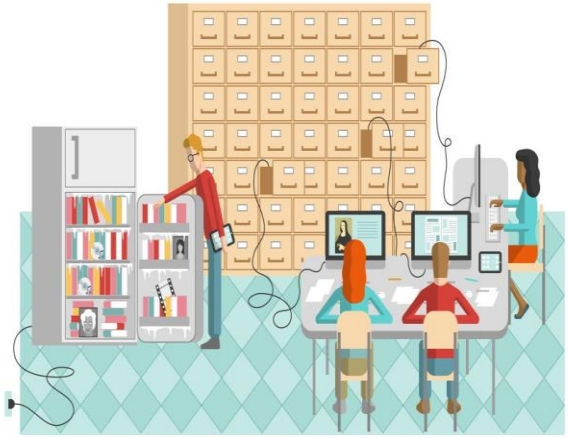
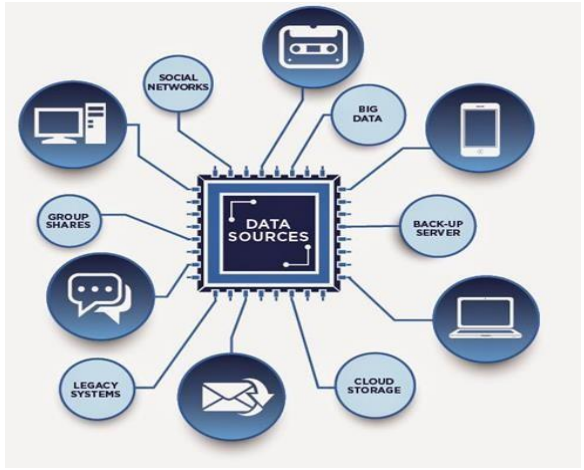
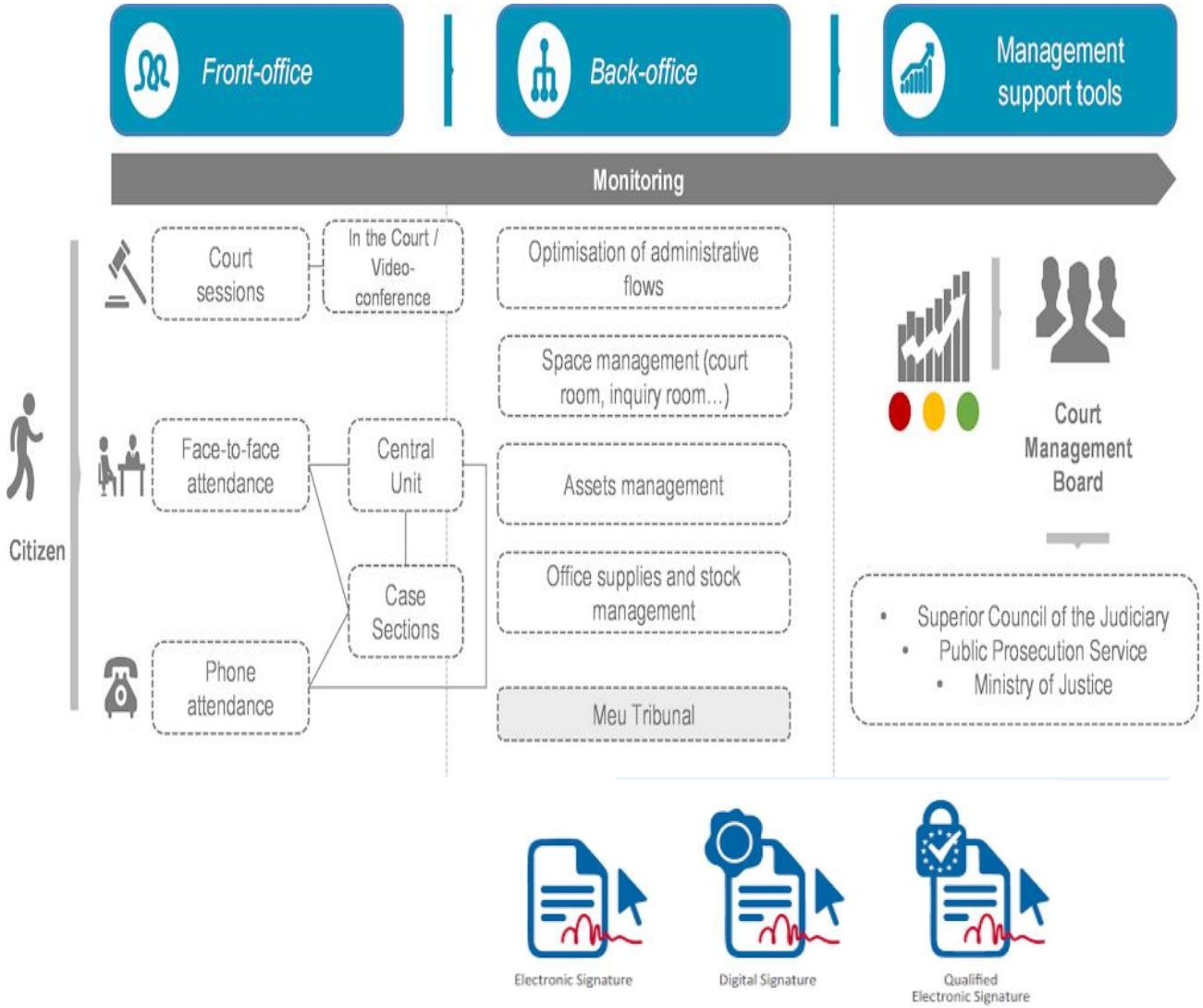
Emerging Technologies and Judicial Integrity: Challenges in Digital Transformation of Courts.







