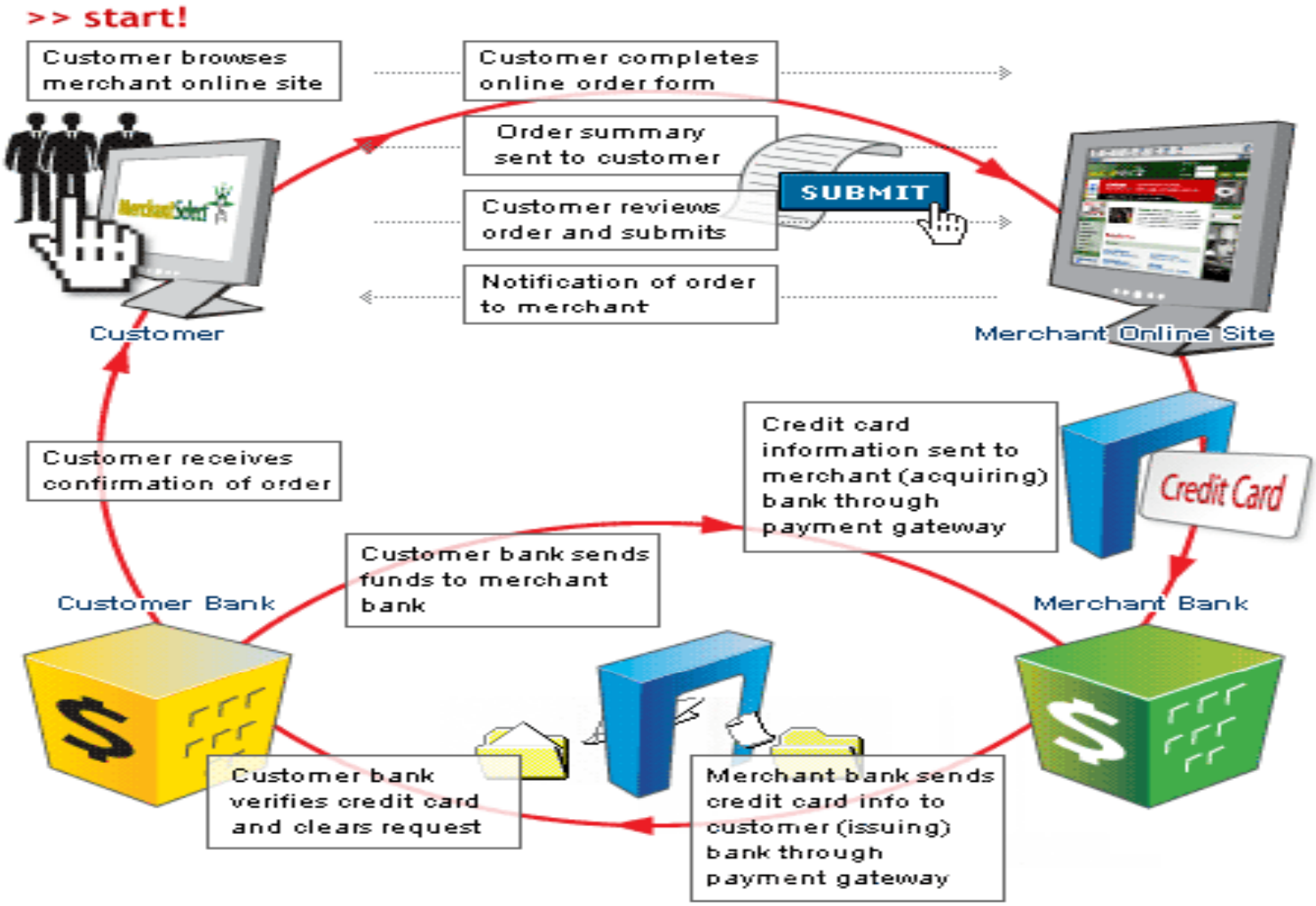
Sist HK

Melakukan Transaksi Elektronik secara online

Di Atur oleh Ketentuan Hukum apa?

Hubungan Hukum

Transaksi Ekonomi



Tugas

- Buat Paper : Sejarah ,Perkembangan dan Lingkup Kajian Hukum Telematika (Hukum apa saja yang terkait dengan telematika, baik dari aspek Pidana, Perdata dll)
- ega.megawati@gmail.com
- www.hakinet.ikht.org
- www.cyberlaw.lkht.org
- www.wipo.org
- www.eu.org
- www.law.washington.edu
- Edmon makarim
- Benjamin wright, law on electronic commerce, texas 1995

Perkembangan pemanfaatan teknologi informasi dan komunikasi

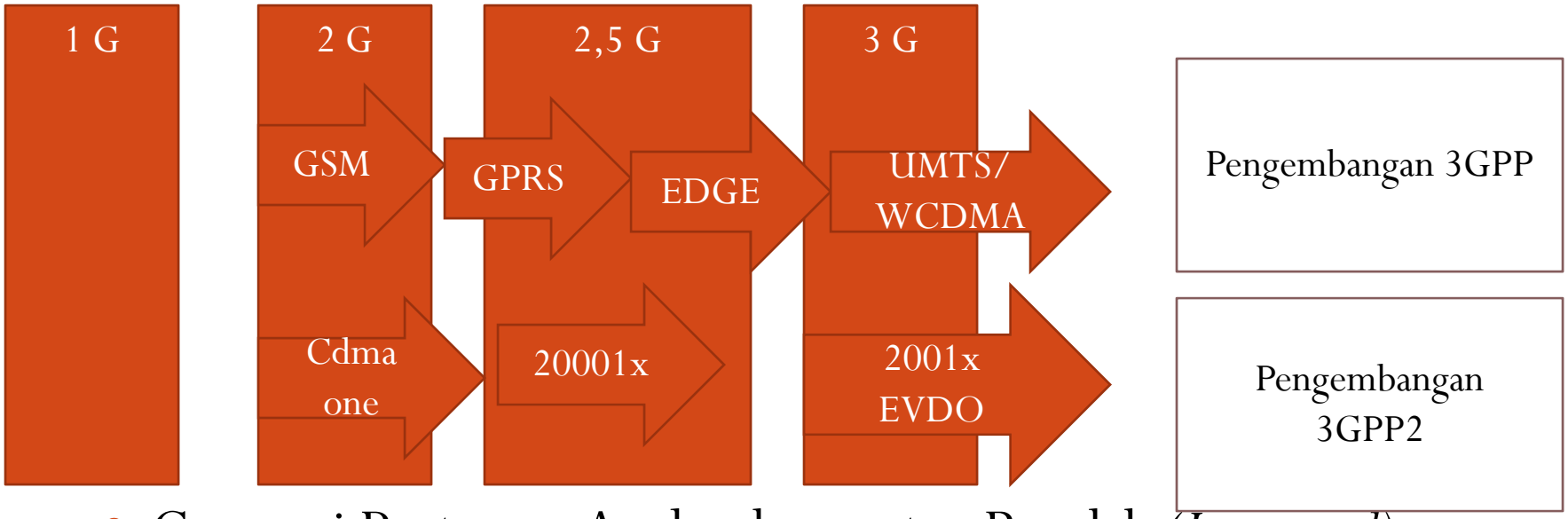
UNIVERSITAS INDONUSA ESA UNGGUL

FAKULTAS HUKUM

TAHUN 2013

Sejarah dan Perkembangan

- 1844 Telegraph
- 1876 Telephone, 1877 Bell co. Akuisisi Western Electric
- 1913 Kingsbury Commitment : QS for All = Universal Service, 1921 Congress Passed the Graham Act to Codify it
- 1934 = US Communication Act, FCC Regulates Telecomunications
- 1948 First Cable system
- 1962 First Communication Satelite (AT & T Telstar, First Digital Phone Network, First Pager)
- 1975 : HBO's first satellite transmission
- 1977 Microwave Communication Inc (MCI Worldcom)
- 1978 Cellular Telephone Service begin in US + (1stG)
- 1984 AT & T Divest Local Operating Companies (RBOC's)
- 1995 Direct Broadcast Satellite (DBS) System = (2nd G PCS)
- 1996 US Telecommunication Act opens up to Competition
- 2002 Telecom 'Meltdown'



- Generasi Pertama : Analog kecepatan Rendah *(Low speed)*, cukup untuk suara. Contoh : NMT (National Mobile Telephone)
- Generasi Kedua : Digilat, kecepatan Rendah-Menengah, Contoh :GSM dan CDMA
- Generasi Ketiga :Digital, kecepatan tinggi, untuk pita lebar *(broadband)* contoh : W-CDMA

ISU UTAMA 3G

- Penggunaan Spektrum frekuensi untuk 3G,apakah akan efektif?
- Bagaimana perkembangan ke depannya apakah aplikasinya siap?
- Bagaimana membuatnya menjadi murah?

Definisi

- Telekomunikasi

  Setiap pemancaran, pengiriman, dan/atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem, kawat,optik, radio atau sistem elektromagnetik lainnya

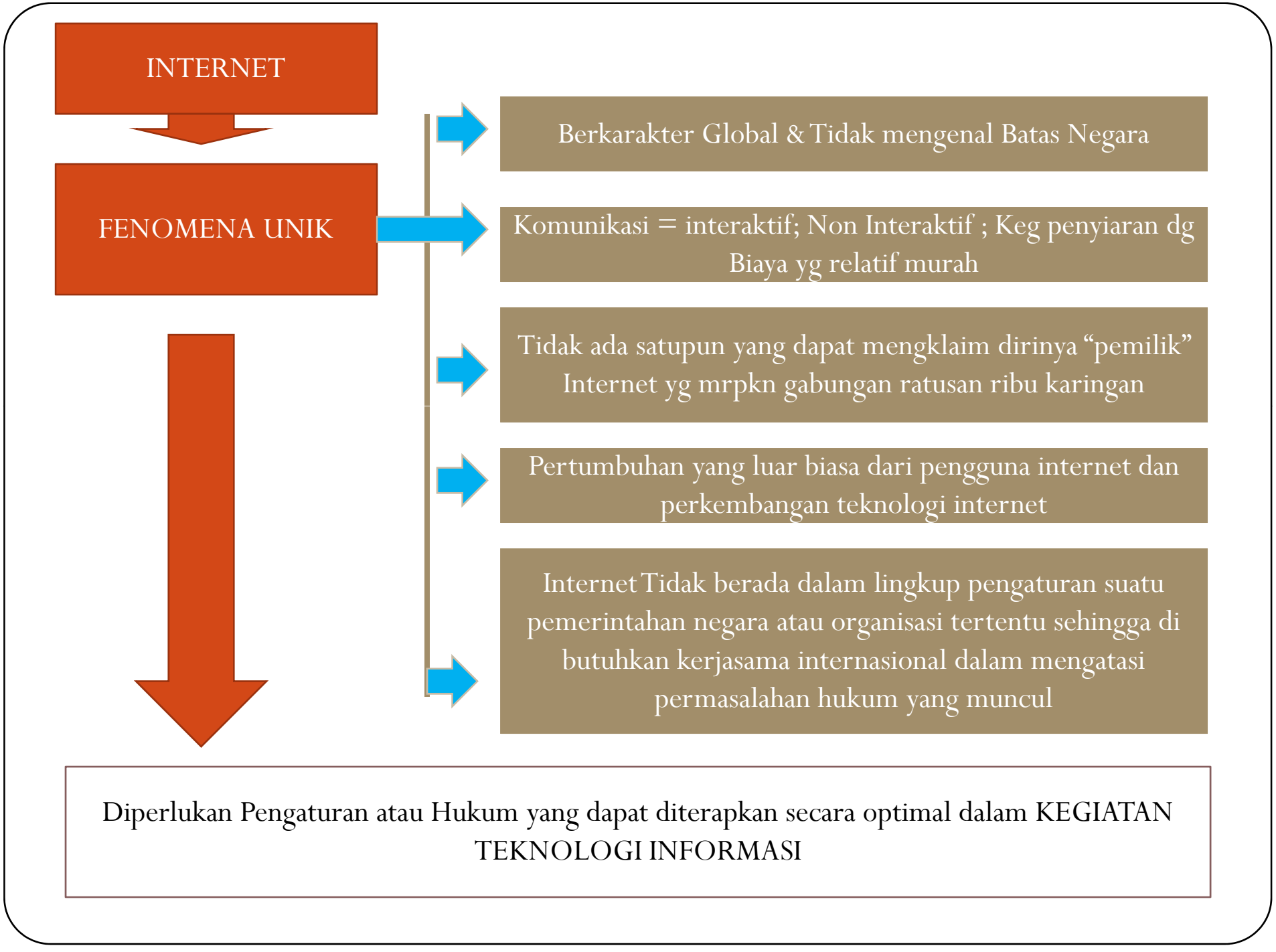
- Bagaimana Paradigma Hukumnya?

  a. *Who Owes the wires?*

  b.Who own the air? Spektrum Frekwensi bersifat terbatas

  * Apakah diperlukan regulasi untuk menata/mengalokasi penggunaan spektrum tersebut?

  * Apakah perkembangan teknologi yang nantinya akan menentukan dasar penataannya?


INTERNET
FENOMENA UNIK
Berkarakter Global & Tidak mengenal Batas Negara
Komunikasi = interaktif; Non Interaktif ; Keg penyiaran dg Biaya yg relatif murah
Tidak ada satupun yang dapat mengklaim dirinya "pemilik" Internet yg mrpkn gabungan ratusan ribu karingan
Pertumbuhan yang luar biasa dari pengguna internet dan perkembangan teknologi internet
Internet Tidak berada dalam lingkup pengaturan suatu pemerintahan negara atau organisasi tertentu sehingga di butuhkan kerjasama internasional dalam mengatasi permasalahan hukum yang muncul
Diperlukan Pengaturan atau Hukum yang dapat diterapkan secara optimal dalam KEGIATAN TEKNOLOGI INFORMASI

INFORMASI

- Definisi “Informasi “ dalam aspek Bahasa

= keterangan, kabar, Pemberitahuan

- Realita pengertian “Informasi” yang berkembang :

= isi atau muatan dokumen yang ditemui sehari-hari

KEBEBASAN MEMPEROLEH INFORMASI

- Kebebasan Memperoleh Informasi = Hak Asasi
- Hak Privat Vs Hak Publik (Pembahasan Lebih dalam pada sesi minggu depan)
- Amerika : Kebebasan memperoleh Informasi tidak di perkenankan melanggar hak-hak pribadi dari seseorang
- Pasal 12 *The Universal Declaration of Human Rights-1948" No-one should be subjectedto arbtrary interference with his privacy, family, home or correspondence nor to attack on his honor or reputation. Everyone has the right to the protection of the Law such interferences or attacks"*

Hak Untuk Mendapatkan Informasi

- Sebelum 1998

  Informasi yang di sampaikan relatif "Terkontrol"

- Setelah 1998

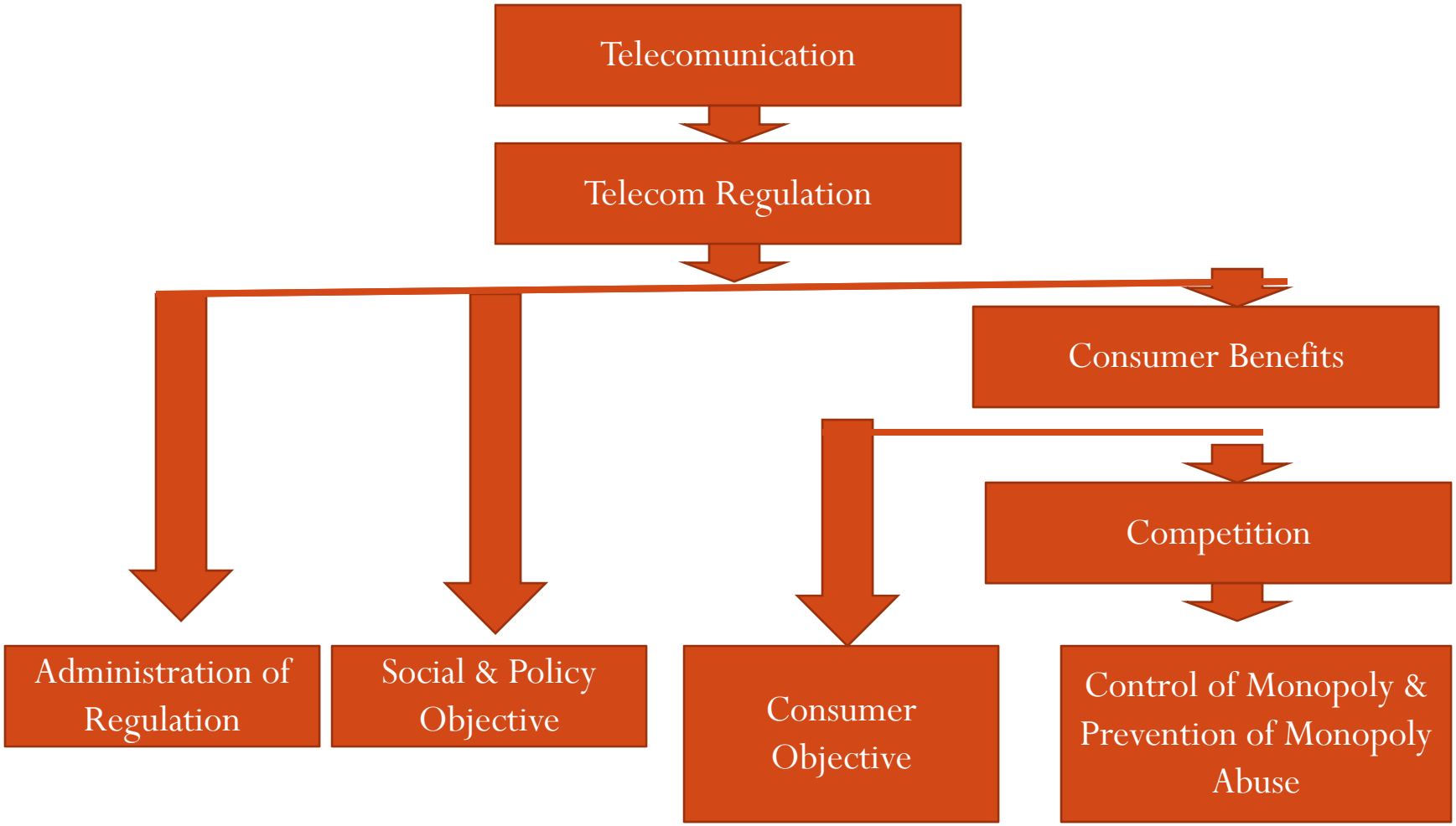
  Terjadi perubahan yang cukup signifikan

Pengaturan

- Pasal 28F dari Amandemen Kedua UUD 1945

  "Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia"

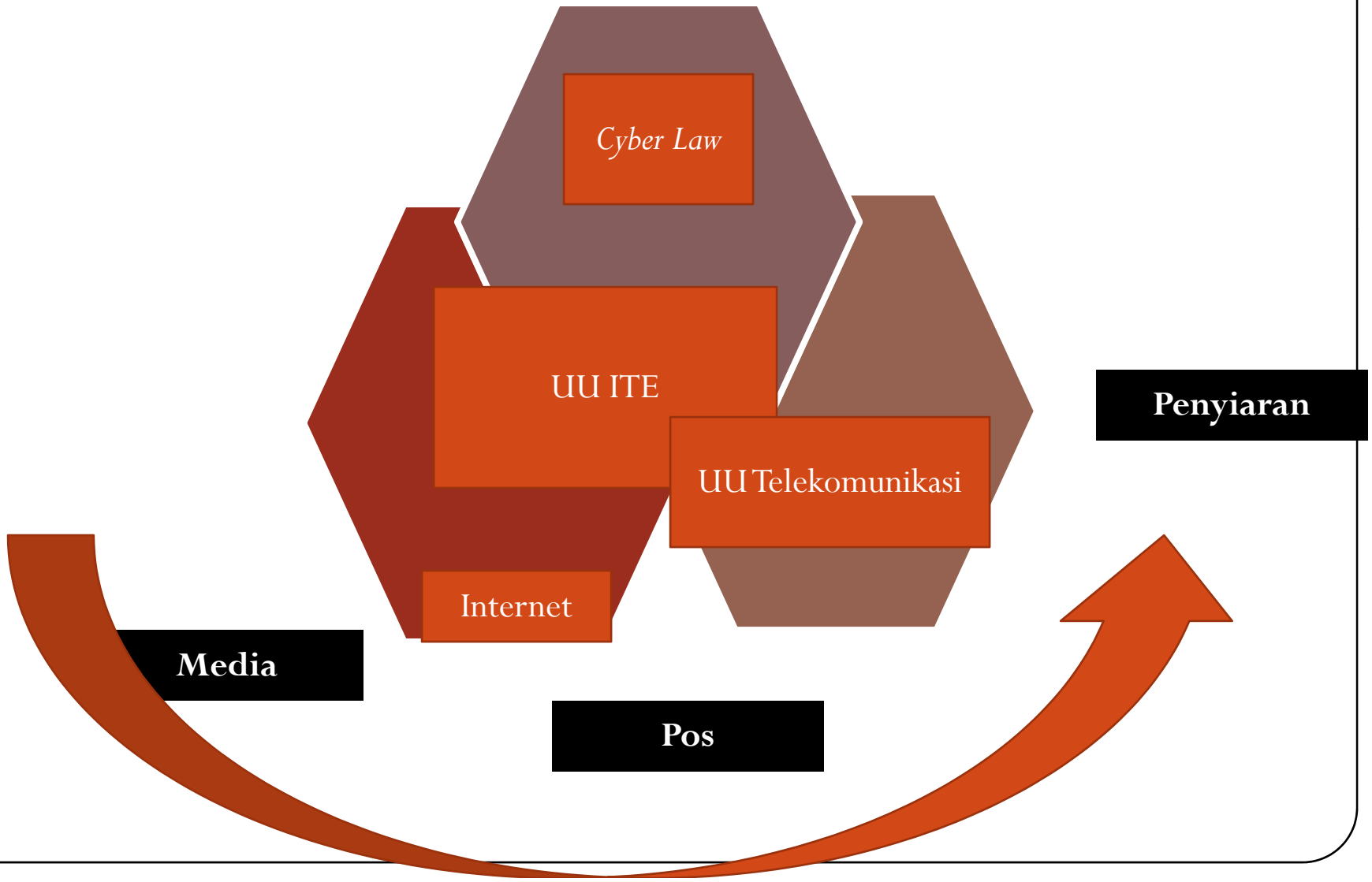
TELECOMUNICATION REGULATION



TELECOM PARADIGM

Old Regime (Pre 1980)	New Regime (Post 1990)
International telephony a jointly-provider service	International telephony a traded service
Monopoly service & Infrastructure Provision	Competitive service & Infrastructure provision
Government ownership of control	Privat Ownership
Traffic travels mainly over PSTN	Traffic over PSTN,leased lines, private nets,internet,ISR, CSP,Network, etc
Traffic travels mainly over PSTN	Multimedia traffic
Balanced traffic flows	Imbalanced traffic flows
Exchange rate stability	Exchange rate instability

Konvergensi Peraturan Perundang-undangan di Indonesia



Tugas

- Resume Perkuliahan
- Paper Perubahan Paradigma Pengaturan Telekomunikasi di Indonesia

PROBLEMATIKA HUKUM DAN INTERNET

TELEKOMUNIKASI SEBAGAI SARANA PEMBANGUNAN

Thomas Franck (1971)

Pembangunan Ekonomi = Pembangunan Hukum

Pembangunan Ekonomi

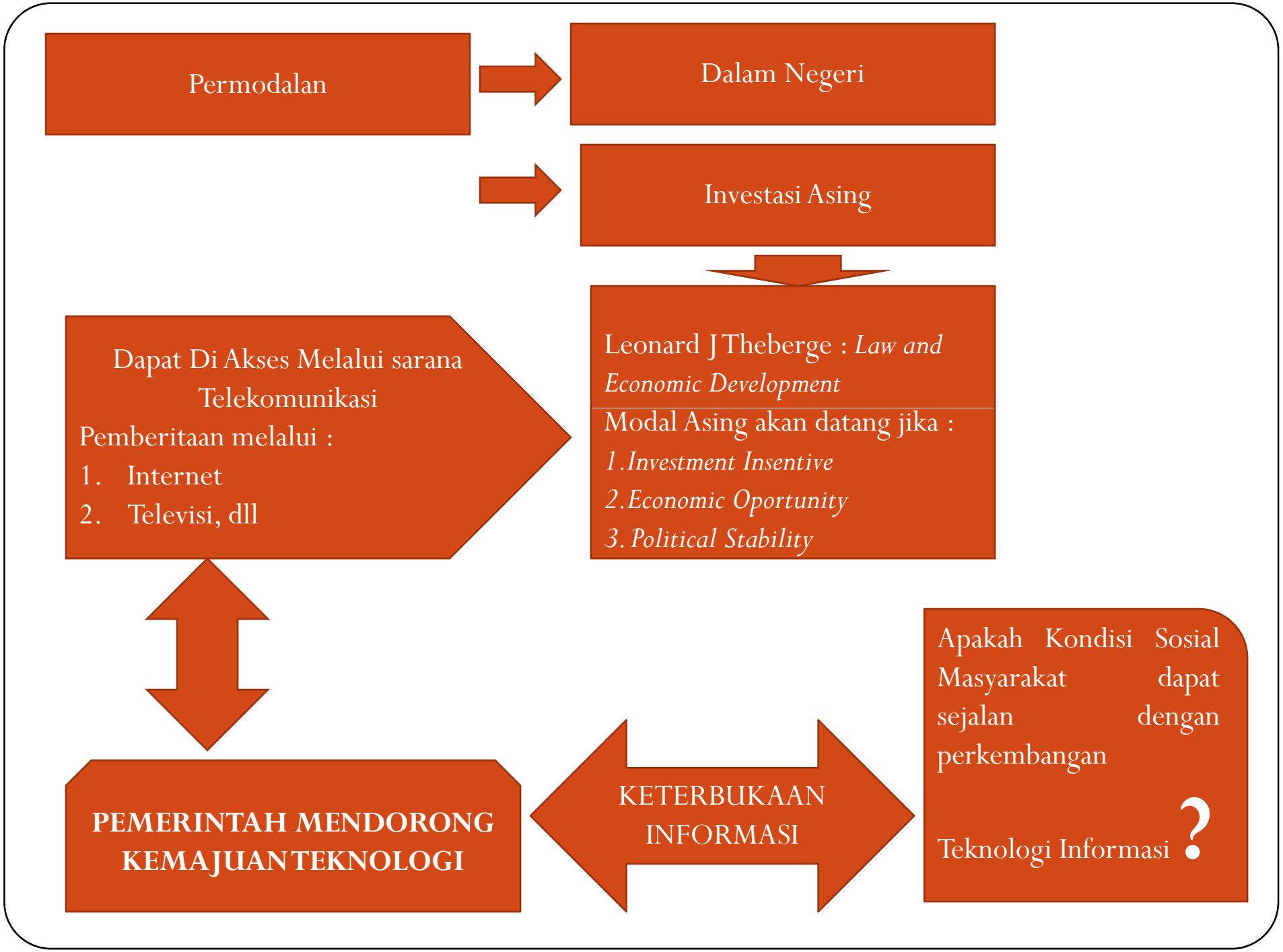
Bersifat Kualitatif, Tidak hanya terkonsentrasi pada pertambahan produksi tapi juga terdapat perubahan-perubahan dalam struktur perekonomian

Pertumbuhan Ekonomi

Proses Perubahan suatu negara secara berkesinambungan menuju keadaan yang lebih baik selama periode tertentu (bersifat Kuantitatif)

Faktor Pendorong Pertumbuhan Ekonomi :

1. Sumber Daya Manusia
2. Sumber Daya Alam
3. Ilmu Pengetahuan dan Teknologi
4. Faktor Budaya
5. **Sumber Daya Modal**


Permodalan
Dalam Negeri
Investasi Asing
Leonard J Theberge : Law and Economic Development
Modal Asing akan datang jika :
1. Investment Insentive
2. Economic Oportunity
3. Political Stability
Dapat Di Akses Melalui sarana Telekomunikasi
Pemberitaan melalui :
1. Internet
2. Televisi, dll
PEMERINTAH MENDORONG KEMAJUAN TEKNOLOGI
KETERBUKAAN INFORMASI
Apakah Kondisi Sosial Masyarakat dapat sejalan dengan perkembangan
Teknologi Informasi ?

DAMPAK PERKEMBANGAN TEKNOLOGI INFORMASI

- Positive
  * Akses Mudah dan Cepat
  * Efisiensi Waktu
  * Nyaman
  * Ekonomis
- Negative

  * Perkembangan Teknologi Informasi sangat cepat, sementara Kondisi masyarakat belum siap menerima perubahan tersebut karena adakalanya bertentangan dengan kondisi sosial dan nilai-nilai yang berlaku dalam masyarakat (Terjadi Instabilitas Sosial)

  * Perkembangan Teknologi Informasi di manfaatkan oleh segelintir orang sebagai sarana untuk melakukan Tindakan Kejahatan melalui Media Elektronik (*Cyber Cirme)*

PROBLEMATIKA HUKUM TERKAIT DENGAN PERKEMBANGAN TEKNOLOGI INFORMASI

- Aspek Hukum Pidana
- Aspek Hukum Perdata
- Aspek Hukum Tata Negara
- Aspek Hukum Administrasi Negara

CYBER CRIME

- Bentuk *Cyber Crime :*

  a. Pencemaran Nama Baik

  b. Pornography

  c. Perjudian

  d. Pembobolan Rekening

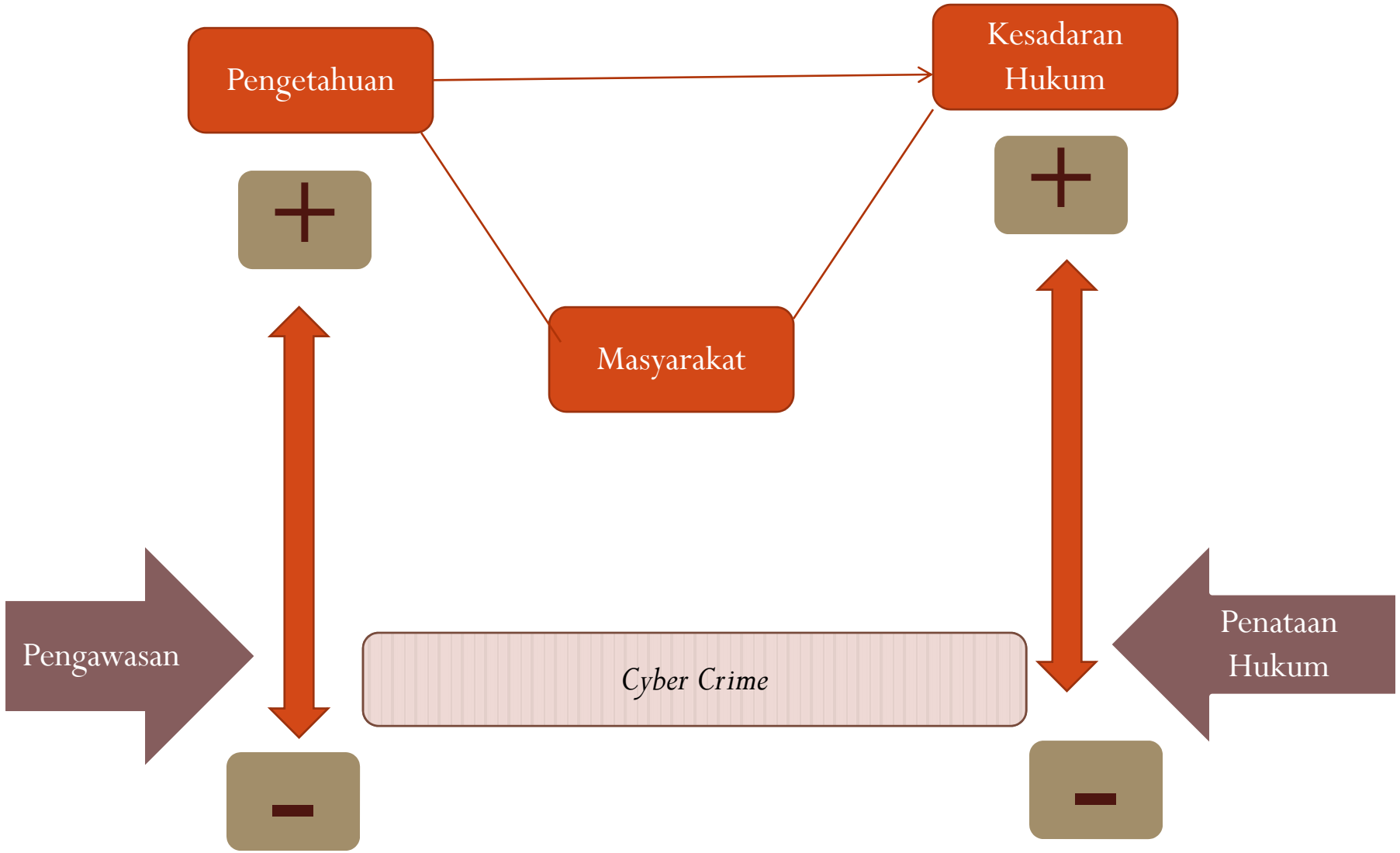
  e. Penipuan

  f. Tindak Pidana Terorisme, dll

Faktor Pendorong Pertumbuhan *Cyber Crime*

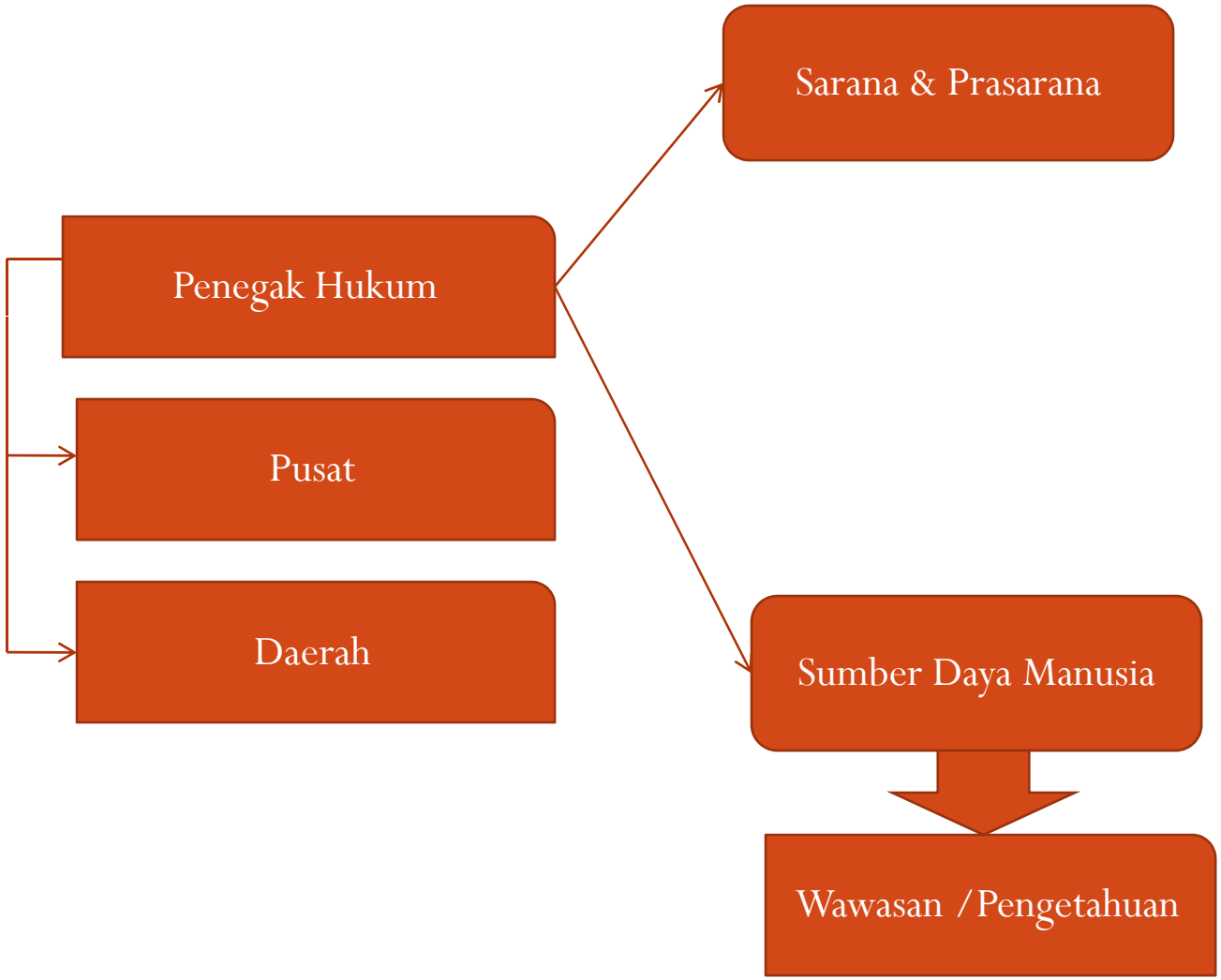
- Kesadaran Hukum Masyarakat
- Faktor Keamanan
- Faktor Penegak Hukum
- Faktor Peraturan per-Undang-Undangan

KESADARAN HUKUM MASYARAKAT

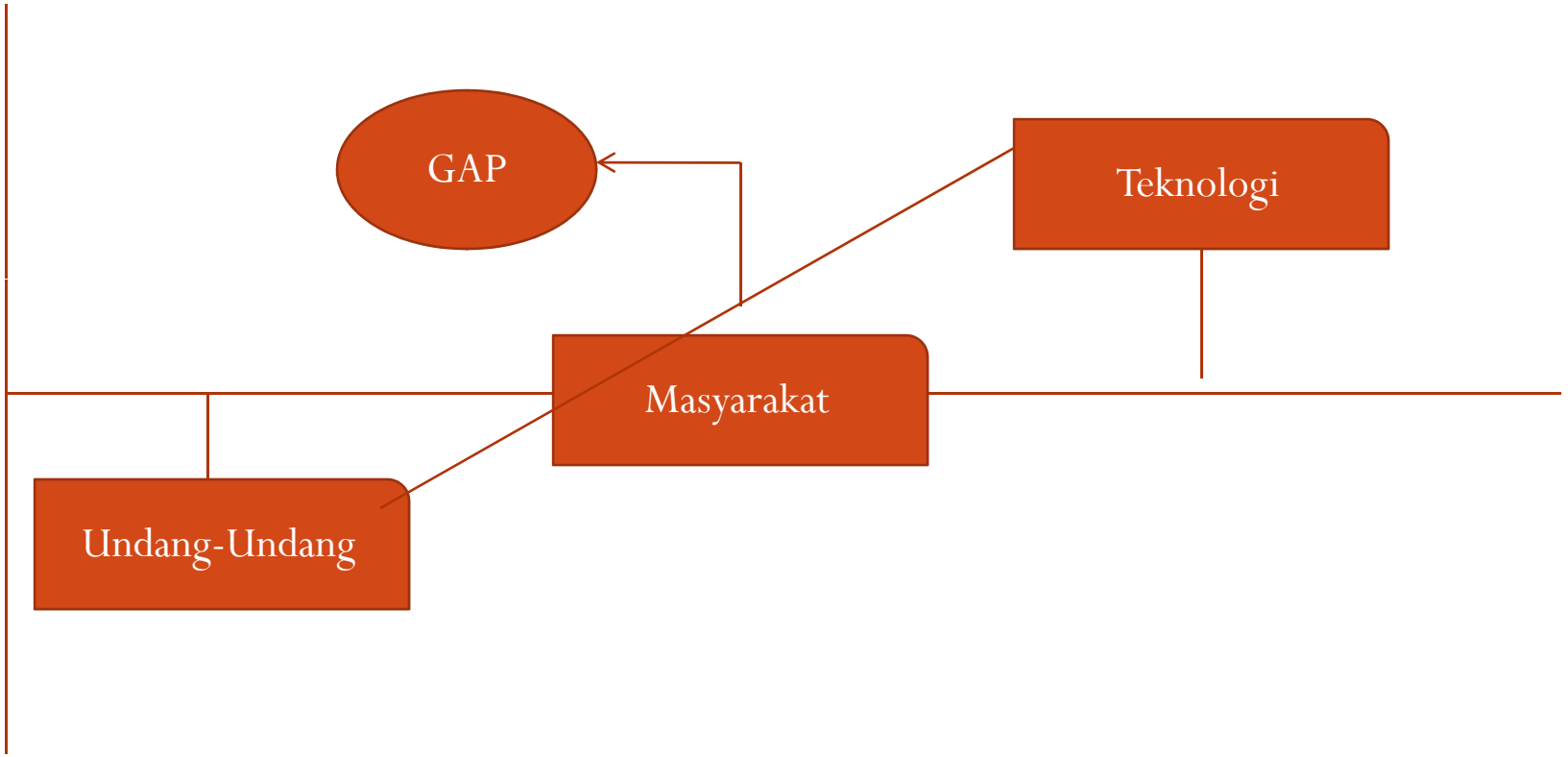


FAKTOR KEAMANAN

Faktor Penegak Hukum



Faktor Peraturan perUndang-Undangan



Transaksi Elektronik dan Sistem Elektronik

- Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya
- Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan,dan/atau menyebarkani elektronik

Implikasi Hukum

- Otentifikasi subjek hukum yang membuat transaksi melalui internet
- Kapans saat perjanjian berlaku dan memiliki kekuatan mengikat secara hukum
- Objek transaksi yang diperjual belikan
- Bagaimana mekanisme peralihan hak
- Hubungan hukum dan pertanggung jawaban para pihak yang terlibat dalam transaksi baik penjual, pembeli, maupun para pendukung seperti perbankan, internet service provider (ISP) dll
- Legalitas dokumen catatan elektronik serta tanda tangan digital sebagai tanda bukti
- Mekanisme Penyelesaian sengketa
- Pilihan Hukum dan forum peradilan yang berwenang dlaam penyelesaian sengketa

Admisbility of Electronic Signature (pas 11)

- Tanda tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah, selama memenuhi persyaratan

a. Data hanya terkait dengan penanda tangan
b. Data pembuatan tanda tangan elektronik hanya berada dalam kuasa penanda tangan
c. Segala perubahan atas tanda tangan dapat diketahui
d. Segala perubahan atas IE yang terkait dengan tanda tangan elektronik dapat diketahui
e. Terdapat cara mengidentifikasi penanda tangan
f. Terdapat cara tertentu untuk menunjukan persetujuan penanda tangan atas IE terkait

Sistem Elektronik yang "Trusted"

- Pelaku usaha yang menawarkan produk melalui sistem elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen dan produk yang ditawarkan (pasal 9)
- Pelaku usaha dapat disertifikasi oleh lembaga sertifikasi keandalam (Pasal 10)
- Sertifikasi keandalan :

a. Bukti pelaku usaha melakukan perdagangan secara layak
b. Logo sertifikasi (*trust mark)*

- Transaksi elektronik yang dituangkan ke dalam kontrak elektronik mengikat para pihak dengan syarat:

  a. Menggunakan sarana yang disepakati

  b. Penerimaan penawaran dilakukan secara elektronik (Formalitas perjanjian)

- Dalam transaksi elektronik internasional, para pihak memiliki kewenangan untuk menentukan (pasal 18)

a. Choice of law
b. Choice of forum
c. Jika tidak ditentukan, maka berlaku asas-asas hukum perdata internasional

Transaksi Elektronik

- Transaksi dianggap terjadi pada saat penawaran transaksi yang dikirim pengirim telah diterima dan disetujui penerima (Pasal 20 ayat (1))
- Persetujuan atas penawaran harus dilakukan dengan pernyataan penerimaan secara elektronik (pasal 20 ayat(2))
- Transaksi dapat dilakukan melalui Kuasa atau Keagenan Elektronik (Pasal 21 ayat(1))
- Tanggung jawab transaksi (Pasal 21 ayat 2))

1. Dilakukan para pihak : Para Pihak
2. Dilakukan dengan kuasa : Pemberi kuasa
3. Dilakukan oleh Agen : Penyelenggara Agen

- Pengecualian : *force majeure*,kesalahan dan/atau kelalaian pengguna sistem elektronik

- Bertanggung jawab atas segala akibat hukum atas:

1. Transaksi elektronik yang menggunakan agen elektronik
2. Gagal beroperasinya agen elektronik akibat tindakan pihak ke-3 (tiga) secara langsung (pasal 21)

- Harus menyediakan fitur pada agen elektronik tertentu yang memungkinkan pengguna melakukan perubahan informasi (edit, cancle,dll) dalam proses transaksi (Pasal 22)

HAPUSNYA TANGGUNG JAWAB PENYELENGGARA SISTEM/AGEN ELEKTRONIK (pas. 15(3), dan pas 21 (5))

- Penyelenggara dapat dilepaskan dari tanggung jawab atas kerugian yang timbul apabila dapat membuktikan :

1. Terjadinya keadaan memaksa
2. Kesalahan dan/atau
3. Kelalaian pihak pengguna sistem elektronik

TUGAS

- Resume
- Kebebasan Berekspresi Vs. Pornografi di Internet

  * Sensorship = *control of access & ownership?* = Perlukah pengaturan Hukum?