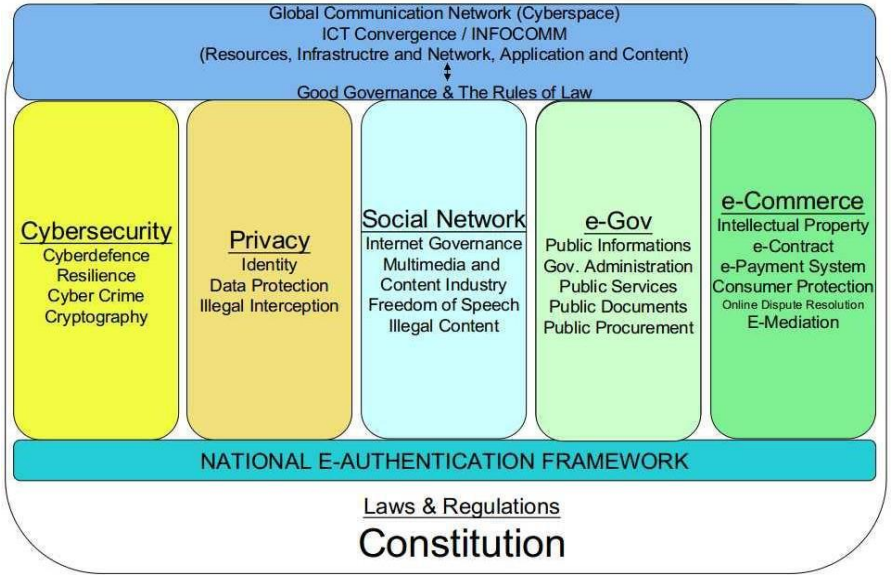
Oleh :

Dr. Edmon Makarim, S.Kom., SH., LL.M

CV

- Nama : Edmon Makarim
  : Dekan dan Dosen bidang HukumTelematika/Cyber Law FH-UI
  - Peneliti Senior, Lembaga Kajian Hukum Teknologi FHUI
- Pendidikan
  - 1988-1993, “S.Kom” (computer degree), Informatics Management, Universitas Gunadarma
  - 1989-1994, “S.H.” (law degree), Economics Law, FH-UI
  - 2002-2004, “LL.M.” (Lex Legibus Master/Master in Law), Comparative Law, University of Washington School of Law, Seattle.
  - 2004-2009, “Doctor” (Doctoral of Law Sciences, FHUI, Depok).
- Pengalaman & Organisasi
  - 1994-1996, Assistant of Lawyer (“SHR Law Firm”)
  - 1996-1999, In-house Legal Counsel (“Sisindosat telematics co)
  - Jan 2008-Dec 2009, Staf Ahli Menteri Bidang Hukum, Depkominfo.
  - 2013-2015, anggota dewan penasehat, masyarakat telematika indonesia.
  - 2013-2015, anggota dewan penasehat, Komisi Informasi Publik DKI Jakarta
  - 2013–present: arbiter (BAM-HKI), Panelist online Dispute Resolution (PANDI), bidang hukum (PAPPRI), Anggota Dewan Penasehat (Masyarakat Fotografi Indonesia).
  - 2016, Anggota Dewan Penasehat, Ikatan Alumni Magister Notariat FHUI
  - 2022 Ketua BKS FH PTN se Indonesia
- Buku:
  - Pengantar Hukum Telematika
  - Tanggung Jawab Penyelenggara Sistem Elektronik
  - Notaris dan Transaksi Elektronik
  - Konstitusi dan Telematika
- Pengembang Sistem Kodifikasi & Informasi Hukum Elektronik (e-Codification & Legal Information System/eclis.id)

Research's Roadmap



Amanat Konstitusi vs Internet

Bahwa sesungguhnya kemerdekaan itu ialah hak segala bangsa dan oleh sebab itu, maka penjajahan di atas dunia harus dihapuskan, karena tidak sesuai dengan perikemanusiaan dan perikeadilan.

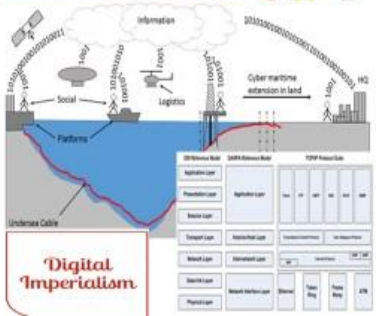
Dan perjuangan pergerakan kemerdekaan Indonesia telah sampailah kepada saat yang berbahagia dengan selamat sentausa mengantarkan rakyat Indonesia ke depan pintu gerbang kemerdekaan Negara Indonesia, yang merdeka, bersatu, **berdaulat**, adil dan makmur.

Atas berkat rakhmat Allah Yang Maha Kuasa dan dengan didorongkan oleh keinginan luhur, supaya berkehidupan kebangsaan yang **bebas**, maka rakyat Indonesia menyatakan dengan ini kemerdekaannya.

Kemudian dari pada itu untuk membentuk suatu Pemerintah Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial, maka disusunlah Kemerdekaan Kebangsaan Indonesia itu dalam suatu UndangUndang Dasar Negara Indonesia, yang terbentuk dalam suatu susunan Negara Republik Indonesia yang **berkedaulatan rakyat** dengan berdasarkan kepada Ketuhanan Yang Maha Esa, **Kemanusiaan Yang Adil dan Beradab**, Persatuan Indonesia dan Kerakyatan yang dipimpin oleh hikmat kebijaksanaan dalam Permusyawaratan/ Perwakilan, serta dengan mewujudkan suatu Keadilan sosial bagi seluruh rakyat Indonesia.

Siapakah Pemilik dan Pengendali *Resources* ?

- Signal & Frequencies
- Code & Crypto
- Computer Program
- Network Infrastructure
- Central of Registry (IP address & Domain Name)
- Content & Application
- Global Standard ?
- Privacy & Personal Data



Th	Judul Kegiatan	Keluaran
1999	Legal framework for e-commerce 1999	RUU-IETE => UU 11/2008 + PP 82/2012
2003	Indonesian Telematics Law/ Cyberlaw (legal framework)	Modul Perkuliahan + Buku Ajar: Kompilasi Kajian Hukum Telematika
2009	Electronic System Provider Liability for Implementing the IT Governance	Buku Ajar: Tanggung Jawab PSE
20102 011	Telematics and Constitutional Rights and Liability Development	Artikel Jurnal Nasional dan Internasional serta Buku Ajar
20102 011	Notary and e-Transaction (cybernotary)	Artikel Jurnal Nasional dan Jurnal Internasional serta Buku Ajar
20112 012	Privacy & Data Protection,	Revisi Buku Ajar + RUU Intersepsi Masukan Rancangan Peraturan Menteri Kominfo ttg Privacy dan Informasi Komersial (spamming)
2014	Information Security & Resilience	RUU Sandi + Rancangan Perpres Cybersecurity
2014	National e-Authentication Framework for ID: National e-Identity Management	Artikel Jurnal Nasional dan Jurnal Internasional serta revisi Buku Ajar
2014	Trust Services by Community: Community Certification Authority	Artikel Jurnal Nasional dan Jurnal Internasional serta revisi Buku Ajar
2015	National e-Authentication for Public Document in Government Administration & Public Services	Artikel Jurnal Nasional dan Jurnal Internasional serta revisi Buku Ajar

e-CLIS

eCLIS.id

e-Codification & Legal Information System => a collaboration system:

- **Codification, Compilation, Analysis, Evaluation, Syncronization, Harmonization of Laws and Regulation** => National, Regional and International

Fast

Clear

Interactive & informative

Multi-stakeholders

Integrated + Collaborative

Collecting & Sharing

Kodifikasi & Kompilasi

KODIFIKASI HUKUM INDONESIA

Code 1 Ketentuan Umum
Code 2 Tujuan, Asas, Dan Ruang Lingkup
Code 3 Bentuk Dan Kedaulatan Negara
Code 4 Majelis Permusyawaratan Rakyat
Code 5 Kekuasaan Pemerintahan Negara
Code 6 Kementerian Negara
Code 7 Pemerintahan Daerah
Code 8 Dewan Perwakilan Rakyat
Code 9 Dewan Perwakilan Daerah
Code 10 Pemilihan Umum
Code 11 Hal Keuangan
Code 12 Badan Pemeriksa Keuangan
Code 13 Kekuasaan Kehakiman
Code 14 Wilayah Negara
Code 15 Warga Negara Dan Penduduk
Code 16 Hak Asasi Manusia
Code 17 Agama
Code 18 Pertahanan Dan Keamanan
Code 19 Pendidikan Dan Kebudayaan
Code 20 Perekonomian Nasional
Code 21 Kesejahteraan Sosial & Pelayanan Publik
Code 22 Bendera, Bahasa, Dan Lambang Negara, Serta Lagu Kebangsaan
Code 23 Perubahan Undang-Undang Dasar Dan Peraturan Perundang-Undangan
Code 24 Hukum Pidana
Code 25 Hukum Perdata
Code 26 Hukum Administrasi Negara
Code 27 Hukum Acara
Code 28 Hukum Internasional
Code 32 Adat Dan Kearifan Lokal
Code 33 Ilmu Pengetahuan dan Teknologi

Notes:
Compilation is the organizing of existing ordinances, usually by subject matter, and then placing the ordinances in chronological order within each subject. Compilation is the first step in codification.

Pasal 28C

(1) Setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan memperoleh manfaat dari **ilmu pengetahuan dan teknologi, seni dan budaya**, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia. **)

(2) Setiap orang berhak untuk memajukan dirinya dalam memperjuangkan haknya secara kolektif untuk membangun masyarakat, bangsa dan negaranya. **)

Pasal 31

(1) Setiap warga negara berhak mendapat pendidikan. ****)

(2) Setiap warga negara wajib mengikuti pendidikan dasar dan pemerintah wajib membiayainya. ****)

(3) Pemerintah mengusahakan dan menyelenggarakan satu sistem pendidikan nasional, yang meningkatkan keimanan dan ketakwaan serta akhlak mulia dalam rangka mencerdaskan kehidupan bangsa, yang diatur dengan undang-undang. ****)

(4) Negara memprioritaskan anggaran pendidikan sekurang-kurangnya dua puluh persen dari anggaran pendapatan dan belanja negara serta dari anggaran pendapatan dan belanja daerah untuk memenuhi kebutuhan penyelenggaraan pendidikan nasional. ****)

(5) Pemerintah memajukan **ilmu pengetahuan dan teknologi** dengan menjunjung tinggi nilai-nilai agama dan persatuan bangsa untuk kemajuan peradaban serta kesejahteraan umat manusia. ****)

Pasal 32

(1) Negara **memajukan kebudayaan nasional Indonesia** di tengah peradaban dunia dengan menjamin kebebasan masyarakat dalam memelihara dalam mengembangkan nilai-nilai budayanya. ****)

(2) Negara menghormati dan memelihara bahasa daerah sebagai kekayaan budaya nasional. ****)

Pasal 33

(1) Perekonomian disusun sebagai usaha bersama berdasar atas asas kekeluargaan.