ASPEK HUKUM PERLINDUNGAN DATA DAN HAK PRIBADI

PERLINDUNGAN PRIVASI DATA PRIBADI

- Apa yang di maksud dengan Privacy?
- Apa yang di maksud dengan perlindungan data?

Keberadaan Informasi dalam Era Informasi dan Masyarakat

- Era Informasi dan Masyarakat Informasi
- Etika Informasi

a. *Privacy*
b. *Accuracy*
c. *Property*
d. *Acessibility*

PENGERTIAN PRIVASI DATA PRIBADI

- Alan F Westin :

Privasi = *"Claim of individuals, groups or institution to determine for themselves when, how, and to what extent information about them is communicated to others"*

Unsur Utama : Kontrol atas Informasi

Konsepsi Umum Perlindungan Privasi

- Aspek Privasi :
  1. *Privacy of a Persons persona*
  2. *Privacy of Data about Person*
  3. *Privacy of a Person's Communications*

Pentingnya Perlundungan Hukum atas Privacy (*Online Privacy)*

- Liu & Maes :2005

"Well iver a milion self – descriptive personal profiles are available across different web-based social cetworks in the US

Pengertian Data dan Data Pribadi Pas.1 (1) Data Protection Act Inggris, 1998

- "Data" = setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang di berikan bai tujuannya dan di simpan dengan maksud untuk dapat di proses
- "Data Pribadi" = data yang berhubungan dengan seorang indibidu yang hidup yang dapat diidentifikasikan dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh data controller

Privasi Data Pribadi dalam Situs Internet

- Cara Situs Internet mengumpulkan data Pribadi :
  a. Cookies
  b. Pendaftaran (on-site registration)
  c. Perdagangan Online
  d. Website Database
- Tujuan pengumpulan data oleh situs Internet:
  a. Untuk meningkatkan perlayanan
  b. Sebagai Komoditas
  c. Sebagai aset Perusahaan

Perlindungan Hukum Privasi data Pribadi dalam Situs Internet

A. Dalam Peraturan Perundang-undangan

I. Directive 95/46/EC of the parliament and the council on the protection of individual with regard to the processing of personal data

II. Data Protection Act 1998 Inggris

III. US Privacy Act 1974 dan UU lainnya

A. *Self Regulation/Privacy Policy/Privacy Statement*

EUROPEAN UNION DATA PROTECTION

Tujuan dari Directive

- Pasal 1

Untuk melindungi hak-hak dasar dan kebebasan dari setiap orang khususnya hak atas privasi dalam kaitannya dengan pemrosesan data pribadi

Ruang Lingkup

- Pengeolahan data pribadi baik secara keseluruhan ataupun sebagian dengan alat otomatik
- Directive ini tidak dapat diterapkan pada dua hal yaitu terhadap masalah keamanan nasional dan Undang-Undang tindak pidana dan mengenai pengolahan data pribadi yang dilakukan oleh orang (pribadi kodrati) dalam kegiatan murni untuk kepentingan pribadi

Perlindungan Dasar

- Informasi yang harus di berikan kepada subjek data
- Akses untuk dan kesempatanuntuk memperbaiki data pribadi
- Kerahasiaan dan keamanan pengolahan data
- Pendaftaran kegiatan pengolahan data
- Tanggung jawab dan ganti rugi
- Larangan Pengiriman data ke luar negeri

Prinsip-Prinsip Perlindungan Data

- Diproses secara jujur dan sah
- Dikumpulkan untuk tujuan-tujuan yang spesifik, eksplisit dan sah
- Pengumpulan data harus sesuai relevan dan tidak berlebih-lebihan
- Data harus akurat dan jika perlu harus *up to date*
- Data tidak disimpan lebih lama dari yang diperlukan sesuai dengan tujuan pengumpulan dan pemrosesannya

Prinsip-Prinsip Perlindungan Data

- Data pribadi harus diperoleh secara jujur dan sah
- Data pribadi harus dimiliki hanya untuk satu tujuan atau lebih yang spesifik dan sah
- Data pribadi harus layak, relevan dan tidak terlalu luas
- Data pribadi harus akurat dan selalu up to date
- Data pribadi harus di proses sesuai dengan tujuannya
- Data pribadi harus sesuai dengan hak-hak dari subjek data
- Tindakan-tindakan pengamanan yang memadai
- Data pribadi tidak boleh di kirim ke negara atau wilayah lain di luar wilayah Ekonomi Eropa

Data Protection Act 1998 Inggris

Hak-Hak Subjek Data

- Untuk mengakses informasi, mencegah pemrosesan yang dapat menyebabkan kerusuhan
- Untuk meminta kompensasi
- Hak untuk mengambil tindakan membatasi, menghalang-halangi, menghapus atau menghancurkan data yang tidak akurat
- Meminta Commissioner untuk membuat penyelesaian terhadap tindakan yang melanggar ketentuan dalam undang-undang ini

Pengecualian-Pengecualian

- Keamanan nasional'
- Kejahatan
- Perpajakan
- Kesehatan
- Pendidikan
- Kerja Sosial

Self Regulation

- Ada beberapa Model dari Self Regulation :

a. Fair information practice Principles – federal trade commission AS prinsip-prinsip dasar mengenai perlindungan privasi :

   1. Notice/awareness (pemberitahuan/kesadaran)
   2. Chocice/Consent (Pilihan/Persetujuan)
   3. Access/Participation (Akses/Partisipasi)
   4. Integrity/Security (Integritas/Keamanan)
   5. Enforcement/Redress (Penerapan/Perbaikan)

Isi Privacy Policy

- Informasi pribadi apa saja yang dikumpulkan oleh situs
- Bagaimana pengorganisasian pengumpulan informasi
- Bagaimana informasi tersebut akan digunakan
- Kepada siapa informasi tersebut akan di bagikan
- Pilihan-pilihan apa saja yang dimungkinkan bagi setiap subjek data berkenaan dengan pengumpulan serta mendistribusikan informasi tersebut
- Prosedur pengamanan yang ditempatkan untuk melindungi kehilangan, penyalah gunaan informasi yang berada dalam kontrol situs
- Bagaimana cara membetulkan informati yang tidak akurat

Perlindungan Data Pribadi

- Tidak ada omnibus law
- US Privacy Act 1974
- Undang-undang lainnya

1. The Federal Cable communication Policy act
2. The Family Educational Right & Privacy Act
3. The Video Privacy Protection Act

Self Regulation

- The Online Privacy Alliance
- Seal Programs

1. TRUSTe
2. BBBOnline Privacy Seal Program

Self Regulation/Privacy Policy/Policy –Statement

Perjanjian antara operator situs dan Pengunjung = Klausula Baku

Perlindungan Privasi Data Pribadi di Indonesia

- UU No.7 Tahun 1971 tentang Ketentuan –ketentuan Pokok Kearsipan

Arsip dalam "…bentuk corak apapun…"

- UU No. 8 Tahun 1997 tentang Dokumen Perusahaan

Pasal 1 : Dokumen perusahaan adalah data, catatan dan atau keterangan yang dibuat dan atau di terima oleh perusahaan dalam rangka pelaksanaan kegiatannya baik tertulis di atas kertas atau sarana lain maupun terekam dalam bentuk corak apapun yang dapat dilihat, dibaca atau di dengar

Perlindungan Privasi Data Pribadi di Indonesia

- UU No 39 Tahun 1999 tentang Hak Asasi Manusia

  Pasal 14 (2) dinyatakan bahwa salahsatu hak mengembangkan diri adalah hak untuk mencari, memperoleh, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia

- UU No 10 Tahun 1998 tentang Perbankan

  Berkenaan dengan masalah rahasia bank, berdasarkan Pasal 40 Undang-Undang Nomor 10 Tahun 1998, Bank di wajibkan untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya

Perlindungan Privasi Data Pribadi di Indonesia

- UU No,23 Tahun 1992 tentang Kesehatan

  Pasal 52 ayat (2) : Tenaga kesehatan dalam melakukan tugasnya berkewajiban untuk mematuhi standar profesi dan menghormati hak pasien

- UU No. 36 Tahun 1999 tentang Telekomunikasi

  Pasal 22 : Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sahm atau manipulasi (a) akses ke jaringan telekomunikasi dan atau (b) akses ke jasa telekomunikasi dan atau (c) akses ke jaringan telekomunikasi khusus

Pasal 42 (1) : Penyelenggara jasa telekomunikasi wajib untuk merahasikan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang di selenggarakannya

UU ITE

- Pasal 26

1) Kecuali ditentukan lain oleh Peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan
2) Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini

Penjelasan Pasal 26

- Pemanfaatan Teknologi Informasi, Perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy right)*
- Hak pribadi mengandung pengertian sebagai berikut:

  1. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan

  2. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan mematamatai

  3. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang

CASE – FACEBOOK – BEACON CASE

- *A class acrion lawsuit filed in August 2008 againts facebook by several users of the social networking site*
- *The suit alleged that facebook and beacon affiliates such as blockbuster and overstock.com had biolated several federal privacy laws, including the electronic communicationn privacy act, when they shared data about facebook users with each other*
- *A federal judge has approved a proposed settlement by facebook under wich it saidit would spend $9,5 Million to set up a privacy foundation docused on online privacy issues as part of its settlement offer, facebook said it would shut down the beacon service entire*

Case - Facebook

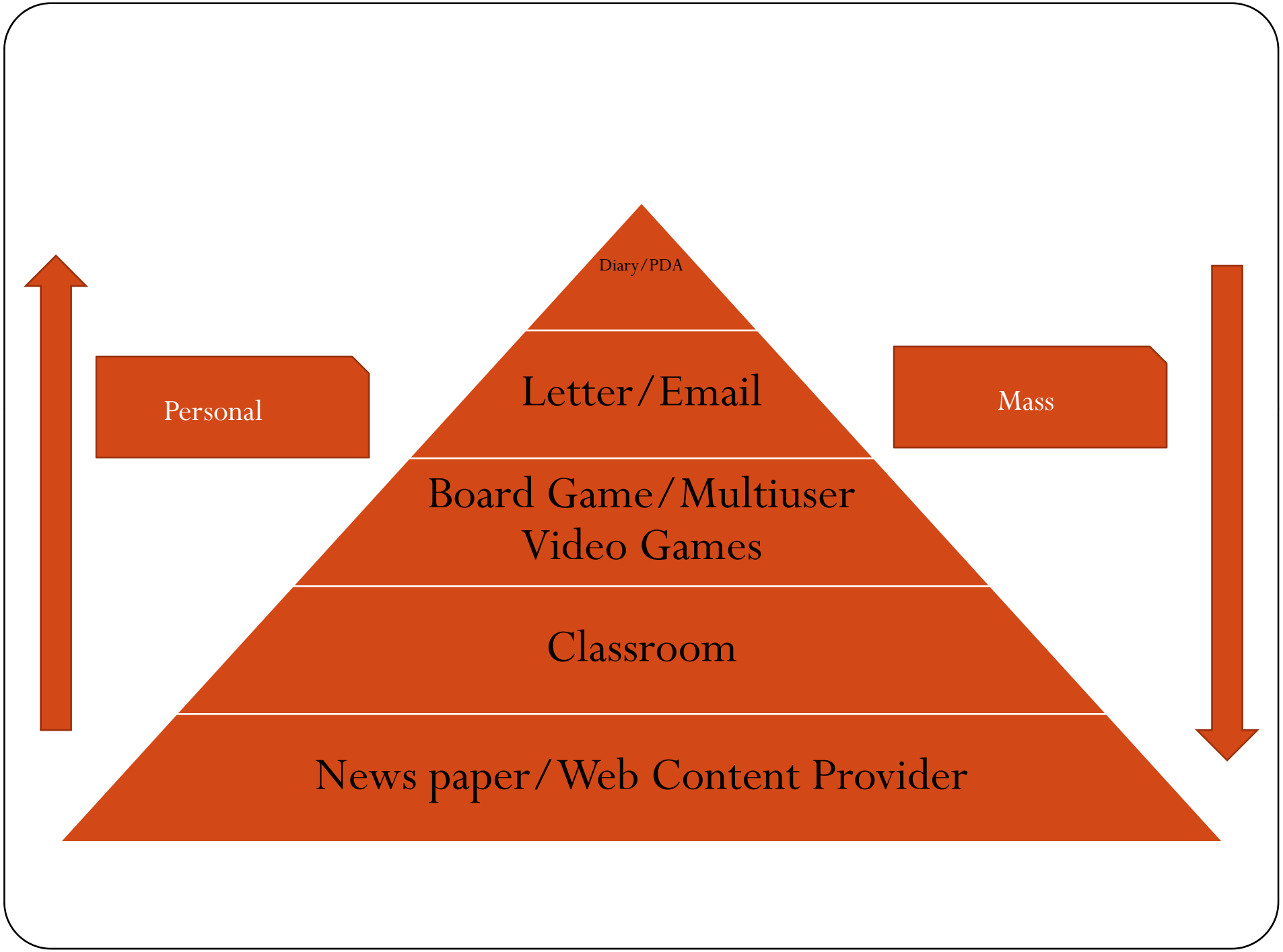
- Tahun 2009 facebook mengubah privacy policy sehingga pengguna boleh menghapus akunnya tetapi facebook masih tetap berhak mengolah akun yang ada
- Protes dari komisi privasi di kanada
- New Privacy policy : *You have the right to delete or change your profile information, that you can delete your entire account from facebook's servers, that there are limitations to removal and that backup coples can exist for up to 90 days after deleting*

Tugas

- Pelajari UU ITE, apakah yang di maksud dengan Penyelenggara Sertifikasi Elektronik dan Sertifikasi Keandalan. Jelaskan perbedaannya
- Jelaskan keterkaitan sertifikasi keadndalan dengan isu Privacy serta perlindungan hak konsumen

ASPEK HUKUM MEDIA DI INTERNET

Informasi dan Komunikasi


Diary/PDA
Letter/Email
Board Game/Multiuser
Video Games
Classroom
News paper/Web Content Provider
Personal
Mass

Pengertian Komunikasi

- Komunikasi adalah sebuah proses interaksi untuk berhubungan dari satu pihak ke pihak lainnya, yang pada awalnya berlangsung sangat sederhana dimulai dengan sejumlah ide-ide yang abstrak atau pikiran dalam otak seseorang untuk mencari data atau menyampaikan informasi yang kemudian dikemas menjadi sebentuk pesan untuk kemudian disampaikan secara langsung maupun tidak langsung menggunakan bahasa berbentuk kode visual, kode suara atau kode tulisan

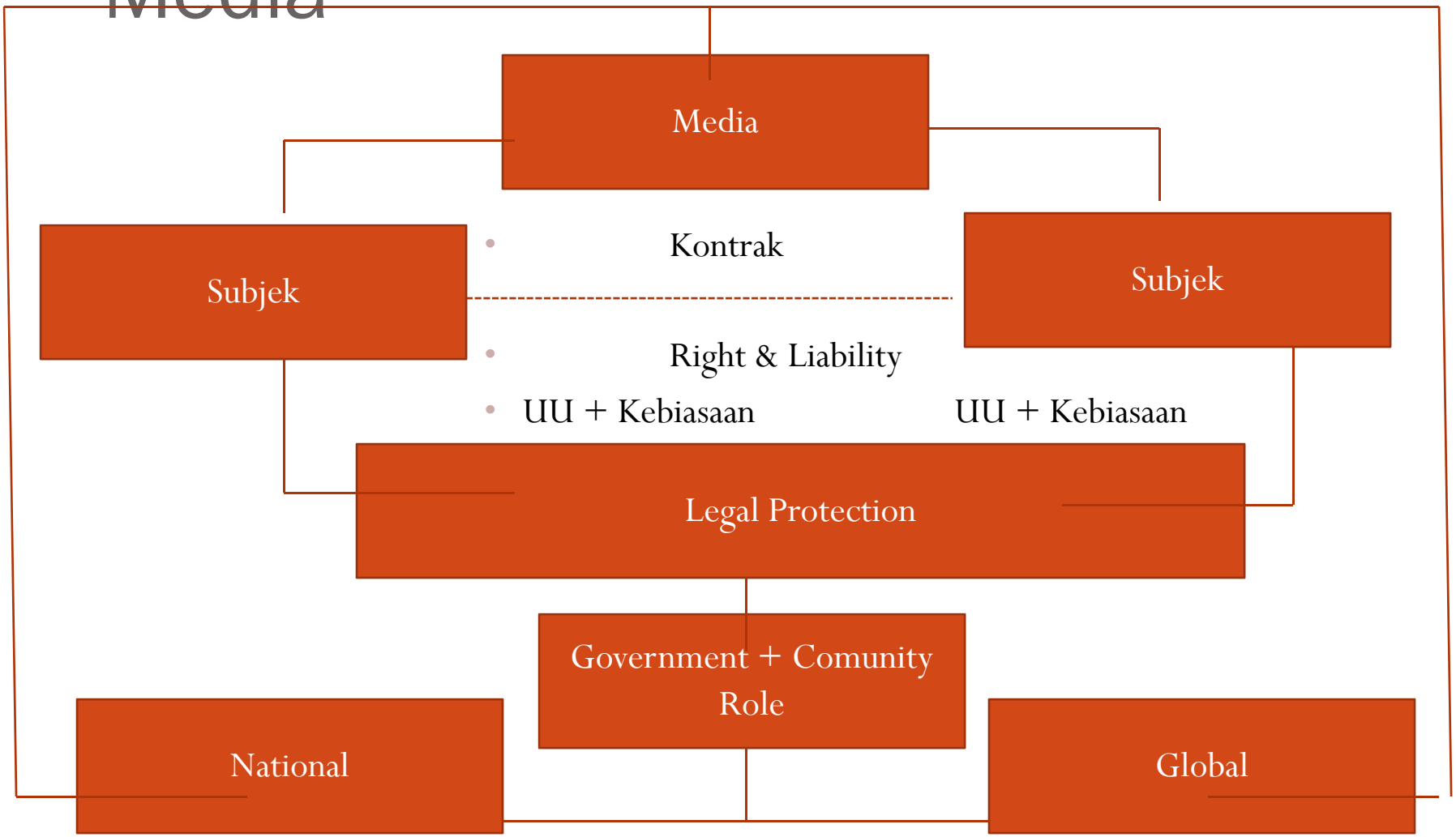
Komponen Komunikasi

- Komunikator
- Pesan
- Media
- Komunikan
- Efek

Media

- Media adalah suatu penghantar informasi yang bersifat netral
- Media adalah laksana ruang bagi publik untuk menyampaikan informasi baik fakta, informasi, pendapat maupun opini
- Sementara informasi adalah hasil intelektual seseorang yang tentu saja bersifat subjektif
- Sejauhmanakah pertanggung jawabanpihak yang menyelenggarakan suatu media sebagai alat komunikasi masa?