(2) Cabangcabang produksi yang penting bagi negara dan yang menguasai hajat hidup orang banyak dikuasai oleh negara.

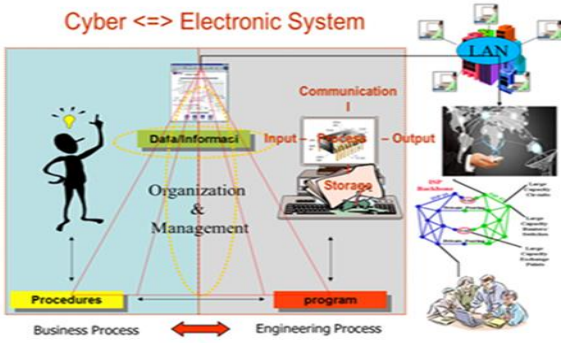
(3) Bumi dan air dan kekayaan alam yang terkandung di dalamnya dikuasai oleh negara dan dipergunakan untuk sebesarbesar kemakmuran rakyat.

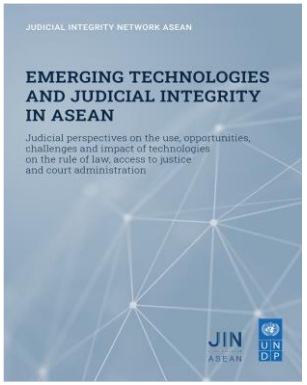
(4) Perekonomian nasional diselenggarakan berdasar atas demokrasi ekonomi dengan prinsip kebersamaan, efisiensi berkeadilan, berkelanjutan, berwawasan lingkungan, kemandirian, serta dengan menjaga keseimbangan kemajuan dan kesatuan ekonomi nasional. ****)

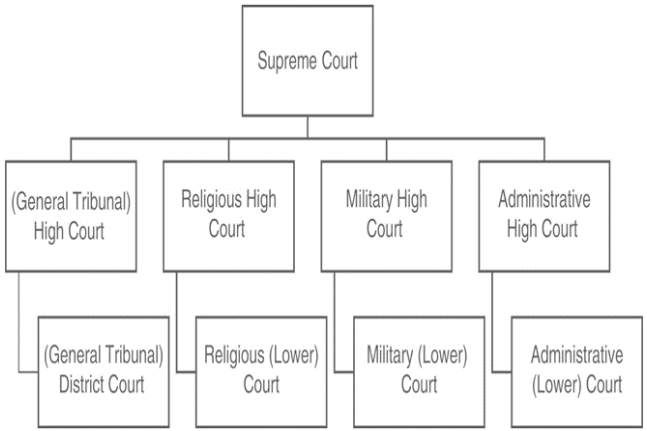
(5) Ketentuan lebih lanjut mengenai pelaksanaan pasal ini diatur dalam undang-undang. ****)

Intro

- Transformasi adalah perapihan kembali setiap *business models/process* dari setiap Organisasi dan Management menjadi suatu penyelenggaraan *engineering process* yang akuntabel & sustainable. Mencakup internal dan eksternal organisasi itu sendiri. Dalam konteks institusi public maka eksternal adalah pelayanan public itu sendiri.
- Are we trust with the "*digital default principle*" or "*conventional principle*"..?? ⇔ *cost effective*.
- *Utility of Technology vs Sosial Justice ⇔ Social Construction by Tech vs Law is Social Engineering*







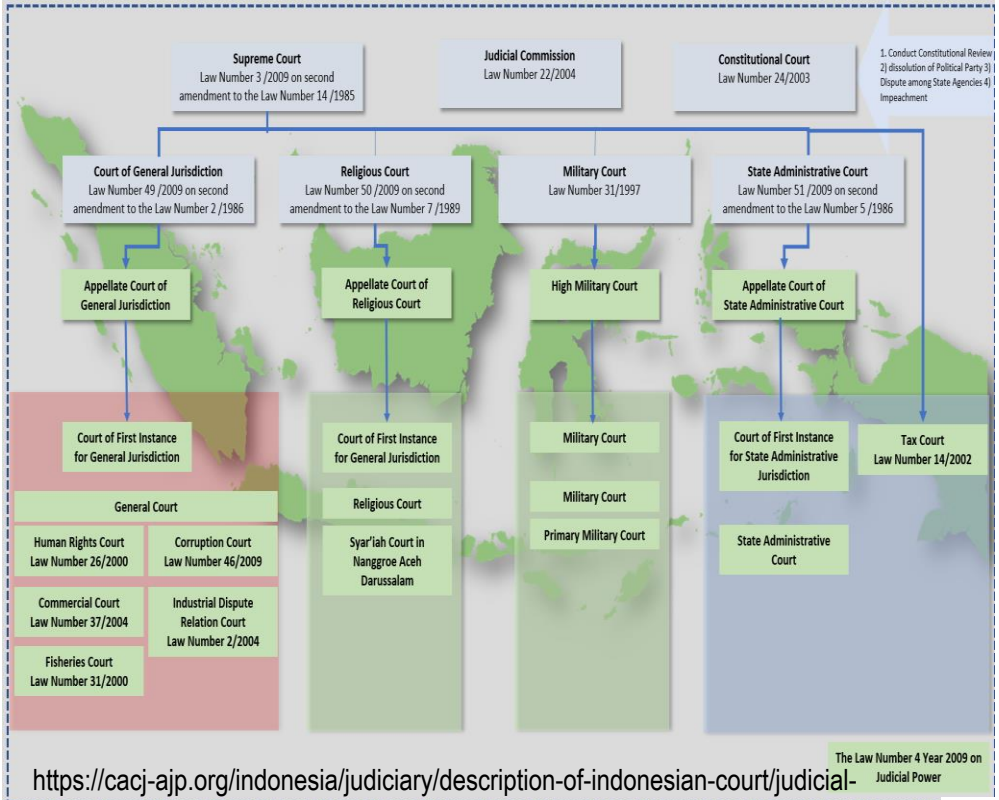
The Bangalore Principles include six values:
Value 1: **Independence**:
Value 2: **Impartiality**:
Value 3: **Integrity**:
Value 4: **Propriety**:
Value 5: **Equality**:
Value 6: **Competence and Diligence**:

Courts across the world are engaging in a variety of projects and long-term programmes, working with international agencies as partners and donors, to *modernize their justice systems*, including:
• case management systems,
• virtual proceedings,
• electronic filing and storage of documents and evidence,
• asynchronous communication between litigants and with the court,
• electronic scheduling, and
• the introduction of new tools such as online dispute resolution, and AI predictive tools.

Judicial integrity is a broad concept that includes a number of key elements of judging to ensure *strong, fair and rights-respecting justice systems*:
• Transparency in decision making
• Transparency in court administration
• Predictability of case timeframes
• Equal access regardless of status, money, or identity
• Equal treatment regardless of status, money, or identity
• Mechanisms to prevent bribery
• Mechanisms to prevent gendered or identity-based threats
• Due process
• Judicial independence
• Separation of political and judicial roles and institutions

Some Critical points:
- System Integration ⇔ vertical, Horizontal & Longitudinal Integration => e-filing/archiving
- Legalization & Notarization
- Trust services ⇔ National e-Authentication
- Payment + duty stamp
- Privacy & Data Protection
- Sovereignty & National Security

++ Cloud, AI/machine learning, Big Data, IoT, etc.



https://cacj-ajp.org/indonesia/judiciary/description-of-indonesian-court/judicial-commission/

National Legal System

History + Source of Law + Outside Influence and Conflict of Interest

(International Convention vs National Interest/Constitution)

Elements;

- Substance + Hierarchy
- Structure
- Legal Culture

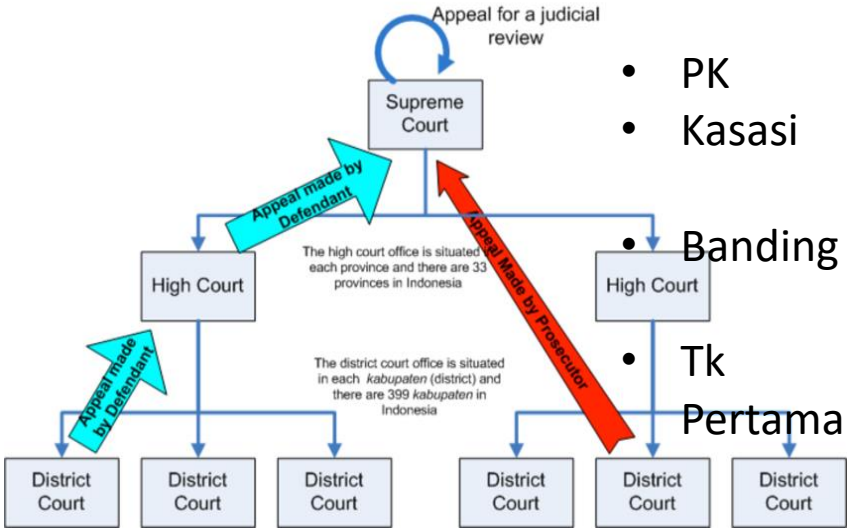
Legal Information System

- From the information and communication perspective ⇔ processing negative feedback to positive
- Will it create prosperity or misery?

Implementation

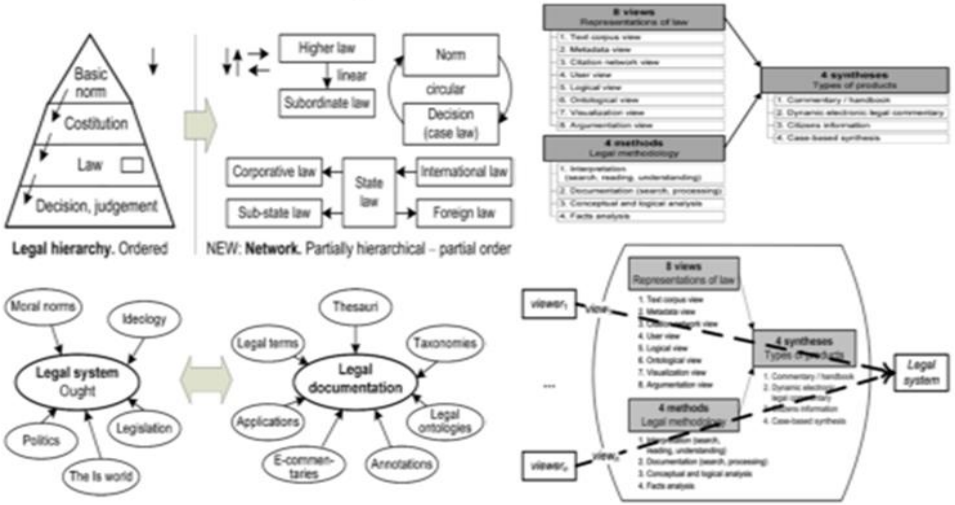
- Philosophical
- Sociological
- Juridical

- A "code" with the rooted system?
- Are the information easy to find and understandable? => consistent legal algorithm (synchronised + harmonized)
- Is the communication in forming and socializing processes good enough? => transparancy, inclusive and participatory
- the structure and organization of Implementing Agency would be efficient and effective ?