Media


Media
Subjek
Kontrak
Subjek
Right & Liability
UU + Kebiasaan
UU + Kebiasaan
Legal Protection
Government + Comunity Role
National
Global

Jenis Komunikasi

- Media Cetak : UU No 40/1999 : Pers
- Media Elektronik : Penyiaran UU No 32/2003
- Media Telekomunikasi : UU No 39/1999
- Media Film : UU No 8/1982
- Internet : UU No 11/08 ITE

PRINSIP-PRINSIP HUKUM

- Prinsip Demokrasi

  Bahwa pers dalam memberikan atau menyiarkan suatu informasi, memperhatikan terlebih dahulu kepentingan umum

- Prinsip Keadilan

  Mendatangkan atau mengetengahkan rasa keadilan yang ada dalam masyarakat

- Prinsip Supremasi Hukum

  Segala sesuatunya dilakukan berlandaskan pada hukum yang berlaku sah di negara Indonesia

- Kejujuran, Itikad baik & Kehati-hatian?

Kebebasan Eks. Dan Fungsi Media

Konstitusi & HAM	Fungsi Media
First Amandement Freedom of Speech and press = expression and action = hierarchy of protected communicative conduct = Unprotected class = unfree-speech	Berdasarkan UU Fungsi Penyampai Informasi Fungsi Pendidikan Fungsi hiburan
▪ Fighting words ▪Obscenity ▪Publication of state secret ▪Incitement to crime ▪Defamation ▪Subliminal communication ▪Commercial speech = legal framework = procedural approaches	Fungsi Kontrol Sosial dan Perekat Sosial Fungsi Pengembangan Budaya Fungsi Lembaga Ekonomi Di Luar UU Fungsi agenda setting Fungsi agent of reform

PENGATURAN KODE ETIK

- UU No 40/1999 mengamanatkan Pembentukan Dewan Pers:

- Fungsi Dewan Pers :

  1. Melindungi kemerdekaan pers dari campur tangan pihak lain
  2. Melakukan pengkajian dan pengembangan kehidupan Pers
  3. Penetapan dan Pengawas pelaksanaan kode etik
  4. Memberi pertimbangan dan mengupayakan penyelesaian pengaduan masyarakat
  5. Memfasilitasi organisasi pers dalam menyusun peraaturan-peraturan di bidang pers dan meningkatkan kualitas profesi kewartawanan

Kode Etik Wartawan Indonesia

- Kemerdekaan pers merupakan sarana terpenuhinya HAM untuk berkomunikasi dan memperoleh informasi. Dalam mewujudkan kemerdekaan pers, wartawan Indonesia menyadari adanya tanggung jawab sosial serta keberagaman masyarakat. Guna menjamin tegaknya kebebasan pers serta terpenuhinya hak-hak masyarakat diperlukan suatu landasan moral/etika profesi yang bisa menjadi pedoman operasional dalam menegakan integritas dan profesionalitas wartawan. Atas dasar itu wartawan Indonesia menetapkan kode etik
- Wartawan Indonesia menghormati hak masyarakat untuk memperoleh informasi yang benar
- Wartawan Indonesia menempuh tatacara yang etis untuk memperoleh dan menyiarkan informasi serta memberikan identitas kepada sumber informasi

- Wartawan Indonesia menghormati asas praduga tak bersalah, tidak mencampurkan fakta dengan opini, berimbang dan selalu meneliti kebenaran informasi serta tidak melakukan plagiat
- Wartawan Indonesia tidak menyiarkan informasi yang bersifat dusta, fitnah, sadis, dan cabul serta tidak menyebut identitas korban kejahatan susila
- Wartawan Indonesia tidak menerima suap dan tidak menyalahkan profesi
- Wartawan Indonesia memiliki hak tolak, menghargai ketentuan embargo informasi latar belakang dan off the record sesuai kesepakatan
- Wartawan Indonesia segera mencabut dan meralat kekeliruan dalam pemberitaan serta melayani hak jawab
- Pengawasn dan Penetapan sanksi atas pelanggaran kode etik ini sepenuhnya diserahkan kepada jajaran pers dan dilaksanakan oleh organisasiyang dibentuk untuk itu

Jenis	Pasal	Sanksi Maksimal
Penghinaan	310 dst	9 bln
Pengaduan Fitnah	317	4 th
Penghinaan terhadap kepala negara dan wakil	134,136 bis 142,143	6 th
Penghinaan terhadap golongan tertentu	56	5 th
Penghinaan terhadap pemerintah	154	7 th
Penghinaan terhadap penguasa umum	207	1 th 6 bln
Penghinaan terhadap agama tertentu	156a	5 th
Penghasutan	160	6th
Penawaran Kejahatan	161	4th
Pembocoran Rahasia Negara	112	7th
Pembocoran Rahasia Biasa	322	9 bln
Pornografi	282	1 thn 6 bl
Penyiaran Kabar Bohong	14 UU No.1/1946	

Penyiaran 32/2002	Telekomunikasi 36/1999
Penyiaran adalah kegiatan pemancarluasan siaran melalui sarana pemancaran dan/atau sarana transmisi di darat, di laut atau di antariksa dengan menggunakan spektrum frekuensi radio melalui udara, kabel dan atau media lainnya untuk dapat diterima secara serentak dan bersamaan oleh masyarakat dengan perangkat penerima siaran (Negara menguasai spektrum frekuensi radio yang digunakan untuk penyelenggaraan	Telekomunikasi adalah setiap alat, pemancaran, pengiriman atau penerimaan tiap jenis tanda, gambar, suara dan informasi dalam bentuk apapun melalui sistem kawat, optik, radio atau sistem elektromagnetik lainnya.
penyiaran guna sebesar besarnya kemakmuran rakyat) 1. Jasa Penyiaran terdiri atas Radio & TV 2. Penyelenggaraan jasa penyiaran : a. Lembaga penyiaran Publik b. Lembaha penyiaran swasta c. Lembaga Penyiaran Komunitas d. Lembaga penyiaran berlangganan	Penyelenggaraan telekomunikasi meliputi : a. Jaringan telekomunikasi b. Jasa telekomunikasi c. Telekomunikasi khusus = penyiaran

KPI

Kewenangan	Tugas dan Kewajiban
• Menetapkan standar program siaran •Menyusun peraturan dan menetapkan pedoman perilaku penyiaran •Mengawasi pelaksanaan peraturan dan pedoman perilaku penyiaran serta standar program siaran	• Menjamin masyarkat untuk memperoleh informasi yang layak dan benar sesuai dengan Hak Asasi Manusia •Ikut membantu pengaturan infrastruktur bidang penyiaran •Ikut membangun iklim persaingan yang sehat antar
•Memberikan sanksi terhadap pelanggaran peraturan dan pedoman perilaku penyiaran serta standar program siaran •Melakukan kooridinasi dan atau kerjasama dengan pemerintah, lembaga penyiaran dan masyarakat	lembaga penyiaran dan industri terkait •Memelihara tatanan informasi nasional yang adil, merata dan seimbang •Menampung meneliti danmenindak lanjuti adua, sanggahan, serta kritik dan apresiasi masyarakat terhadap penyelenggaran penyiaran •Menyusun perencanaan pengembangan sumber daya manusia yang menjamin profesionalitas di bidang penyiaran

UU NO 32/2002 tentang Penyiaran

- Salah satu pokok pikiran

3. …harus mempertimbangkan penyiaran sebagai lembaga ekonomi yang penting dan strategis baik dalam skala nasional maupun internasional

7. …untuk meningkatkan daya tangkal masyarkat terhadap pengaruh buruk nilai budaya asing

- Salah satu arah penyiaran

  G. Mencegah monopoli kepemilikan dan mendukung persaingan yang sehat di bidang penyiaran

- Salah satu kewenangan KPI

  pasal 2 (a) standar program siaran

PP 49-52/2005

- Ketentuan umum
- Pendirian dan Perizinan
- Penyelenggaraan Penyiaran
- Permodalan
- Pembatasan Kepemilikan Silang
- Rencana dasar teknik dan persyaratan teknis perangkat penyiaran dan
- Sanksi administratif serta
- Ketentuan peralihan yang mengatur mengenai Lembaga penyiaran yang telah ada sebelum berlakunya peraturan pemerintah ini

Konsentrasi Kepemilikan & Kepemilikan SIlang

- Pemusatan kepemilikan dan penguasaan Lembaga Penyiaran Swasta oleh satu orang atau satu badan hukum, baik di satu wilayah siaran maupun di beberapa wilayah siaran, dibatasi
- Kepemilikan silang antara Lembaga Penyiaran Swasta yang menyeleggarakan jasa penyiaran radio dan lembaga penyiaran swasta yang menyelenggarakan jasa penyiaran televisi, antara lembaga penyiaran swasta dan perusahaan media cetak serta jasa penyiaran lainnya baik berlangsung maupun tidak berlangsung
- Pengaturan jumlah dan cakupan wilayah siaran lokal, regional dan nasional baik untuk jasa penyiaran radio maupun jasa penyiaran televisi, disusun oleh KPI bersama pemerintah
- Pada saat ini didirikan 100% lokal, namun setelah izin prinsip boleh asing maksimal 20% dari modal yang ditempatkan dan telah disetor penuh (Setiap perubahan 5% ada laporan kepada Menteri)

Mengapa Harus Dibatasi

- Pemodal akan mempengaruhi/merefleksikan perspektif Politik dan Ekonomi
- Iklan niaga maksimal 20% iklan layanan masyarakat minimal 10%
- Berita Lokal vs impor = 60% : 40%
- Jatah Mata Acara domestik 80% : 20%
- Kepentingan ekonomi nasional? Maksimal 20% asing

PP 50/2005 Penyelenggaraan Penyiaran LPS

- Pasal 33

Ketentuan ini dimaksudkan agar Lembaga Penyiaran Swasta tidak memiliki 3 (tiga) jenis media masa sekaligus yakni radio, telebisi dan media cetak dengan kepemilikan saham pada masing-masing lembaga penyiaran dan perusahaan media cetak tersebut sebesar 25% atau lebih atau dibawah 25% tetapi bertindak sebagai pengendali pada masing-masing lembaga penyiaran dna perusahaan media cetak tersebut. Sehingga lembaga penyiaran swasta dimaksud tidak dapat memonopoli opini publik

Bagaimana dengan Internet

Internet sebagai media massa atau media komunikasi?

- Revolusi teknologi informasi = konvergensi telekomunikasi dan media (media cetak dan media elektronik/penyiaran)
- Timbulnya berbagai bisnis media massa di internet
- Selain itu lembaga penyiaran dan produsen film juga penggunaan internet untuk aktivitas bisnis mereka
- Timbul individual jurnalisme vs capitalism Jurnalism
- Perkembangan bidang hukum yang mengatur konten internet

Tugas

- Resume

KAJIAN ASPEK PIDANA

URGENSI UU ITE

- Selain nilai positif yang dapat di ambil dari kemajuan perkembangan teknologi yang semakin konvergen antara perkembangan teknologi informasi, media dan telekomunikasi (telematika) ternyata hal tersebut juga di barengi dengan tindakan penyalahgunaan yakni untuk melakukan kejahatan
- Dengan dalih "legalitas" hukum yang telah berlaku di anggap tidak cukup jelas atau bahkan tidak adil dalam konteks perkembangan telematika dan *cyberspace*
- Selain merumuskan ketentuan hukum yang khusus maka dalam menjawab 'keadilan' kita tetap harus mengoptimalkan hukum yang telah ada

Apa, Mengapa & Bagaimana HK Pidana diperlukan dalam *cyberspace*

- Mengapa harus di lindungi ? Karena demi kepentingan publik
- Apa yang harus di lindungi? Kepentingan hukum (Pribadi, masyarakat atau bangsa) terhadap keberadaan suatu sistem informasi/telekomunikasi yang baik (terjaganya keutuhan sistem informasi & keamanan infrastruktur (*security & integrity))*
- *Bagaimana ia dilindungi?*

1. *serangan* (attack)
2. *Penyusupan (intruder) atau*
3. *Penyalah gunaan (misuse/abuse)*

- *Bagaimana melindunginya?*

  Perlu perlindungan secara teknis, manajemen dan hukum

Kepentingan Hukum Publik

- Secara garis besar kepentingan hukum terhadap sistem elektronik mencakup:

1. Kepentingan hukum untuk memperoleh kekuatan pembuktian terhadap informasi elektronik (*validity of eleectronic evidence)*
2. Kepentingan hukum untuk memperoleh penyelenggaraan sistem elektronik yang baik (akuntabilitas) dengan cara penerapan prinsip upaya yang terbaik (best practice) dalam penerapan teknologi
3. Kepentingan hukum untuk memperoleh perlindungan hukum terhadap penyelenggaraan Sistem Elektronik tersebut sehingga ada kewajiban terhadap setiap pembuat dan pengguna yang memperoleh manfaat untuk tidak melakukan tindakan yang bertentangan denganhukum,

- *protect works*
- *Protect computing*
- *Protect comunication*
- *Protect comunity*

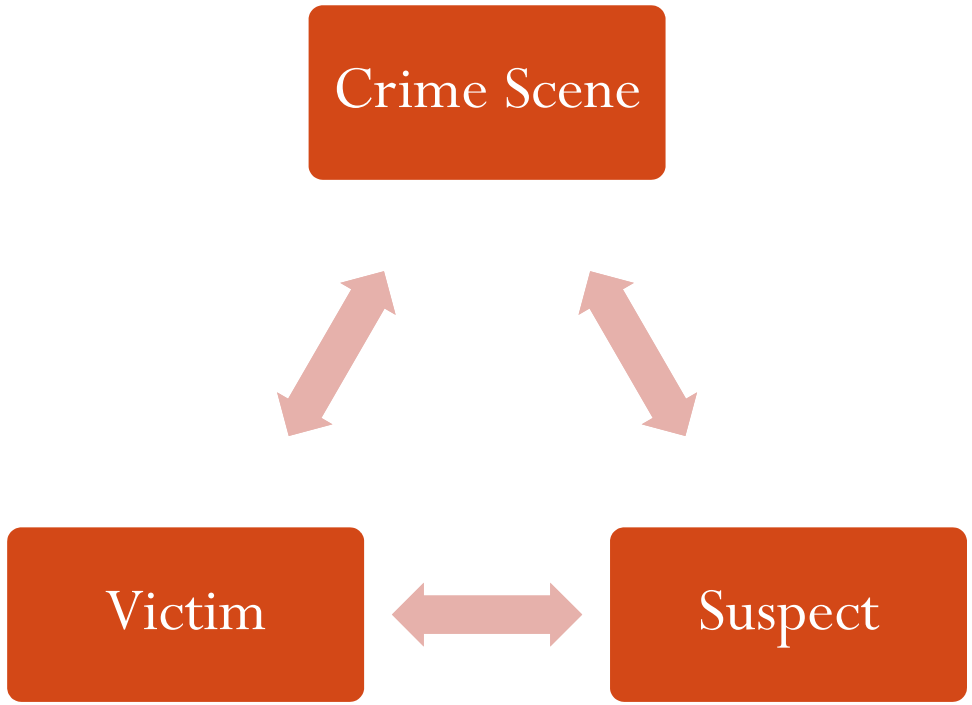
Potensi Pidana Para Pihak

Segala macam tindakan yang dilakukan dengan sengaja dan melawan hukum terhadap informasi dan/atau sistem informasi elektronik dapat dilakukan oleh:

- Si pengguna (*user crime)* = tanpa hak atau bertindak, diluar kewenangannya untuk mengakses, menggunakan, mengubah, menggandakan, mengumumkan atau dll
- SI pengembang/pembuat (*developers crime)*= membuat informasi atau sistem yang bersifat melawan hukum dan/atau berdampak merugikan orang lain
- Si penyelenggara (*Providers crime)*= menyelenggarakan sistem elektronik (sebagai suatu media) yang bersifat melawan hukum

KETERKAITAN KOMPUTER DENGAN TINDAK PIDANA

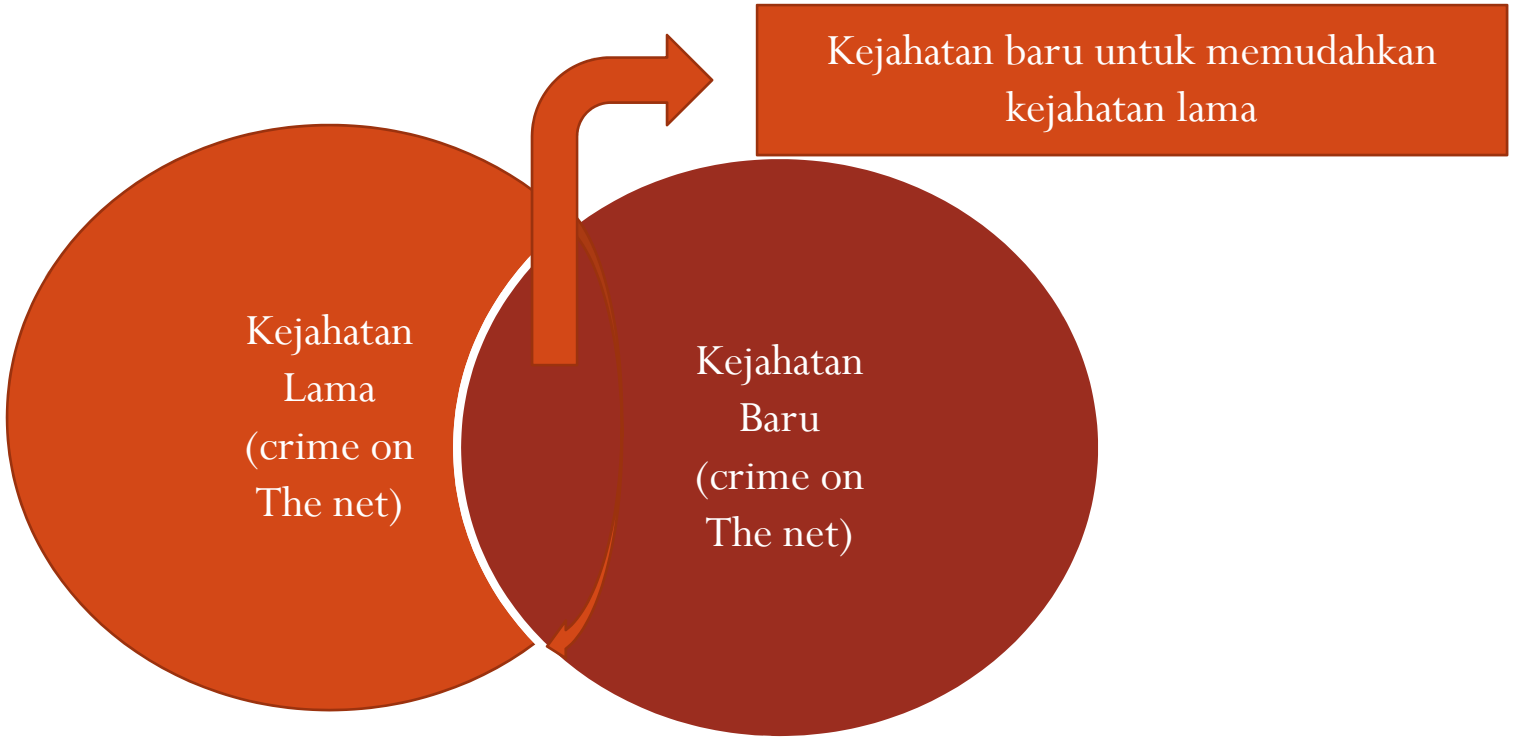
1. *Computer as a tool*
2. *Computer as an Object*
3. *Computer as a storange device*



Computer as a tool

- Pada dasarnya adalah bentuk perkembangan dari old crimes, misalkan : Fraud, Child Pornography, IPR Violations, Money Laundring, sale illegal, etc

Kejahatan baru atau kejahatan lama?



- Kejahatan Biasa (*offline*)

Computer as a target

- Dikenal juga dengan sebutan “network crime”
- Secara umum ada 2 hal perbuatan yang dilakukan :

1. Menggunakan, memperoleh, mengumumkan, menyimpan atau mengubah informasi tanpa hak
2. Menyebabkan kerusakan pada sistem komputer

Computer as a Storage Device

- Intinya hanya menggunakan komputer untuk menyimpan data yang penting mengenai hal-hal yang berhubungan dengan suatu kejahatan
- Misal :

  1. Mafia peredaran Narkoba Internasional

  2. Menyimpan data mengenai nama-nama yang berhubungan dengan mata rantai organisasi atau untuk kepentingan money laundering

Pengertian Cyber Crime

- Cybercrime in a narrow sense (computer crime) : any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them
- Cybercrime in a broader sense (computer related crime) : any illegal behaviour committed by means on in relation to a computer system or network, including such distributing information by means of a computer system or network

Cybercrime meliputi kejahatan, yaitu yang dilakukan:

- Dengan menggunakan sarana dari sistem atau jaringan komputer
- Di dalam sistem atau jaringan komputer
- Terhadap sistem atau jaringan komputer

Pidana Umum ataukah Tertentu?

Perhatikan definisi UU yang terkait antara lain:

- Telekomunikasi adalah setiap pemancaran, pengiriman, dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat,optik, radio atau sistem elektromagnetik lainnya;
- Penyiaran adalah kegiatan pemancarluasan siaran melalui sarana pemancaran dan/atau sarana transmisi di darat, di laut, di antariksa dengan menggunakan spektrum frekuensi radio melalui udaram kabel, dan/atau media lainnya untuk dapat diterima secara serentak dan bersamaan oleh masyarakat dnegan perangkat penerimaan siaran

- Pers : Lembaga sosial dan wahana komunikasi masa yang melaksanakan kegiatan jurnalistik meliputi mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi baik dalam bentuk tulisan, suara, gambarm suara dan gambar, serta data dan grafuk maupun dalam bentuk lainnya dengan menggunakan media cetak, media elektronik dan segala jenis saluran yang tersedia
- Film adalah karya cipta seni dan budaya yang merupakan media komunikasi massa pandang-dengar yang dibuat berdasarkan sinematografi dengan direkam pada pita seluloid, pita video, piringan video, dan/atau bahan hasil penemuan teknologi lainnya dalam segala bentuk, jenis dan ukuran melalui proses kimiawi proses elektronik atau proses ainnya denganatau tanpa suara yang dan/atau ditaaangkan dengan sistem proyeksi mekanik elektronik dan/atau lainnya

PIDANA UMUM

- Pencurian (Pasal 362 KUHP)
- Penipuan (Pasal 378 KUHP)

PIDANA TERTENTU/KHUSUS I

- Akses Tidak Sah (Pasal 22 UU No.36/1999)
- Ketentuan Pidana Telekomunikasi (Pasal 50 UU No.36/1999)
- Pasal 38 Pengamanan Telekomunikasi

PIDANA TERTENTU/KHUSUS 2

- Pelanggaran hak Moral

  Attribution = Identitas Pencipta

  Integrity= Integritas/Keutuhan Ciptaan
- Pelanggaran Hak Ekonomis

  Memperbanyak

  Mengumumkan
- Merusak Sarana Kontrol Teknologi
- Merusak Informasi Manajemen Hak Cipta

UU No 32/2004 (Penyiaran)

- Pasal 35
- Pasal 36

UU No.40/1999 tentang Pers

- Pasal 5
- Pasal 18 (2)

TUGAS

- Resume

KAJIAN HUKUM INTERNASIONAL

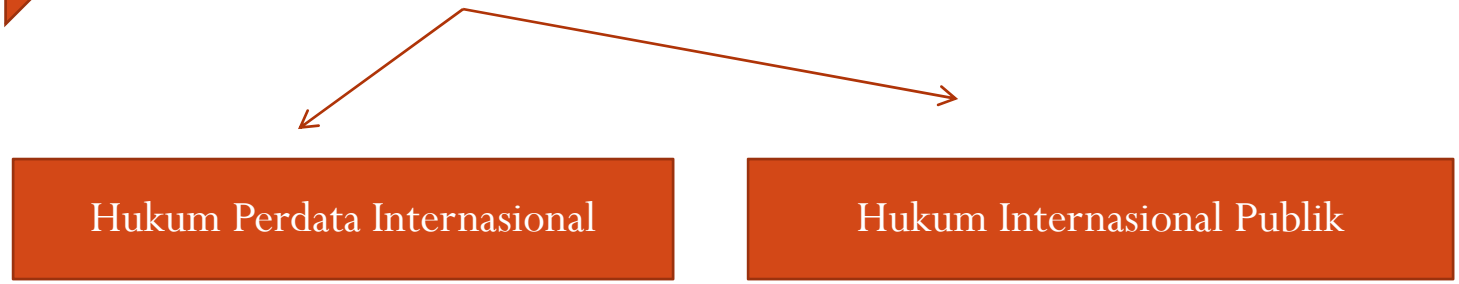
Konsepsi Umum tentang hukum internasional

- Definisi Hukum Internasional

Hukum yang berlaku dalam hubungan atau persoalan yang melintasi batas negara

Hendry R. Cheeseman " *Law that governs affairs between nations and regulates transactions between individual and business of different countries*"

Mochtar Kusuma Atmadja



Hukum internasional publik

- Starke :

  Hukum Internasional : "*Body of law wich is composed fo its greater part of the principles and rules of conduct wich states feel themselves bound to observe and therefore, do commonly observe in their relation with each other*"

- Unsur-Unsur :

  1. Kaidah-kaidah hukum yang berkaitan dengan berfungsinya lembaga-lembaga atau organisasi-organisasi internasional, baik mengenai hubungan mereka antara satu dengan yang lainnya, maupun hubungan mereka dengan negara-negara atau individu-individu

  2. Kaidah-kaidah hukum tertentu yang merupakan hubungan antara lembaha organisasi internasional baik dengan individu-individu maupun dengan badan-badan non negara sejauh hak-hak dan kewajiban individu dan badan non negara tersebut terlalu penting bagi masyarakat internasional

YURISDIKSI DALAM LINGKUP HUKUM INTERNASIONAL PUBLIK

- Yurisdiksi Pengatur

  Kemampuan suatu negara untuk menerapkan ketentuan hukumnya

- Yurisdiksi Pemaksa

  Ketentuan dimana suatu negara memiliki kekuasaan di bawah hukum internasional untuk mengatur hukum nasionalnya dan memaksakan yurisdiksi tersebut selama berada di wilayah teritorialnya

YURISDIKSI DALAM LINGKUP HUKUM PERDATA INTERNASIONAL

- Yurisdiksi Teritorial

  Pelaksanaan yurisdiksi oleh suatu negara terhadap harta benda, orang, tindakan/peristiwa yang terjadi dalam wilayahnya

a. Teritorial Objektif : negara akan menerapkan yurisdiksi terhadap pelanggaran yang diselesaikan dalam wilayah teritorialnya walaupun ada elemen-elemen dari pelanggaran tersebut yang di lakukan di negara asing
b. Teritorial subjektif : Yurisdiksi yang diterapkan terhadap semua pelanggaran atau hal-hal yang terjadi dalam wilayah teritorial suatu negara, walaupun beberapa elemen atau penyelesaian di selesaikan di negara lain

- Yurisdiksi terhadap Nasionalitas : pada dasarnya yurisdiksi ini tergantung pada kewarganegaraan atau seseorang yang berada dalam kekuasaan suatu negara.

  1. Nasionalisme Aktif : Suatu negara dapat melaksanakan yurisdiksinya terhadap Warga Negaranya dimanapun ia berada

  2. Nasionalisme Pasif : dimana negara hanya dapat menjalankan yurisdiksinya apabila warga negaranya menerima kerugian
- Yurisdiksi menurut prinsip Perlindungan : suatu negara boleh menerapkan yurisdiksinya terhadap orang asing atau tindakan-tindakan yang dilakukan di luar wilayah teritorialnya yang menyebabkan gangguan keamanan terhadap negara tersebut
- Yurisdiksi Menurut Prinsip Universal, dimana di dasarkan atas adanya kejahatan tertentu yang dianggap sangat merugikan bagi masyarakat internasional sehingga setiap negara di perbolehkan menerapkan yurisdiksinya. Contoh : Perompakan

HUKUM PERDATA INTERNASIONAL

- Sekumpulan kaidah hukum nasional yang dimaksudkan untuk menyelesaikan perkara-perkara yang mengandung unsur asing atau unsur-unsur yang melampaui batas-batas teritorial suatu negara
- Bagaimana menetukan apakah suatu masalah masuk dalam HPI atau bukan?

  Di dasarkan pada titik pertalian.

Titik pertalian primer

- Faktor-faktor yang menciptakan bahwa suatu hubungan menjadi hubungan HPI
- Terdiri dari :

1. Kewarganegaraan
2. Domisili
3. Bendera Kapal
4. Tempat Kediaman
5. Tempat Kedudukan
6. Pilihan Hukum Intern

TITIK PERTAUTAN SKUNDER

- Titik taut penentu yang menentukan hukum mana yang akan di berlakukan
- Terdiri dari :

1. Tempat (situs) suatu benda
2. Tempat perbuatan hukum di lakukan
3. Tempat timbulnya akibat perbuatan Hukum
4. Tempat pelaksanaan perbuatan-perbuatan hukum resmi dan tempat perkara/gugatan di ajukan

INTERNET DAN YURISDIKSI

- Kompleksitas Penerapan Yurisdiksi menurut Gaye l Middleton dan Jpcelyn A Aboud :

  the internet further complicates the aplication of this complex teritoriality based jurisdictional principles because :

1. *Material posted on internet has worldwide audience*
2. *There is an enormous and growing number of internet users internationally*
3. *Its easy to move a website from one jurisdiction to another*
4. *AWebsite can be hosted in one juricdiction but directed at users in another jurisdiction*
5. *Parts of a website may be hosted in one jurisdiction, while other parts of the website are hosted in another jurisdiction and*
6. *Its not always possibel to determine where a website or a user is located*

Karakteristik dan sifat keberadaan website

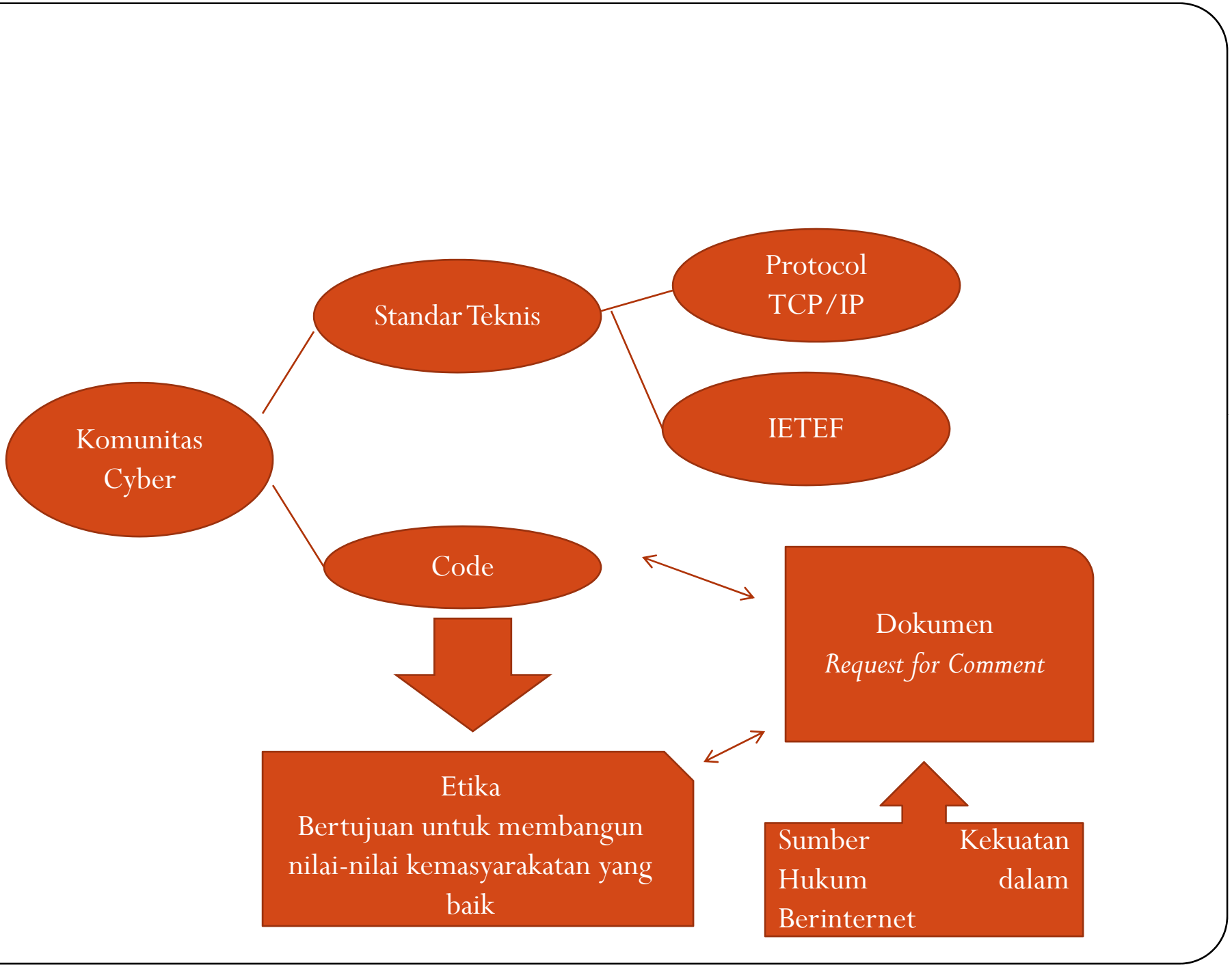
- *Website it self constitutes purposeful availment sufficient for a forum to exercise jurisdiction over a foreign defendant*
- *Website doesnt constitute purposeful abailment by foreign defendant*
- *Website may constitute purposeful availment by a foreign defendant when combined with other act*

Zippo Manufacturing Vs Zippo dot com

- Tepatkan penentuan keberadaan yurisdiksi berdasarkan lokasi server dan/atau sifat dari website jika di kaitkan dengan pelanggaran terhadap hak merek?

KOMUNITAS CYBER VS KEPENTINGAN BANGSA

- Cyberspace = boardless
- Apakah dengan menjadi komunitas *cyber space* berarti kita melepaskan status kewarga negaraan dan tunduk pada ketentuan-ketentuan hukum yang terbangun dalam medium komunitas *cyber*>


Komunitas Cyber
Standar Teknis
Protocol TCP/IP
IETEF
Code
Dokumen
Request for Comment
Etika
Bertujuan untuk membangun nilai-nilai kemasyarakatan yang baik
Sumber Hukum Berinternet
Kekuatan dalam

Tugas

- Resume

Merek Dagang (US)

Menurut U.S. Patent & Trademark Office (PTO)

yang tercantum dalam Lanham Act

Merek dagang di klasifikasikan dalam 5 kategori

- Generic marks →bersifat umum tidak dapat di daftarkan
- Descriptive Marks →tidak akan menerima perlindungan kecuali pendaftar dapat membuktikan ada sifat yang khusus atau telah di kenal dengan pengertian lain di pasaran
- Suggestive marks → yang bersifat mempengaruhi/ mengusulkan
- Arbitrary marks (berdasarkan ketergantungan pada situasi)→ ada tanpa hubungan melekat pada produk
- Fanciful marks (memiliki keanehan/daya imajinasi)→ tidak memiliki hubungan dengan produk

Merek Dagang (US)

C/O: Apple

Apple computer ,Inc dapat mendaftarkan merek dagang Apple, logo buah apel, dan Machintosh, dengan mengaplikasikan kalimat umum terhadap produk yang tidak berhubungan, Apple Computer menciptakan sebuag Image yang Khas.

- → Pasar buah apel tidak dapat mendaftarkan Apel sebagai merek dagang, sebab bersifat sangat umum.
- Descriptive Marks →Apple, adalah sebuah perusahaan yang menjual computer, dapat mendaftarkan Apple sebagai merek dagang karena sudah dikenal sebagai merek dagang sebuah computer.
- Sugestive Marks → Apple dapat mendaftarkan logonya (gambar sebuah Buah apel yang telah digigit) karena memiliki pengertian untuk mempengaruhi konsumen bahwa produknya mudah digunakan.
- Arbitrary Marks→ dikerenakan tidak adanya hubungan antara buah apel dengan computer, merek dagang ini dapat di daftarkan, sepanjang memiliki ke khasan yang melekat.
- Fanciful Marks → Merek dagang Apple dengan Macintosh dalam hubungannya dengan computer tidak ada perbedaan yang signifikan

UU 15 tahun 2001 Tentang MEREK

Pasal 1 (1)

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.

UU no 15 tahun 2001, Pasal 1 (2)

Merek Dagang adalah Merek yang digunakan pada barang yang diperdagangkan oleh seseorang atau beberapa orang secara bersama-sama atau badan hukum untuk membedakan dengan barang-barang sejenis lainnya.

UU no.15 tahun 2001, tentang MEREK, Pasal 1 (3)

- Merek Jasa adalah Merek yang digunakan pada jasa yang diperdagangkan oleh seseorang atau beberapa orang secara bersama-sama atau badan hukum untuk membedakan dengan jasa-jasa sejenis lainnya

UU No.15 tahun 2001 tentang MEREK, Pasal 1 (4)

- Merek Kolektif adalah Merek yang digunakan pada barang dan/atau jasa dengan karakteristik yang sama yang diperdagangkan oleh beberapa orang atau badan hukum secara bersama-sama untuk membedakan dengan barang dan/atau jasa sejenis lainnya

PRINSIP

- MEMILIKI DAYA PEMBEDA

MEREK Vs Nama Domain

- Apa itu Nama Domain
-

- Nama domain adalah alamat internet, dan biasanya digunakan untuk mencari websites.

- Misalnya, nama domain WIPO 'wipo.int' digunakan untuk menentukan website WIPO pada www.wipo.int.

- UU sebuah negara atau pengadilan sering kali memperlakukan pendaftaran merek yang dimiliki oleh suatu perusahan atau individu sebagai nama domain menjadi suatu pelanggaran merek, yang lebih dikenal dengan nama cybersquatting

- Jika hal ini terjadi, usaha yang dimiliki tidak hanya harus mengalihkan atau menarik nama domain tersebut, tetapi juga harus membayarkan kerugian atau DAPAT DIKENAKAN HUKUMAN YANG BERAT

- jika sebuah merek yang dimiliki oleh suatu perusahaan digunakan dalam sebuah nama domain atau telah dilanggar oleh pihak lain/ perusahaan lain maka tindakan keras dapat diambil untuk menghentikan pelanggaran tersebut

Kapan Nama Domain di Kualifikasikan sebagai merek dagang ?

- Sebuah nama domain, dapat memenuhi syarat sebagai merek dagang bila digunakan dalam kaitannya dengan sebuah website yang menawarkan layanan kepada publik.
- seperti yahoo.com, google.com dll..

Paradigma

Nama Domain

- Nama Domain di llindungi untuk kurun waktu tertentu selama Domain name itu masih digunakan oleh penggunanya

MEREK

- bahwa merek terdaftar mendapat perlindungan hukum untuk jangka waktu 10 (sepuluh) tahun sejak tanggal penerimaan dan jangka waktu perlindungan itu dapat diperpanjang untuk jangka waktu yang sama

Paradigma

Nama Domain

- Nama Domain karakteristiknya terdiri atas susunan huruf dan angka dimana dalam cyber space susunan ini dinamakan digit,

MEREK

- Merek karakteristiknya terdiri dari susunan gambar, nama, kata, huruf-huruf, angka-angka, susunan warna, ataupun kombinasi dari unsur-unsur tersebut.

Paradigma

Nama Domain

- Nama domain didaftarkan pada penyedia layanan pembuatan nama domain

MEREK

- MEREK didaftarkan kepada Ditjen HKI, Kemenkumham RI

Paradigma

Nama Domain

- Yang di lindungi hanya digitnya

MEREK

- Merek, haruslah didaftarkan mulai dari apakah yang didaftarkan kata-kata, gambar ataupun hanya warna saja, terkadang pemilik merek harus teliti bahwa semua unsurnya terdaftarkan. Bila ada salah satu unsur yang tidak didaftarkan, maka akan membuka kemungkinan pemilik merek lain memanfaatkan kelemahan itu untuk membuat efek kabur

Kasus

Mustika Ratu Vs

Tjandra Sugiono

- Tjandra terjerat kasus pidana pendaftaran *domain name mustika-ratu.com*. Sialnya, Tjandra menggunakan *name server belia-online.com*, nama situs perusahaan saingan Mustika Ratu, yakni Martina Berto.
- Murgiana Haq, saksi ahli yang sampai medio 2001 lalu menjadi *President Asian Intellectual Property Association* (A-IPA), berpendapat bahwa pendaftaran *domain name*, walaupun pada kenyataannya tidaklah dikelola, dapat menunjukkan itikad buruk dari si pendaftar (*registrant*).
- Hal ini dikarenakan pendaftaran tersebut akan menghalangi pemilik yang sah untuk menggunakan *domain name*, khususnya dalam merepresentasikan nama bisnisnya. Dalam hal pendaftaran Tjandra Sugiono, Murgiana menilai pendaftaran yang dilakukan oleh Tjandra Sugiono dapat menunjukkan adanya persaingan curang.
- Pasalnya, berdasarkan database *whois* yang terdapat di Network Solutions, Tjandra menggunakan *name server* belia-online.com yang dimiliki oleh Cakraweb Hosting. Nah, menurut Murgiana yang juga praktisi HKI (Hak Kekayaan Intelektual) di Singapura sejak tahun 1974, *belia-online.com* ini merupakan situs yang berisi produk-produk milik Martina Berto.
- Pencantuman *name server belia-online.com* ini, lanjut Murgiana, dapat menarik pengguna internet ke situs belia-online yang menampilkan produk-produk Belia, salah satu produk andalan Martina Berto. Hal ini dapat menimbulkan persepsi adanya hubungan antara produk belia dengan Mustika Ratu.

- untuk kasus domain name yang pendaftar (registrant) domain name maupun pemilik merek adalah sama-sama warga negara atau badan hukum Indonesia seperti kasus mustika-ratu.com,
- UU No. 15 Tahun 2001 tentang Merek di bawah yurisdiksi Indonesia sudah cukup memadai untuk dijadikan dasar hukum.