- PK
- Kasasi
- Banding
- Tk Pertama

Law Hierarchy to Network



Vytautas Čyras), Friedrich Lachmayer, and Erich Schweighofer, Views to Legal Information Systems and Legal Sublevels

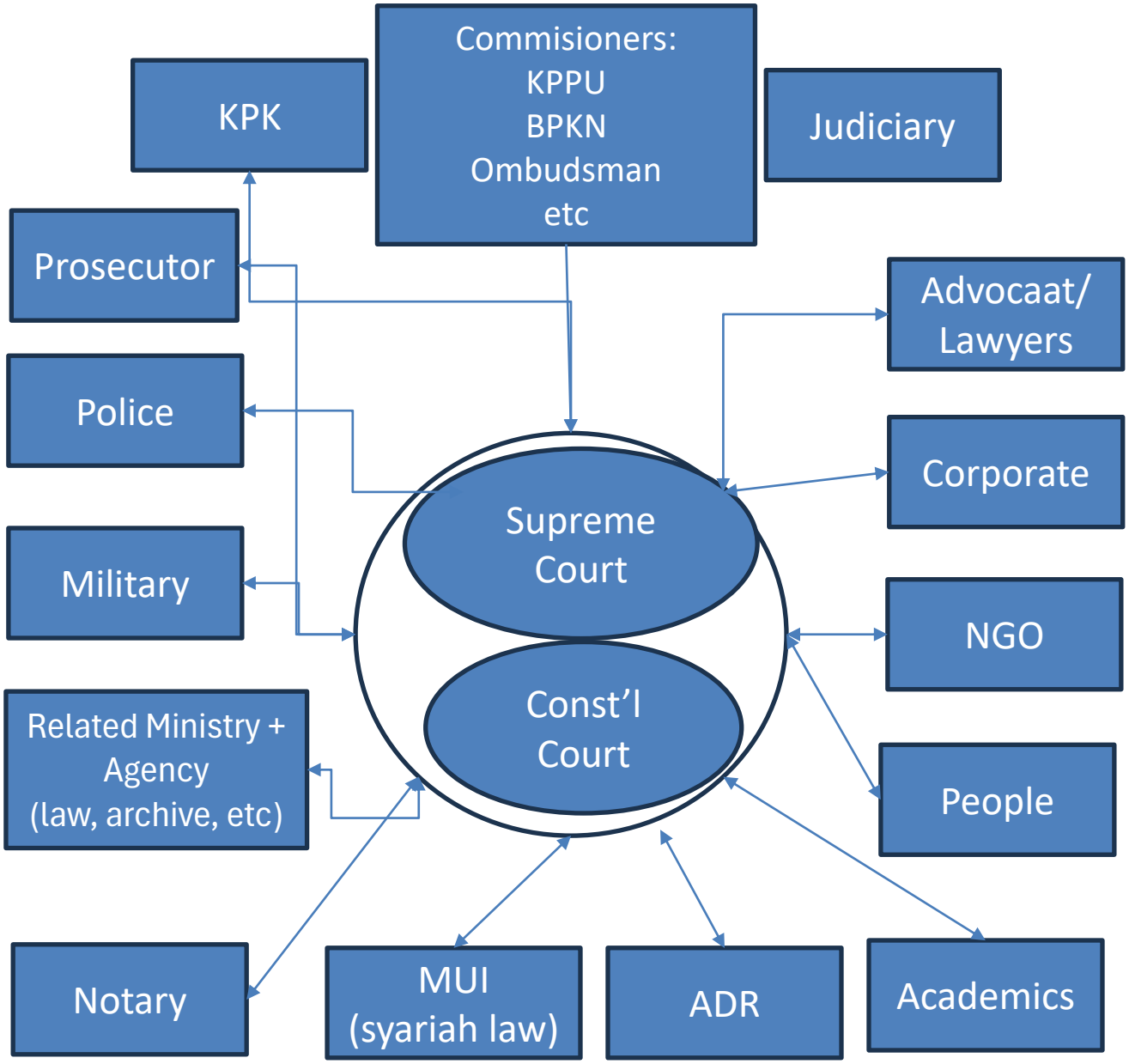
e-Justice

E-justice initiatives include the strategies, process (re)engineering, automation, data collection, integration of systems as well as online dispute resolution, e-filing, remote court process and technologies used to digitize, store, and provide access to legal documents and evidence.

Digitization is the process of converting existing processes and content from analog into digital formats. This includes developing online forms and portals to submit documents or access decisions to make existing in-person court processes available online.

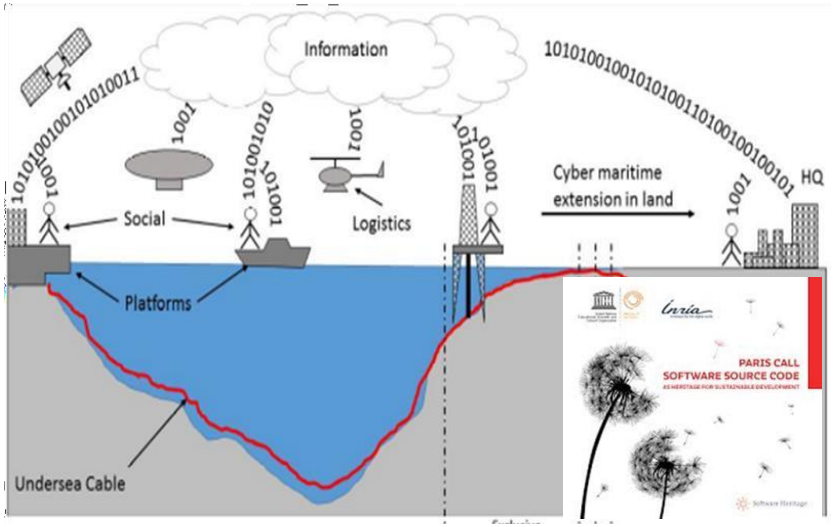
Digitalization is the use of digital technologies to change justice processes and business models. This includes digital technologies that allow for completely new ways of delivering or administering justice.