Sepanjang syarat-syaratnya terpenuhi:

- pertama, adanya bukti bahwa penggugat memiliki hak yang sah atas merek terkait, yakni melalui pendaftaran atau pemakaian pertama. Tanggal pendaftaran atau pemakaian pertama ini harus lebih dulu dari tanggal efektif pendaftaran domain name tersebut.
-
- Syarat kedua, domain name tersebut memiliki persamaan keseluruhan atau pada pokoknya (identical or confusingly similar) dengan merek pihak yang merasa dirugikan.
-
- Syarat ketiga, pihak registrant tidak cuma sekadar mendaftarkan domain name tersebut, tetapi juga menggunakannya untuk memperdagangkan barang/jasa yang sejenis. Namun untuk merek terkenal, unsur persamaan jenis barang/jasa dapatlah dikesampingkan.
-
- Syarat keempat, pihak registrant domain name mendaftarkan dan memakai domain name dengan itikad buruk , Ini adalah syarat yang terpenting yang dapat ditunjukkan oleh keadaan-keadaan tertentu. Misalnya untuk menjual, menyewakan, atau mengalihkan registrasi domain name kepada pemilik merek yang bersangkutan.

C/O kasus nama domain sebagai merek dagang.

- Kasus lainnya, adalah nama domain philips-indo.com yang akhirnya harus diserahkan ke produsen elektronik asal Belanda, Phillips Electronics. Keputusan serupa juga terjadi pada domain bluesclues.com, mtv-girl.com, mtv-girl.net dan mtv-girl.org –semuanya didaftarkan oleh pihak di Indonesia– yang diputuskan untuk diserahkan ke Viacom.

- Kasus nama domain dari Peter F. Saerang, penata rambut ternama. Pada tahun 2007, WIPO memutuskan bahwa nama domain peterfsaerang.com harus dikembalikan pada sang penata rambut. Sebelumnya, nama domain tersebut didaftarkan oleh sebuah perusahaan di Australia.

- Kasus lain yang pernah terjadi di dunia internasional juga cukup menarik perhatian. Misalnya, kasus McDonalds.com yang dibeli oleh seorang wartawan teknologi informasi dari majalah Wired. Kasus itu akhirnya diselesaikan di luar pengadilan dengan McDonalds (jaringan waralaba restoran) mendapatkan nama domain itu kembali. Namun sang wartawan berhasil membujuk McDonalds untuk menyumbangkan sejumlah uang ke sebuah organisasi sosial.

Cybersquatting

- *dapat diartikan sebagai kegiatan yang dilakukan dalam pembelian suatu domain di Internet, dimana domain tersebut memiliki penulisan yang mirip dengan nama perusahaan, nama orang, nama produk dll., dan kemudian sang pembeli domain tersebut menjualnya dengan harga tinggi kepada mereka yang berkaitan dengan nama domain tersebut. Kadangkala Cybersquatting ini diartikan juga sebagai calo.*

- Verizon, salah satu perusahaan komunikasi besar di dunia, memenangkan tuntutan pengadilan sebesar $31.15 juta dari perusahaan pendaftar domain OnlineNIC.
-
- Dalam kasus Verizon ini, pihaknya merasa dirugikan atas pendaftaran domain-domain yang memiliki kemiripan nama domain dengan mereka dan lalu menuntut OnlineNIC, sebuah perusahaan pendaftar domain/registrar untuk domain .asia .biz .com .info .mobi .name .net .org .pro dan .tel.
-
- Pihak Verizon menuntut OnlineNIC karena mendaftarkan 663 nama domain yang mirip atau justru membingungkan terhadap merk dagang Verizon. Dua diantara dua nama domain yang dianggap membingungkan pelanggan Verizon adalah verizon-cellular.com dan buyverizon.net.

Prosedur mengatasi cybersquatting

- Menggunakan Prosedur Internet Corporation of Assigned Names and Numbers (ICANN)
- Pada tahun 1999, ICANN mulai menerapkan Uniform Domain Name Dispute Resolution Policy (UDNDRP), sebuah kebijakan untuk penyelesaian sengketa nama domain.

- Alasan yang dapat digunakan untuk mengajukan gugatan menggunakan prosedur ICANN :

a. Nama domain adalah identik atau mirip dengan merek dagang atau merek jasa yang dimiliki penggugat

b. Pemilik nama domain tidak memiliki hak atau kepentingan yang sah atas nama domain

c. Nama domain telah didaftarkan oleh orang lain dan digunakan dalam hal yang tidak baik,

Jika gugatan diterima, maka nama domain akan dibatalkan atau dialihkan kepada penggugat.

Prosedur Mengatasi Cybersquatting

- Menggunakan Prosedur Anticybersquatting Consumer Protection Act (ACPA) PTO U.S
- Anticybersquatting Consumer Protection Act (ACPA) memberi hak untuk pemilik merek dagang untuk menuntut sebuah cybersquatter di pengadilan federal dan mentransfer nama domain kembali ke pemilik merek dagang. Dalam beberapa kasus, cybersquatter harus membayar ganti rugi uang.

- pemilik merek dagang harus membuktikan semua hal berikut:

a. Para pendaftar nama domain memiliki niat buruk dan mengambil keuntungan dari merek dagang orang lain

b. Merek dagang sudah ada pada saat nama domain pertama kali didaftarkan
Nama domain adalah identik, membingungkan atau mirip dengan merek dagang tersebut,

c. Merek dagang tersebut memenuhi syarat dan memiliki badan hukum atau hak patent - dan pemiliknya adalah orang pertama yang menggunakan merek tersebut dalam perdagangan.

- http://teknologi.vivanews.com/news/read/22405-cybersquatter_indonesia_serahkan_domain
- Ahmad Rusli, seorang cybersquatter asal Indonesia diminta oleh World Intellectual Property Organization atau badan yang mengurusi permasalahan hak cipta PBB untuk mengembalikan domain yang ia beli ke pemilik nama aslinya.
- Domain www.carlosslimhelu.com, domain yang dipermasalahkan tersebut merujuk ke pemilik nama aslinya Carlos Slim Helu. Ia adalah seorang miliuner telekomunikasi asal Meksiko. Menurut daftar orang terkaya di seluruh dunia versi majalah Forbes, tahun 2008 ini nilai kekayaan Carlos Slim Helu mencapai 60 miliar dolar AS. Carlos menempati urutan kedua orang terkaya di dunia setelah Warren Buffet, CEO dari Berkshire Hathaway yang memiliki kekayaan senilai 62 miliar dolar AS dan di atas Bill Gates, pendiri Microsoft yang mengantongi aset senilai 58 miliar dolar AS.
- Rusli, yang mengaku berdomisili di Kemanggisan, Jakarta Barat telah meminta bayaran pada Helu sebesar 55 juta dolar jika sang miliuner itu ingin memiliki domain www.carlosslimhelu.com. Rusli mengancam akan menghubungkan (me-link) situs tersebut ke situs berkonten pornografi jika Helu mengabaikannya.

- Menurut informasi Reuters, 14 Januari 2009, pengacara Helu mengadukan masalah ini ke WIPO. Didukung dengan dokumentasi yang lengkap mengenai Helu, alamat domain, serta bukti permintaan uang terhadap Helu dari Rusli, akhirnya WIPO menyatakan bahwa domain itu didaftarkan dengan niat yang tidak baik.
- Meski lewat email, Rusli menyatakan bahwa ia hanya bermaksud untuk melindungi alamat domain itu untuk Helu dan ancaman yang ia berikan hanya untuk menarik perhatian sang miliuner, tetapi WIPO tetap pada keputusannya. Rusli harus mengembalikan domain pada Carlos Slim Helu tanpa bayaran.
- Selain memiliki domain carlosslimhelu.com, sampai 16 Januari 2009 ini Rusli tercatat sudah mendaftarkan 197 domain yang siap ia jual

Nama Domain dalam UU ITE no.11 tahun 2008

- Pasal 23 yaitu ayat (2) yaitu "*Pemilikan dan penggunaan Nama Domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada itikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain.*"
-
- penjelasan UU ITE pasal 23 ayat (2) yang berbunyi *"Yang dimaksud dengan "melanggar hak Orang lain", misalnya melanggar merek terdaftar, nama badan hukum terdaftar, nama Orang terkenal, dan nama sejenisnya yang pada intinya merugikan Orang lain.*"

UU ITE

- Domain secara jelas diterangkan dalam pasal 23 ayat 3, yang berbunyi:

- Setiap penyelenggara negara, Orang, Badan Usaha, atau masyarakat yang dirugikan karena penggunaan Nama Domain secara tanpa hak oleh Orang lain, berhak mengajukan gugatan pembatalan Nama Domain dimaksud.

Parameter Pasal 23 (3)

- Yang dimaksud dengan "penggunaan Nama Domain secara tanpa hak" adalah :
- pendaftaran dan penggunaan Nama Domain yang semata-mata ditujukan untuk menghalangi atau menghambat Orang lain untuk menggunakan nama yang intuitif dengan keberadaan nama dirinya atau nama produknya,atau untuk mendompleng reputasi Orang yang sudah terkenal atau ternama, atau untuk menyesatkan konsumen.
-

UNCITRAL Model Law on Electronic Signatures (2001)

Latar Belakang

- PBB membentuk suatu badan yang bertugas untuk menyiapkan kebijakan - kebijakan yang terkait dengan pembentukan hukum yang berkenaan dengan perdagangan internasional yaitu UNCITRAL (United Nations Commision on International Trade Law).

- UNCITRAL membuat model laws yang dapat diadopsi oleh negara - negara anggota PBB yang bertujuan agar aspek - aspek hukum yang terkandung dalam perdagangan internasional tersebut dapat diakomodasi secara mudah.

- UNCITRAL merasa berkepentingan untuk membuat suatu model law yang mengatur kegiatan perdagangan internasional yang menggunakan media elektronik.
- UNCITRAL mengeluarkan Model Law on E-Commerce pada tahun 1996 dan Model Law on Electronic Signatures pada tahun 2001 .

Model Law on Electronic Signatures 2001

- Pada pasal 2 model law mengatur tentang defenisi,antara lain:

a) Electronic signatures adalah data dalam bentuk elektronik yang berkaitan atau secara logikal berhubungan dengan pesan data, yang dapat digunakan untuk mengidentifikasi si pemilik tanda tangan yang berkaitan dengan pesan data dan sebagai tanda persetujuan pemilik tanda tangan atas informasi yang terdapat di dalam pesan data tesebut.

Model Law on Electronic Signatures 2001

- Certificate adalah pesan data atau bentuk lain yang dapat membuktikan hubungan antara pemilik tanda tangan dan data tanda tangan tersebut.
- Data Message adalah pengiriman, penerimaan dan penyimpanan informasi melalui cara – cara elektonik, optik atau cara – cara lainnya seperti electronic data interchange (EDI), elektonik mail, telegram, telex atau telecopy.

Model Law on Electronic Signatures 2001

Signatory adalah orang yang memiliki tanda tangan dan bertindak atas dirinya sendiri atau atas diri orang lain yang digantikannya.

Certification Service Provider adalah pihak yang melakukan verifikasi terhadap identitas pemilik tanda tangan elektronik.

Relying party adalah pihak – pihak yang bertindak atas dasar tanda tangan elektronik tersebut.

- Model law ini mengandung asas netral teknologi karena tidak hanya mengacu pada satu teknologi (public key infrastructure)

Contoh: Digital Signature Act yang dikeluarkan oleh Utah, Amerika Serikat. Digital Signature Act ini dianggap sebagai suatu kesalahan karena mengkhususkan pengaturannya pada tanda tangan digital yang termasuk ke dalam tanda tangan elektronik, dimana tanda tangan digital hanya mengacu pada satuteknologi dan infrastruktur

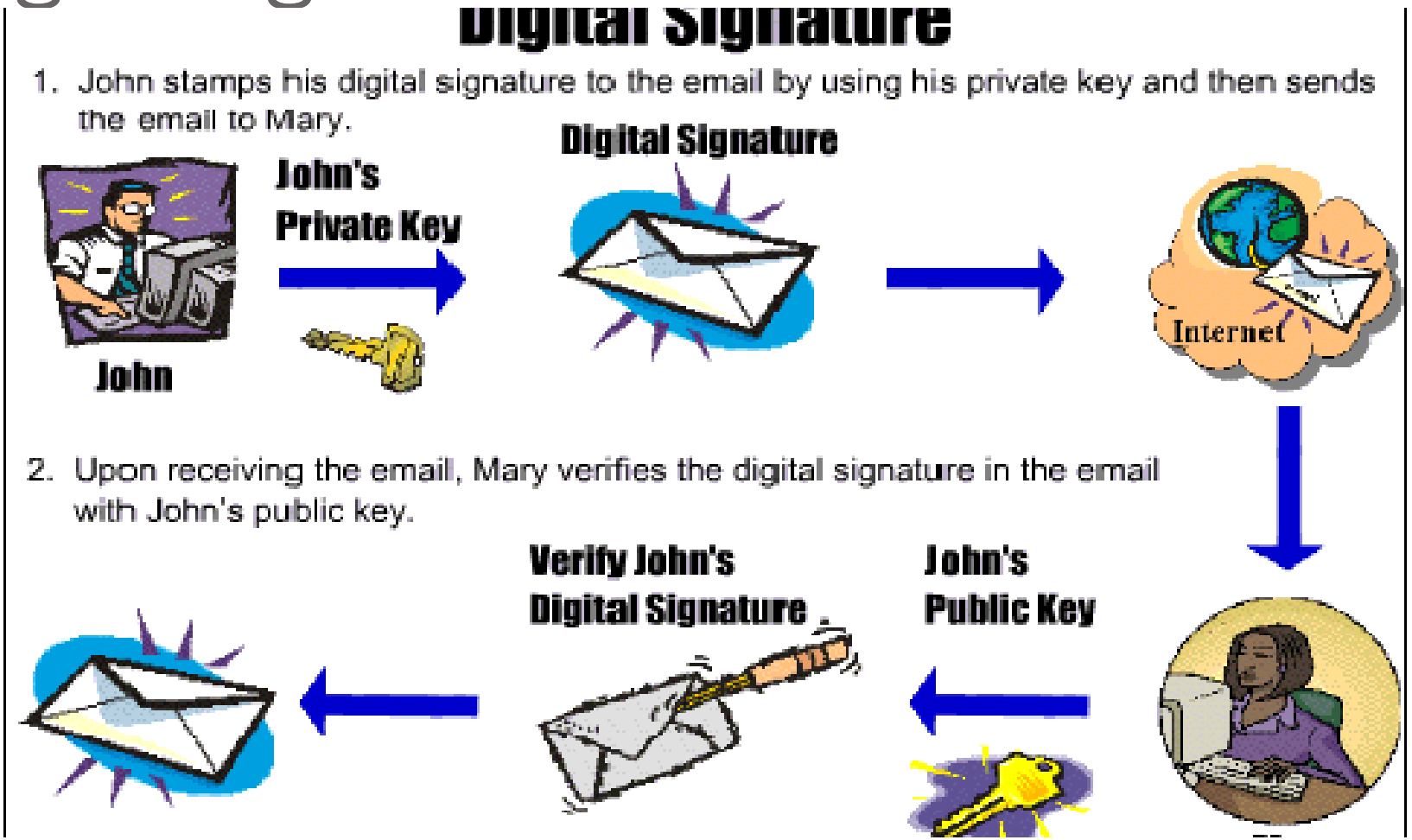
- Akan tetapi di dalam pelaksanaannya, public key infrastructre (PKI) masih digunakan, dalam PKI yang melakukan verifikasi adalah Certification Authority (CA). Sedangkan dalam UNCITRAL 2001 ini, yang melakukan verifikasi adalah Certification Service Provider (CSP), hal ini diatur di dalam pasal 9.
- Penggunaan PKI di dalam UNCITRAL 2001 ini adalah disebabkan karena PKI dianggap sebagai suatu mekanisme pengamanan yang tak terkalahkan

- UNCITRAL 2001 mengatakan bahwa Certification Service Provider (CSP) adalah person (orang) bukan legal entity. Dimana CSP memiliki tanggung jawab publik , dimana apabila tidak dilaksanakan dengan benar maka akan diminta pertanggungjawabannya oleh pemerintah.
- Hal ini menjadi permasalahan karena bagi negara – negara yang mengimplementasikannya, karena pada saat sekarang ini negara – negara di dunia mengenal subjek hukum orang perorangan dan badan hukum. Akan lebih mudah untuk menuntut pertanggungjawaban badan hukum dari pada orang perorangan.

- UNCITRAL 2001 mencoba menghilangkan kesulitan dalam cross certification atau cross recognition dengan mengakomodir untuk memungkinkan penggunaan tanda tangan elektronik maupun sertifikat yang dibuat, digunakan atau diterbitkan di luar negara yang menerapkan UNCITRAL 2001, akan tetapi harus sesuai dengan standard internasional yang berlaku.
- Peniadaan cross recognition ini dapat membantu menumbuhkembangkan pemanfaatan tanda tangan elektronik dan sertifikat elektronik di seluruh dunia.

  (hal ini diatur di dalam pasal 12 model law).

Digital signature



On 11/29/11 10:24 AM,

XXXX wrote:

> Dear all, >

> Thank you for your kind comments. I have revised the draft asattached.

My bests, > >

Yonglin.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.9 (Darwin) Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

iQEVAwUBTtUrmKozOCHcm84kAQLN7Qf9HsAtncrJ+U7gFgITI2tbsQC7HmrQ7daW
Jkm/X7fzOZHwWOoBylPU8zbMWBZUMhBRq4gBdW1LbI+3Qy3ULLC6zw2BMZ6N
QvR+
0mz9NQwTeiHUhD2aEyBpgxxQLP7FCK6VLmqo1qurgszH+3gW7IGsOgArf1dKMCw
Q
6o+kULNjqh3rg/MQKTUtktGfbZ0aOx0Rp2wKmhWSm3JPz92cNvR/7czQp/ztI0IW
fahsg1dZMGsjfhgz7S3CvyvVbcPyNFYFn+3xDTMs/WQqgG3fdba+oB+35NXVsXat
ytWtqGvce4G4NRwyJINM7cgA8PMXq+LQE3Ycd156tHjacx4Dr6oV1w===tTsi

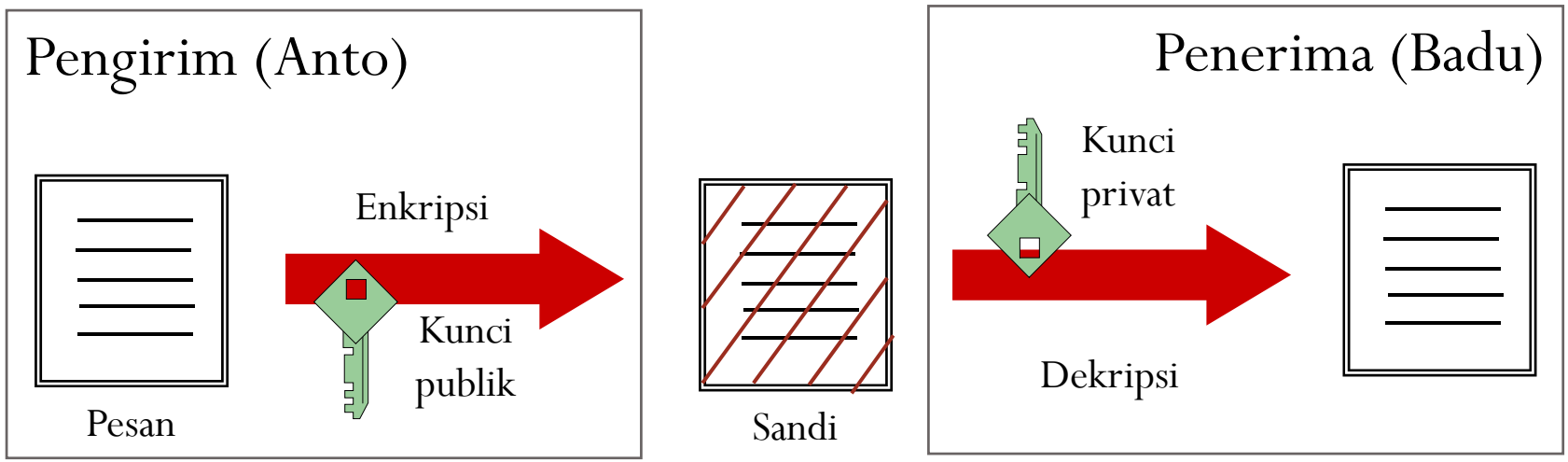
-----END PGP SIGNATURE-----

Public Key Cryptography

- Ada 2 kegunaan yang mendasar:
  - Menandatangani pesan
  - Mengirim surat rahasia dalam amplop yang tidak bisa dibuka orang lain
- Ada sepasang kunci untuk setiap orang (entitas):
  - kunci publik (didistribusikan kepada khalayak ramai / umum)
  - kunci privat (disimpan secara rahasia, hanya diketahui diri sendiri)

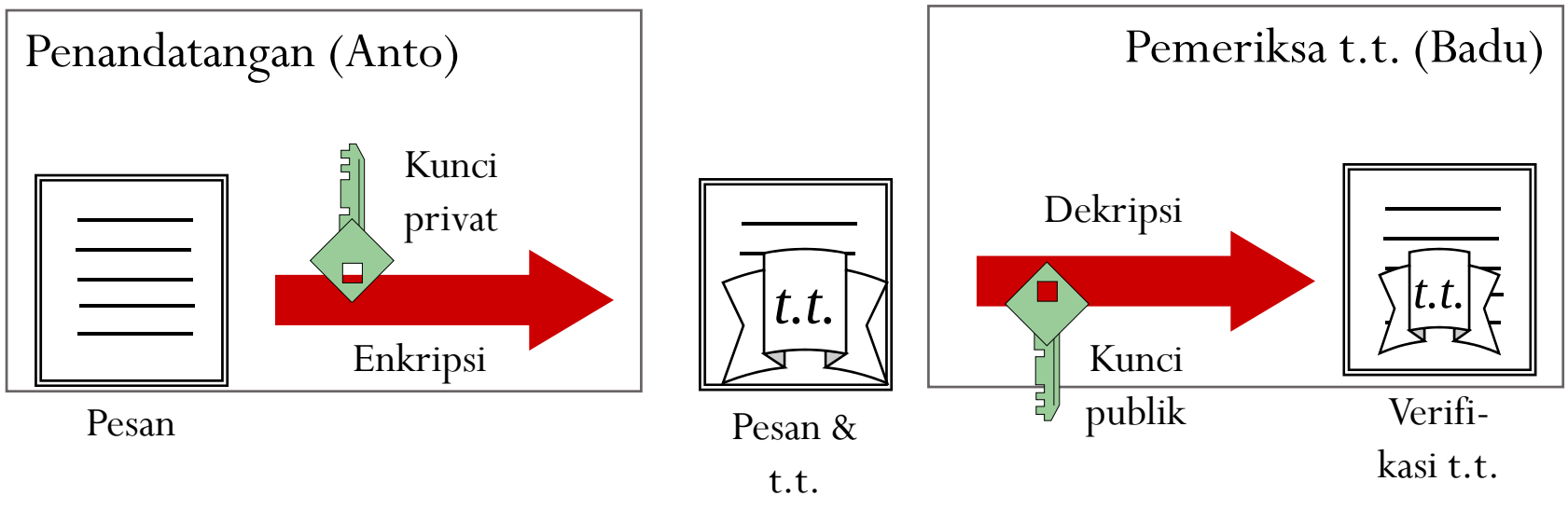
Membungkus pesan

- Semua orang bisa (Anto, Chandra, Deni) mengirim surat ke "Penerima" (Badu)
- Hanya "penerima" yang bisa membuka surat
- *(pada prakteknya tidak persis spt ini)*



Menandatangani pesan dgn public-key cryptography

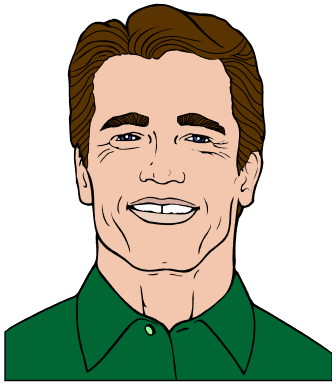
- Hanya pemilik kunci privat (penandatangan, Anto) saja yang bisa membuat tanda tangan digital
- Semua orang (Badu, Chandra, Deni) bisa memeriksa tanda tangan itu jika memiliki kunci publik Anto
- *(disederhanakan)*



Sifat tanda tangan digital:

- Otentik, dapat dijadikan alat bukti di peradilan (kuat)
- hanya sah untuk dokumen (pesan) itu saja, atau kopinya. Dokumen berubah satu titik, tanda tangan jadi invalid!
- dapat diperiksa dengan mudah oleh siapapun, bahkan oleh orang yang belum pernah bertemu (dgn sertifikat digital tentunya)

Sertifikat digital



Kunci publik
Arnold

C=US, O=Warner Bross
OU= Movies Division,
CN= Awak-Seger, Arnold

arnold@hollywood.com
www.arnold.com

Berlaku s/d 1 Juli 2002

Certificate policy:
e-mail security

CA

Berhubungan
dengan hak dan izin
menggunakan
domain name ybs

Keuntungan sertifikat digital

- bisa membuat "saluran komunikasi" tertutup antara 2 pihak
- bisa dipergunakan untuk mengotentikasi pihak lain di jaringan (mengenali jati dirinya)
- bisa dipakai untuk membuat dan memeriksa tanda tangan
- bisa dipakai untuk membuat surat izin "digital" untuk melakukan aktifitas tertentu, atau identitas digital
- bisa untuk off-line verification

Penutup

UNCITRAL Model law on Electronic Signature merupakan salah satu instrumen yang sangat penting dalam Electronic Commerce,karena pada saat sekarang ini negara – negara di dunia sudah menggunakan sarana elektonik signature dalam melakukan transaksi maupun kontrak – kontrak elektronik.

Lampiran
UNCITRAL Model Law on Electronic Signature (2001)

Article 1 Sphere of application

This law applies where electronic signatures are used in the context of commercial activities. It does not override any law intended for the protection of consumers

Article 2 Defenitions

For the purposes of this law:

a) Electronic signatures means data in electonic form in, affixed to or logically associated with, a data message,which may be used to identify the signatory in relation to data message and to indicate the signatory's approval of the information contained in the data message.

b) Certificate means a data message or other record confirming the link between a signatory and a signature creation data.

c) Data message means information generated,sent,received or stored by electronik,optical or similar means including, but not limited to EDI,electronic mail,telegram,telex or telecopy and acts either on its behalf of the person it represents.

d) Signatory means a person that holds signature creation data and acts on its behalf or on behalf of the person it represents

e) Certification service provider means a person that issues certificates and may provide other services related to electronic signatures

f) Relying party means a person that may act on the basis of a certificate or on electronic signature.

Article 3 equal treatment of signature technologies

Nothing in this law, except article 5, shall be applied so as to exclude restrict or deprive of legal effect any method o creating an electronic signature that satisfies the requirements referred to in article 6,paragraph 1 or otherwise meets the requirements of applicable law.

Article 4 Interpretation

1. In the interpretation of this law,regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of goodfaith
2. Questions concerning matters governed by this law which are not expressly settled in it are to be settled in conformity with the general principles on which this law is bassed

Article 5 Variation by Agreement

The provisions of this law may be derogates from or their effect may be varied by agreement,unless that agreement would not be valid or effective under applicable law

Article 6 Compliance with a requirement for a signature

1. Where the law requires a signature of a person,that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purposefor which the data message was generated or communicated,in the light of all the circumstances,including any relevant agreement.
2. Paragraph 1 applies whether he requirement reffered to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
3. An electronic signatureis considered to be reliable for the purposes of satisfying the requirement referred to in paragraph 1 if:

a) The signature creation data are,within the context in which they are used,linked to the signatory and to no other person.

b) The signature creation data were,at the time of signing, under the control of the signatory and of no other person

c) Any alterations to the electronic signature,made after the time of signing,is detectable

d) Where the purpose of legal requirement for a signature is to provide assurances as to integrityof the information to which it relates,any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

a) To establish in any other way,for the purposes of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature

b) To adduce evidence of non-reliability of an electronic signature

5. The provisions of this article do not apply to the following (...)

Article 7 Satisfaction of article 6

1. [any person,organ or authority,whether public or private,specified by the enacting state as competent] may determine which electronic signatures satisfy the provisions of article 6 of this law.
2. Any determination made under paragraph 1 shall be consistent with recognized international standars.
3. Nothing in this article affects the operation of the rules of private international law.

Article 8 Conduct of signatory

1. Where signature creation data can be used to create a signature that has legal effect,each signatory shall:

a) Exercise reasonable care to avoid unauthorized use of its signature creation data.

b) Without undo delay,utilize means made available by the CSP pursuant to article 9 of this law,or otherwise use reasonable efforts,to notify other person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronid signture if:

i. The signatory knows that the signature creation data have been compromised

ii. The circumstances known to th signatory give rise to a substantial risk that the signature creation data may have been compromised.

c) Where a certificate is used to support the electronic signature,exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

2. A signatory shall bear the legal consequances of its failure to satisfy the requirements of paragraph 1.

Article 9 Conduct of the CSP

1. Where a CSP provides services to support an electronic signature that may be used for legal effect as a signature,that CSP shall:

a) Act in accordance with representations made by it with respect its policies and practies.

b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate.

c) Provide reasonably accessible means that enable a relying party to ascertain from th certificate:

i. The identify of the CSP

ii. That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued.

iii. That signature creation data were valid at or before the time when the certificate was issued

d) Provide reasonably accessibl means that enable a relying party to ascertain,where relevant,from th certification or otherwise:

i. Th method used to identify the signatory

ii. Any limitation on the purpose or value for which the signture creation data or certifcate may be used

iii. That the signature creation data are valid and have not been compromised

iv. Any limitation on the scope or extent of liability stipulated by the CSP

v. Whether means exist for the signatory to give notice pursuant to article 8,paragraph 1(b) of this law.

vi. Whether a timely revocation service is offered.

e) Where services under subparagraph (d)(v) are offered,provide a means for a signatory to give notice pursuant to article 8,paragraph 1(b) of this law and,where services under subparagraph (d)(vi) are offered, ensure the availability of a timely revocation service.

f) Utilize trustwothy systems,procedurs and human resources in performing its services.

2. CSP shall bear the legal consequences of its failure to satisfy the requirement of paragraph 1.

Article 10 Trustworthiness

For the purpose of article 9,paragraph 10(f) of this law in determining whether,or to what extent,any system,procedurs and human resources utilized by CSP are trustworthy,regard may be had to the following factors:

a) Financial and human resources,including exixtence of assets.

b) Quality of hardware and software system

c) Procedurs for processing of certificates and applications for certificates and retention of records

d) Availability of information to signatories identified in certificates and to potential relying party

e) Regularity and extent of audit by an independent body

f) The existence of a declaration by the state, an accreditation body or the CSP regarding compliance with or existence of foregoing

g) Any other relevant factor.

Article 11 Conduct of the relying party

A relying party shall bear the legal consequences of its failure:

a) To take reasonable steps to verify the reliability of an electronic signature

b) Wher an electronic signature is supported by a certificate, to take reasonable steps:

i. To verify the validity,suspension or revocation or the certificate

ii. To observe any limitation with respect to the certificate.

Article 12 Recognition of foreign certificates and electronic signature

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:

a) To the geographic location where the certificate is issued or the electronic signature created or used, or

b) To the geographic location of the place of business of the issuer or signatory.

2. A certificate issued outside shall have the sam legal effect in the enacting state as a certifcate issued in the enacting state if its offers a subtantially equivalent level of reliability.

3. An electronic signature created or used outside he enacting state shall have the same legal effect in enacting state as an electronic signature created or used in the enacting state if its offers a subtantially equivalent level or reliability.

4. In determining whether a certificate or an electronic signature offers a substantially equivalent level or reliability for the purposes of paragraph2 or 3, regard shall be had to recognized international standards and to any other relevant factors

5. Where,notwithstanding paragraph 2,3 and 4 parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as a sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

Permasalahan dalam hubungan Kontrak

E-Commerce >< Kontrak

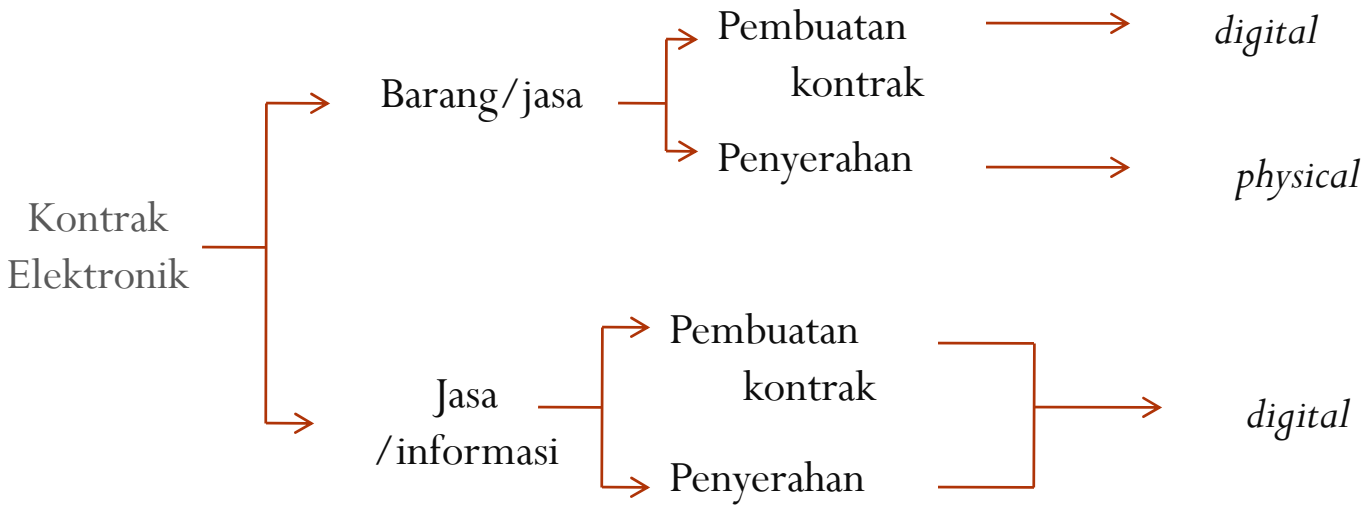
- *Electronic Commerce Transaction* adalah transaksi dagang antara penjual dengan pembeli untuk menyediakan barang, jasa atau mengambil alih hak.
- Kontrak ini dilakukan dengan media elektronik (*digital medium*) di mana para pihak tidak hadir secara fisik.
- Medium ini terdapat di dalam jaringan umum dengan sistem terbuka yaitu internet atau *world wide web*
- .Transaksi ini terjadi terlepas dari batas wilayah dan syarat nasional.
- Terdapat 6 (enam) komponen dalam *Electronic Commerce Transaction* (Kontrak Dagang Elektronik):
  - Ada kontrak dagang.
  - Kontrak itu dilaksanakan dengan media elektronik.
  - Kehadiran fisik dari para pihak tidak diperlukan.
  - Kontrak itu terjadi dalam jaringan publik.
  - Sistem terbuka, yaitu dengan internet atau www.
  - Kontrak itu terlepas dari batas yurisdiksi nasional.

- E- Commerce (*electronic commerce*) merupakan metode untuk menjual produk secara *on line* melalui fasilitas internet.
- E- Commerce merupakan bidang multidisipliner (*multidisciplinary field*) yang mencakup:
  - Bidang teknik: jaringan, telekomunikasi, pengamanan, penyimpanan dan pengambilan data dari multimedia;
  - Bidang bisnis: pemasaran (marketing), pembelian dan penjualan (procurement and purchasing), penagihan dan pembayaran (billing and payment), manajemen jaringan distribusi (supply chain management);
  - Aspek hukum *information privacy*, hak milik intelektual (*property right).*

Digital Contract

- Kontrak baku yang dirancang, ditetapkan, dan disebarluaskan secara *digital* melalui suatu situs di internet (*website*), secara sepihak oleh pembuat kontrak, untuk ditutup secara *digital* pula oleh penutup kontrak.
- Ciri-ciri kontrak elektronik:
  - Kontrak elektronik dapat terjadi secara jarak jauh, bahkan melampaui batas-batas suatu negara melalui internet;
  - Para pihak dalam kontrak elektronik tidak pernah bertatap muka (faceless nature), bahkan mungkin tidak akan pernah bertemu

Jenis Kontrak Elektronik



Electronic Commerce Transaction (Kontrak Dagang Elektronik) dan KUHPerdata

- sahnya perjanjian (Pasal 1320 KUHPerdata):
  - Kesepakatan untuk membuat suatu perjanjian;
  - Cakap melakukan perbuatan hukum;
  - Suatu hal tertentu;
  - Suatu sebab yang halal.

- Saat terjadinya kesepakatan:
  - Pernyataan dari pihak yang menawarkan (*offerte*) dan yang menerima penawaran tersebut (*acceptatie*).

- **Persoalan hukum berkaitan dengan keabsahan**:
  - Penggunaan tandatangan digital (*digital signature*) belum sepenuhnya menumbuhkan kepercayaan semua pihak yang berkepentingan.

(Digital Signature sudah diatur dalam UU no:11 tahun 2008 tentang Informasi dan Transaksi Elektronik)

  - **Kecakapan menutup kontrak sukar dideteksi berhubung kontrak tersebut bersifat nir tatap buka** (*faceless nature*).

Dunia Maya >< Dunia Nyata

- Berakunya hukum bagi dunia maya (*virtual world*)
  - Informasi yang didapat dari internet berupa data/informasi tertulis, suara dan gambar (integrated service digital network/ISDN).
  - Disebut virtual world (dunia maya) sebagai lawan real world (dunia nyata), hal yang dapat dilakukan di dunia nyata, dapat pula dilakukan di dunia maya.
  - Interaksi dan perbuatan-perbuatan hukum yang terjadi melalui atau di dunia maya adalah sesungguhnya interaksi antara sesama manusia dari dunia nyata dan apabila terjadi pelanggaran hak atas perbuatan hukum melalui atau di dunia maya itu adalah perbuatan hukum yang dilakukan oleh manusia di dunia nyata dan hak yang dilanggar adalah hak manusia dunia nyata, maka hukum yang berlaku dan harus diterapkan adalah hukum dari dunia nyata.

Aspek Hukum E-Commerce

- Penggunaan *Domain name*
  - Penentuan alamat dalam dunia maya dikenal dengan istilah *domain name*. Contoh. *Klikbca.com*
  - Caranya dengan mendaftarkan pada InterNIC untuk mencek apakah *domain name* tersebut telah digunakan oleh pihak lain atau belum. *InterNIC* adalah suatu organisasi yang mendaftar *domain name* dan mengikuti perkembangannya melalui *database searcher* yang disebut *whois*.
  - Di US dibuat undang-undang mengenai penggunaan *domain name* pada jaringan internet dan melarang seseorang untuk mendaftarkan suatu nama yang seharusnya tidak dimiliki oleh pihak tersebut.
  - Pihak yang mendaftarkan suatu nama harus memberikan alasan mengapa pihak tersebut ingin mendaftarkan dengan nama tertentu. → ingat tentang Merek di CyberSpace, kasus Aple.

Aspek Hukum E-Commerce

- Alat bukti
  - Transaksi tradisional menggunal kertas (*paper based transaction)*, apabila terjadi sengketa dokumen kertas itu sebagai alat bukti masing-masing pihak untuk memperkuat posisi hukum masing-masing.
  - Transaksi *e-commerce* adalah *paperless transaction*, dokumen yang digunakan adalah *digital document*.
  - .

(UU no.11 tahun 2008 , menyatakan dokumen elektronik dapat di jadikan alat bukti)

- Pengakuan pemberitahuan *e-mail* sebagai pemberitahuan tertulis
  - Dalam undang-undang terdapat ketentuan tertulis yang mengharuskan adanya “pemberitahuan tertulis” sebagai syarat dari suatu perjanjian.
  - Apakah “pemberitahuan *e-mail*” dapat menggantikan fungsi “pemberitahuan tertulis” sebagaimana dimaksud dalam suatu perjanjian atau suatu peraturan perundang-undangan ?.

Saat ini pelaku usaha sudah umum menggunakan e-mail sebagai bagian pelaksanaan dari kontrak,

Perlindungan Hukum pada E-commerce

- Keandalan dan tingkat keamanan web site penjual.
- Kontrak baku dan ketentuan jual beli.
- Hukum yang berlaku dan konpetensi forum.
- Konsumen dan nasabah bank

Perlindungan Hukum pada E-Commerce

- Kontrak baku dan ketentuan jual beli
  - Konsumen umumnya disodori kontrak baku yang tertuang dalam website untuk berbelanja.
  - Konsumen harus secara seksama membaca klausula-klausula kontrak yang ada sebelum memberikan persetujuannya.
  - Konsumen berada pada situasi tidak ada pilihan
  - Konsumen harus berani menolak atau membatalkan ("*cancel*") jika terdapat klausul kontrak yang menyatakan bahwa barang yang sudah dibeli tidak dapat ditukarkan atau dikembalikan


End User License Agreement (EULA)
Flight Sim Developers (FSD) EULA Agreement
FSD add-on software for Microsoft Flight Simulator.
IMPORTANT-READ CAREFULLY: BY INSTALLING THIS SOFTWARE YOU ARE AGREEING TO THE TERMS SPECIFIED BELOW!
This FSD End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and FSD, for the software product identified above. "SOFTWARE PRODUCT" is hereby identified as, and includes, any or all computer software, associated media, printed materials, and "online" or electronic documentation associated with it. By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not
If you agree to the above terms press "I Accept". Otherwise press "Cancel" to cancel installation.
I Accept
Cancel

Perlindungan Konsumen pada Transasksi E-Commerce

- Pada UU ITE
- Pasal 2
- Undang-Undang ini 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.

- Pasal 9
- Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

- Pasal 10
- Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.

- Pasal 18

Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.

Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya.

Jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional.

Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari Transaksi Elektronik internasional yang dibuatnya.

Jika para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (4), penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata Internasional

- Pasal 20
- Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.
  Persetujuan atas penawaran Transaksi Elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

- Pasal 21
- Pengirim atau Penerima dapat melakukan Transaksi Elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui Agen Elektronik.
- Pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:
  jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi;
- jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau
  jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.
  Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik.
  Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.
  Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

- Pasal 22
- Penyelenggara Agen Elektronik tertentu harus menyediakan fitur pada Agen Elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi.
  Ketentuan lebih lanjut mengenai penyelenggara Agen Elektronik tertentu sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah

Perlindungan Hukum Pada E-commerce

- Hukum yang berlaku dan konpetensi forum (lihat slide 13,14 dan 15).
- Konsumen dan nasabah bank
  - Khususnya dalam pelayanan jasa perbankan melalui internet (*internet banking*) perlu diperhatikan kesiapan bank mengingat bank bertanggung atas pengendalian dan monitoring sistem yang dibuat maupun yang dioperasikan oleh vendor.
  - Hal lain yang perlu dilakukan adalah perlunya dibuat perjanjian interkoneksi (*interconnected agreement*) antara website satu bank dengan website bank lain atau perusahaan lain interkoneksi dengan sistem *internet banking*.
  - Hendaknya dibuat klausul eksenorasi yang intinya melepaskan tanggungjawab bank atas kemungkinan gugatan konsumen akibat memanfaatkan informasi dari penjual yang ter interkoneksi atau iklan-iklan lain yang muncul pada *homepag*e bank tersebut.