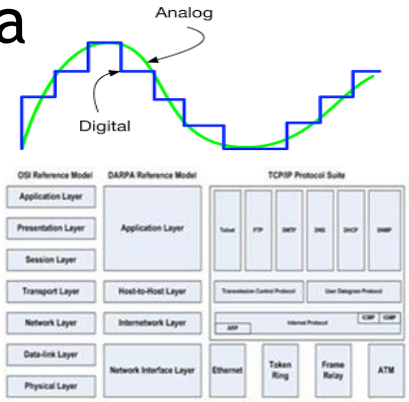
Digital Transformation is the cultural change in systems and institutions through digital technology. This includes *user-centred design* and technologies that allow employers and users to work differently.

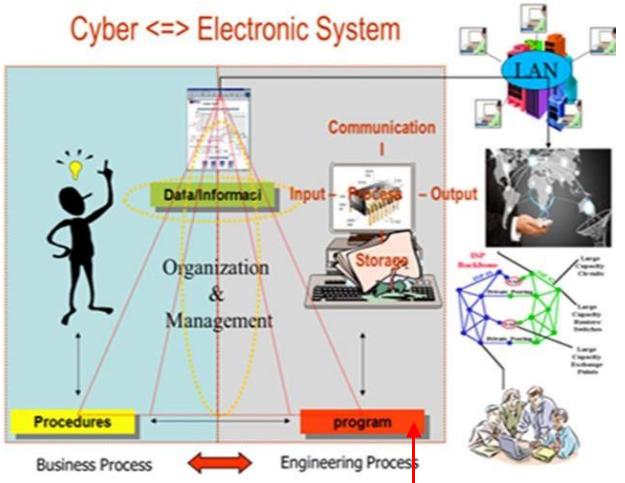


To what extent we can have trustworthiness for all of the e-system components => evidence, decision and archives => legal certainty, time constraint & fair ++ predictive

Cyber: Signal & Code ⇔ S/W + Data







Lack of Security

Owns & control digital *resources* ➔

- Signal & frequency
- IP Address & DNS
- **Code**: ***Crypto***, Software & Data
- Privacy & Personal Data ?

Trust & Secure ⇔ Kejelasan "Code/ command & "Control" ⇔ Resiko, Mitigasi & Tanggung Jawab Hukumnya + Ketersediaan dan Keautentikan Data

InterNet ⇔ common heritage for mankind..???

Ethics => Privacy, Accuracy, Property, Accesibility, Responsibility, Liability, Due Process, Accountability

Sistem informasi & Komunikasi Global

Information Security ⇔ Secured Communication

1. Confidentiality
2. Integrity
3. Availability

==========

1. Authorization
2. Authenticity
3. Non-Repudiation

Evidential Purpose

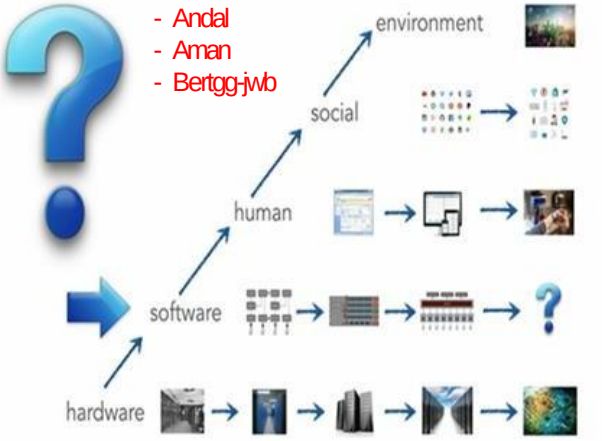
E-authentication = E-signatures ?

	Confidentiality	Integrity	Authencity	Authorization	Non Repudation
minimum	X	X	X	X	X
Intermediate	√	√	√	√	X
strong	√	√	√	√	√

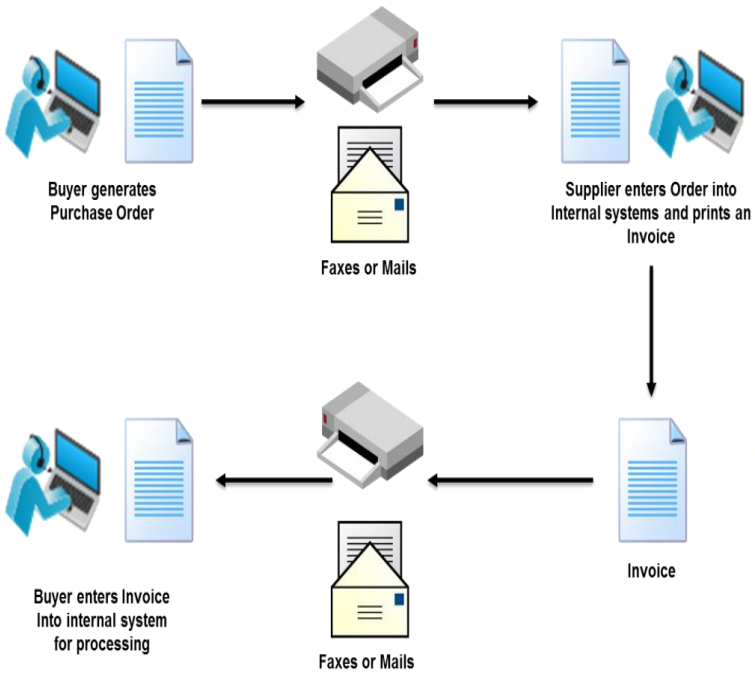
- *Functional Equivalent Approach ➔ writing, signed, original*
- *Trustworthiness of the Content, depends on trustworthiness of the process ⇔ the accredited e-system would create the authentic document which non repudiable*
- *No security ➔ no evidence ➔ no deal [Thomas J. Smedinghoff].*