Klausula Eksonerasi

- Keberadaan klausula eksonerasi dalam perjanjian didasarkan pada asas kebebasan berkontrak dalam pasal 1388 ayat 1 KUH Perdata.
- Hakekat klausula eksonerasi dalam perjanjian tidak lain adalah untuk adanya pembagian beban resiko yang layak,
- dalam praktik makna klausula eksonerasi disalahgunakan oleh mereka yang memiliki keunggulan ekonomi yaitu tidak hanya untuk membebaskan diri dari beban tanggung jawab yang berlebihan tetapi juga sampai pada penghapusan tanggungjawab.
- Oleh karena itu perlu adanya pemabtasan terhadap pengunaan klausula eksonerasi dalam perjanjian sebagai perlindungan terhadap konsumen.

- dalam **Pasal 18** **UU No. 8 Tahun 1999 tentang Perlindungan Konsumen** **("UUPK")**.
- Dalam UUPK ini klausula eksonerasi merupakan salah satu bentuk "**klausula baku**" yang dilarang oleh UU tersebut.

- tujuan dari larangan pencantuman klausula baku yaitu bahwa larangan ini dimaksudkan untuk menempatkan kedudukan konsumen setara dengan pelaku usaha berdasarkan prinsip kebebasan berkontrak. Karena pada dasarnya, hukum perjanjian di Indonesia menganut asas kebebasan berkontrak
- (**Pasal 1338 Kitab Undang-Undang Hukum Perdata - KUHPerdata**). Dalam hal ini setiap pihak yang mengadakan perjanjian bebas membuat perjanjian sepanjang isi perjanjian tersebut tidak bertentangan dengan prinsip-prinsip hukum yang berlaku, tidak melanggar kesusilaan dan ketertiban umum (lihat **Pasal 1337 KUHPerdata**).

Aspek Pembuktian

HUKUM PEMBUKTIAN KEJAHATAN TEKNOLOGI INFORMASI

- **HUKUM PEMBUKTIAN** :
  - Merupakan sebagian dari hukum acara pidana yang mengatur **macam-macam alat bukti yang sah** menurut hukum, **sistem yang dianut** dalam pembuktian, **syarat-syarat** dan **tata cara mengajukan bukti** tersebut serta kewenangan hakim untuk menerima, menolak dan menilai suatu pembuktian
- **SUMBER HUKUM PEMBUKTIAN :**
  1. Undang-undang (UU No. 8 Tahun 1981 tentang Hukum Acara Pidana/ KUHAP)
  2. Doktrin atau ajaran
  3. Jurisprudensi

HUKUM PEMBUKTIAN KEJAHATAN TEKNOLOGI INFORMASI

- **Alat Bukti**
  - Segala seuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa.
- **Sistem Pembuktian**
  - Pengaturan tentang macam-macam alat bukti yang boleh dipergunakan, penguraian alat bukti dan dengan cara-cara bagaimana alat bukti tersebut dipergunakan dan dengan cara bagaimana hakim harus membentuk keyakinannya

TUJUAN DAN GUNA PEMBUKTIAN

- **Bagi Penuntut Umum**,
  - Pembuktian adalah merupakan usaha untuk meyakinkan hakim yakni berdasarkan alat bukti yang ada, agar **menyatakan seorang terdakwa bersalah** sesuai dengan surat atau catatan dakwaan.
- **Bagi Terdakwa atau Penasehat Hukum**,
  - Pembuktian merupakan usaha sebaliknya, untuk meyakinkan hakim, yakni berdasarkan alat bukti yang ada, agar **menyatakan terdakwa dibebaskan** atau dilepaskan dari tuntutan hukum atau meringankan pidananya. Untuk itu terdakwa atau penasehat hukum jika mungkin harus mengajukan alat-alat bukti yang menguntungkan atau meringankan pihaknya. Biasanya bukti tersebut di sebut bukti kebalikan.
- **Bagi Hakim**
  - Atas dasar pembuktian tersebut yakni dengan adanya alat-alat bukti yang ada dalam persidangan baik yang berasal dari Penuntut Umum atau Penasehat Hukum/ Terdakwa dibuat **dasar untuk membuat keputusan**

ALAT BUKTI

- Pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan adalah berupa kegiatan yang berhubungan dengan **pembuktian** atau kegiatan **untuk membuktikan**.

- Mencari bukti sesungguhnya adalah mencari alat bukti. Bukti yang terdapat pada alat bukti itu kemudian dinilai oleh pejabat penyelidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana ataukah tidak

- **ALAT BUKTI** menurut **UU INFORMASI DAN TRANSAKSI ELEKTRONIK** :
- Pasal 5 (1) dan (2) UU ITE :
  - **Informasi Elektronik** dan/atau **Dokumen Elektronik** dan/atau **hasil cetaknya** merupakan **alat bukti hukum yang sah**.
- PasaL 44 UU ITE :
  - **Alat bukti penyidikan, penuntutan dan pemeriksaan** di pengadilan adalah sbb :
    - Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dana
    - Alat bukti lain berupa **Informasi Elektronik** dan/atau **Dokumen Elektronik**.

SUMBER BUKTI DIGITAL

- Selain deskripsi undang-undang ITE tersebut, dikenal pula alat bukti digital. Atribut-atribut khas serta identitas dalam sebuah proses kejahatan dalam dunia komputer dan internet inilah yang disebut dengan bukti-bukti digital.

- Tiga kategori besar **SUMBER BUKTI DIGITAL**, yaitu :
  - **Open Computer Systems**
  - **Communication Systems**
  - **Embedded Computer Systems**

Open Computer Systems

- Perangkat-perangkat yang masuk dalam kategori jenis ini adalah yang umum di sebut dengan **perangkat komputer**. Sistem yang memiliki media penyimpanan, keyboard, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, desktop, server, dan perangkat-perangkat sejenis lain.
- Perangkat yang memiliki sistem media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi.

- Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut di akses, dan informasi lainnya semua merupakan informasi penting.

Communication Systems

- **Sistem telepon tradisional**, **komunikasi wireless**, **Internet**, **jaringan komunikasi data**, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini.

- Sebagai contoh, jaringan Internet membawa pesan-pesan dari seluruh dunia melalui e-mail. Kapan waktu pengiriman e-mail ini, siapa yang mengirimnya, melalui mana si pengirim mengirim, apa isi dari e-mail tersebut merupakan bukti digital yang amat sangat penting dalam investigasi.

Embedded Computer Systems

- Perangkat telepon bergerak (**ponsel**), personal digital assistant (**PDA**), **smart card**, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini.

- Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini. Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul-modul diagnosa yang dipasang dapat menyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang amat berguna

PEMBUKTIAN CYBERCRIME

- Dikatakan selanjutnya bahwa asas ini dikenal dengan adagium " *Nullum delictum noella poena praevia sine lege peonali ".*
- *Nullum crimen sine lege* berarti tidak ada tindak pidana tanpa undang-undang dan
- *Nulla poena sine lege* berarti tidak ada pidana tanpa undang-undang.
- Jadi **undang-undang menetapkan dan membatasi perbuatan mana dan pidana (sanksi) mana yang dapat dijatuhkan kepada pelanggarnya**

Menilai Evidence

- Faktor yang menjadi pertimbangan :
  - Penilaian kasus
  - Onsite consideration
  - Analisa lokasi pemprosesan
  - Pertimbangan hukum
  - Analisa evidence

Analisa Evidence (Barang Bukti)

- Lokasi ditemukan evidence
- Stabilitas media yang dilakukan pemeriksaan
- Menentukan bagaimana evidence didokumentasi
- Mengevaluasi lokasi media penyimpanan
- Memastikan kondisi dari evidence
- Menganalisa kebutuhan akan cadangan listrik

Pemeriksaan Evidence (BarangBukti)

- Pengujian dilakukan dengan tahap :
  - Persiapan sebagai langkah awal
  - Ekstraksi
  - Menganalisa data terekstrak
  - Kesimpulan

Perlindungan Barang Bukti

- Menurut Jim Mc Millan " Banyak kasus tidak dibawa ke pengadilan karena barang bukti yang tidak memadai "
- Barang bukti komputer berupa :
  - Barang sensitif
  - Salah menangani akan rusak
  - Bersifat mekanis - elektromekanis

Ancaman terhadap barang bukti

- Menurut Jim Mc Millan " Importance of a standard methodology in computer forensics " :
  - Virus
  - Prosedur cleanup
  - Ancaman eksternal - lingkungan

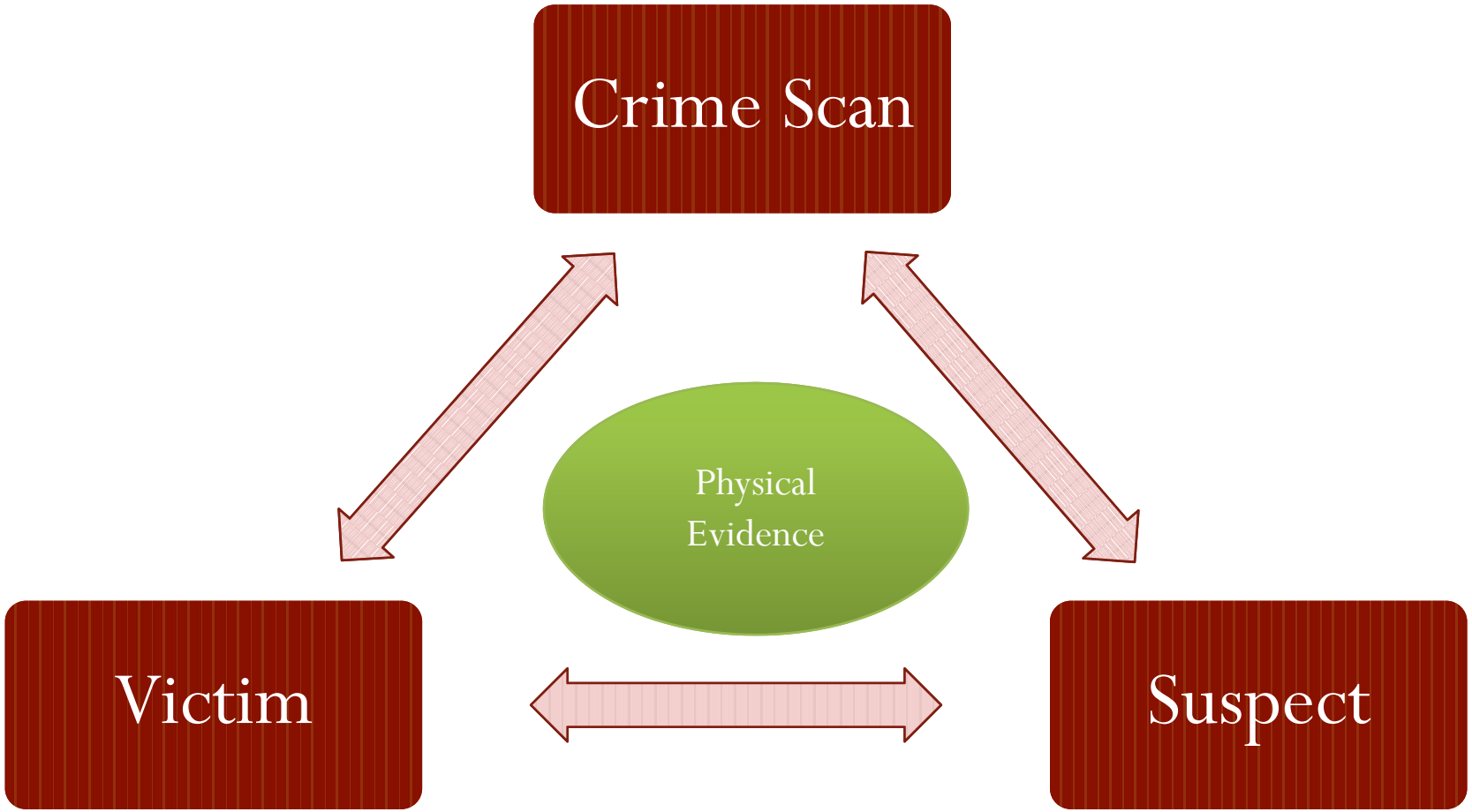
Ancaman terhadap barang bukti

- Menurut Judd Robin " An explanation of computer forensics " mensyaratkan :
  - Barang bukti tidakakan rusak oleh prosedur penyelidikan
  - Tidak terinfeksi virus komputer
  - Barang bukti dilindungi dari keruksakan mekanis dan elektromekanis
  - Penerapan pemelihraan
  - Membatasi dampak pada operasi bisnis
  - Informasi client dihargai secara etis dan tidak diumumkan

Faktor yang tidak berkaitan dengan barang bukti secara fisik

- Rangkaian pemeliharaan
- Batasan waktu
- Informasi yang tidak diumumkan – informasi client
- Register, peripheral memori dan cache
- Memori (kernel dan fisik)
- Keadaan jaringan
- Proses yang sedang berjalan
- Disk
- Floppy disk dn media backup
- CD-Rom dan printout

Locard's Exchange Principle



Pembuktian

- peran hakim dalam proses pembuktian adalah mencari segala macam informasi untuk mendapatkan keyakinan ttg adanya peristiwa hukum dan/atau suatu hubungan hukum dengan menggunakan berbagai media/alat bukti, sejauh hal itu relevan dan valid.
- 1865. Setiap orang yang mendalilkan bahwa ia mempunyai sesuatu hak, atau, guna meneguhkan haknya sendiri maupun membantah suatu hak orang lain, menunjuk pada suatu peristiwa, diwajibkan membuktikan adanya hak atau peristiwa tersebut.

- **1866 BW: Alat Bukti**
  - Bukti Tulisan
  - Bukti dengan saksi2
  - Persangkaan2
  - Pengakuan
  - Sumpah

- 184 KUHAP: Alat bukti yg sah;
  - Keterangan Saksi;
  - Keterangan Ahli;
  - Surat;
  - Petunjuk;
  - Keterangan Terdakwa.

Pembuktian: KUHPer

- 1867. Pembuktian dengan tulisan dilakukan dengan tulisan otentik maupun dengan tulisan di bawah tangan
- 1868. Suatu akta otentik ialah suatu akte yang didalam bentuk yang ditentukan oleh Undang-undang, dibuat oleh atau dihadapan pegawai2 umum yang berkuasa untuk itu ditempat dimana akte dibuatnya. => lihat juga UU 30/2004 ttg Jabatan Notaris (penambahan klausul "pukul" pada akta)
- 1869. Suatu akta yg karena tdk berkuasa atau tidak cakapnya pegawai termaksud diatas, atau karena suatu cacad dalam bentuknya, tidak dpt diperlakukan sbg akta otentik, namun mempunyai kekuatan pembuktian sbg tulisan dibawah tangan jika ditandatangani oleh para pihak
- 1877. Jika suatu akta otentik, yg berupa apa saja, dipersangka kan palsu, maka dpt ditangguhkan menurut ketentuan2 Reglement Acara Perdata.

Pembuktian: Acara Pidana

- Ps.183. Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang2nya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar2 terjadi dan bahwa terdakwalah yang bersalah melakukannya.
- Ps.184. Hal yang secara umum telah diketahui tidak perlu dibuktikan.
- Psl.187. Surat dibuat atas sumpah jabatan atau dikuatkan dengan sumpah;

  a. Berita acara dan surat lain dlm bentuk resmi …. dst

  b. surat yg dibuat menurut ketentuan peraturan perundang-undangan atau surat yg dibuat oleh pejabat mengenai hal yg termasuk dlm tatalaksana yg menjadi tgg jwbnya dan yg diperuntukan bagi pembuktian sesuatu hal atau sesuatu keadaan.

  c. Surat Keterangan dari seorang ahli ….. dst.

  d. surat lain yg hanya dpt berlaku jika ada hubungannya dgn isi dari alat pembuktian yg lain.

Informasi Elektronik: Alat Bukti Lain ?
(Tipikor, Money Laundring & Terorisme)

- Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana (korupsi, money laundering & terorisme) juga dapat diperoleh dari:
- alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan
- dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna."

Informasi Elektronik = Otentik ?

- Suatu tulisan dibawah tangan yg diakui oleh orang terhadap siapa tulisan itu hendak dipakai, atau yg dengan cara menurut UU dianggap sebagai diakui, memberikan terhadap orang-orang yang menandatanganinya serta para ahli warisnya dan orang2 yang mendapat hak daripada mereka, bukti yang sempurna spt suatu akta otentik, dan demikian pula berlakulah ketentuan ps. 1871 utk tulisan itu (penuturan hrs berhubungan langsung dgn pokok isi akta, jika tdk hanya jadi "bukti permulaan").
- Jika seseorang memungkiri tulisan atau ttd-nya ataupun jika para ahli warisnya atau org2 yg mendpt hak daripadanya menerangkan tidak mengakuinya, maka Hakim harus memerintahkan supaya kebenaran dari pada tulisan atau ttd tersebut diperiksa dimuka pengadilan

Otentisitas Informasi Yang Dihadirkan (*trustworthy*) tergantung Akuntabilitas Sistem *?*

- Suatu sistem elektronik hanya dapat dipercaya apabila sistem tersebut dapat dipertanggung-jawabkan dan telah dilakukan pemeriksaan oleh para profesional yang terkait/mempunyai kemampuan untuk itu (tehnikal, manajemen dan hukum), sehingga ia dapat dikatakan handal dan aman serta bekerja sebagaimana mestinya (*working properly*).
- Bertanggung jawab: apabila sistem elektronik tsb jelas keberadaan indentitas subyek hukumnya sebagai Pelaku Usaha (Pengembang dan/atau Penyelenggara).
- Handal: apabila sistem elektronik tersebut secara tehnikal telah dibuat sesuai perencanaan/pengimplementasiannya dengan peruntukannya.
- Aman apabila sistem tersebut telah mengembangkan sistem keamanan elektronik yang sesuai dan/atau dapat dijamin oleh si penyelenggara sistem elektronik tersebut.

Apakah seseorang dapat mungkir ?

- Mungkir/ingkar adalah hak setiap orang jika memang bukan ia pelakunya, tetapi adh suatu “kebohongan” atau “keterangan palsu” bahkan indikasi “penipuan” jika memang ia pihak yang seharusnya ber-tgg-jwb terhadap informasi tsb.
- Pihak lain mempunyai hak untuk tidak mengakui namun ia harus mematuhi jika pemeriksaan dimuka pengadilan menyatakan hal tsb valid.
- Standar terhadap semua “komponen dan fungsi” dalam penyelenggaraan sistem informasi dan komunikasi (*good governance* + *best practices*) akan menentukan validitas/ otentisitas informasi dimuka pengadilan.
- *Trusted Third Party* harus berperan aktif dalam konteks ini.

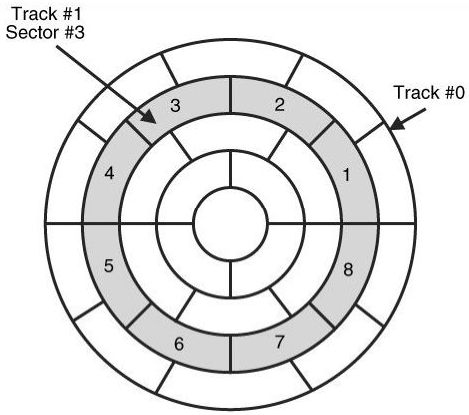
Tak Dapat Dipungkiri (Non-Repudiation)

- UU ITE telah memberikan tempat agar suatu informasi elektronik dapat diterima, dan memberikan prosedur tertentu untuk pedoman bagi hakim dalam pemeriksaan dan pembuktian.
- Jika telah ada UU yang menerima keberadaan sistem security secara baik maka sepanjang tidak dapat dibuktikan lain Subyek Hukum yang tercatat oleh sistem tidak dapat menampiknya karena telah "dianggap" sebagai pihak yang bertanggung jawab atas informasi tersebut.
- *No security = no evidence = no deals.*

Pada saat file di simpan (save)

- Pada saat file disimpan maka pada saat itu disimpan juga beberapa tanda (attributes) :
  - Data kapan file dibuat;
  - Data kapan file terahir di rubah, atau dimodifikasi;
  - Data kapan file terakhir di akses.
- Informasi ini disimpan sebagai bagian dari daftar file yang dikenal sebuah directory. Direktori ini dilihat oleh pengguna sebagai isi (contents) dari sebuah folder.

Deleted data - apakah benar-benar Hilang?



Misalkan, beberapa files dihapus:
Abdul.doc, Hitung.xls, Weblog.htm

Sistem Operasi hanya menghapus (deletes) huruf pertama dari nama file dari tabel pengalokasian file (file allocation table), dan melaporkan sektor yang terdapat "file yang dihapus" menjadi kosong atau tersedia untuk menyimpan data yang baru

Sistem Operasi membacanya menjadi

_bdul.doc _itung.xls _eblog.htm

Catatan :

- **Data tetap "utuh" dan tidak berubah sampai data baru disimpan (written) pada sektor dan cluster yang sepesifik yang berisikan data "tertinggal"**
- **"residu" data terhapus pada saat ada "*Overwriting*" data baru pada sektor yang memiliki "data lama"**