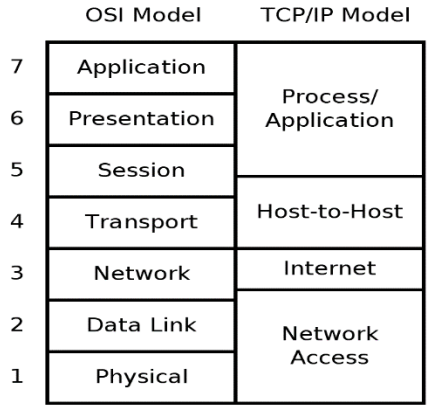
Akuntabilitas:

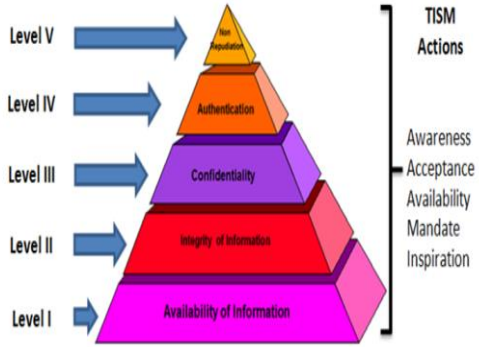
- Andal
- Aman
- Bertgg-jwb



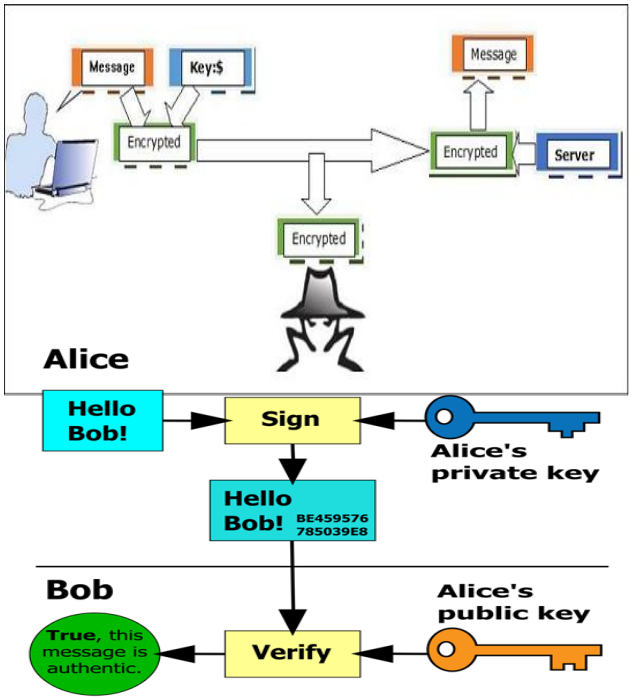
Transaksi via EDI







Transaksi via internet



Security Property	Meaning
Confidentiality	Information is only available to the people intended to use or see it.
Integrity	Information is changed only in appropriate ways by the people authorized to change it.
Availability	Apps and services are ready when needed and perform acceptably.
Authentication	A person's identity is determined before access is granted if anonymous people are not allowed.
Authorization	People are allowed or denied access to the app or app resources.
Nonrepudiation	A person cannot perform an action and then later deny performing the action.

Source: Mike Gualtieri, Principal Analyst, Forrester Research

Dasar Pemikiran: Informasi yang dihasilkan SE Security = Bobot Kekuatan Pembuktian

- *"Where information is recorded by mechanical means without the intervention of a human mind, the record made by the machine admissible in evidence, provided of course, it is accepted that the machine is reliable" [Professor Smith, 1981]*
- *Computers would be useless if they were not able to record information with a fair degree of reliability, which consist of 2 elements;*
  - *The trustworthiness of the Content.*
  - *The trustworthiness of the Process*

Secured communication ⇔ secured information

- Arsitektur **internet tidak diciptakan *by design* untuk menjamin keamanan informasi**
- Informasi yang ditransmisikan melalui internet pada dasarnya tdk dijamin keotentikannya
- ***No security -> no transaction evidence -> no deal***
- Transaksi digital membutuhkan teknologi yang menjamin keotentikan informasi yang ditransaksikan dan para pihak yang terlibat dalam transaksi
- **Siapa dan bagaimana cara menjamin keotentikan informasi yang disampaikan melalui internet?**

EIT LAW Article 15

AMAN

ANDAL

Bertgg Jawab

Jika sistem elektronik terjamin keandalannya, maka transaksi yang digunakan dalam suatu sistem elektronik pun akan terjaminkeandalannya.

Penyelenggara Sistem Elektronik

PSE Lingkup Publik

Instansi dan institusi yang ditunjuk oleh Instansi Penyelenggara Negara, tetapi tidak termasuk PSE yang merupakan otoritas pengatur dan pengawas sektor keuangan.

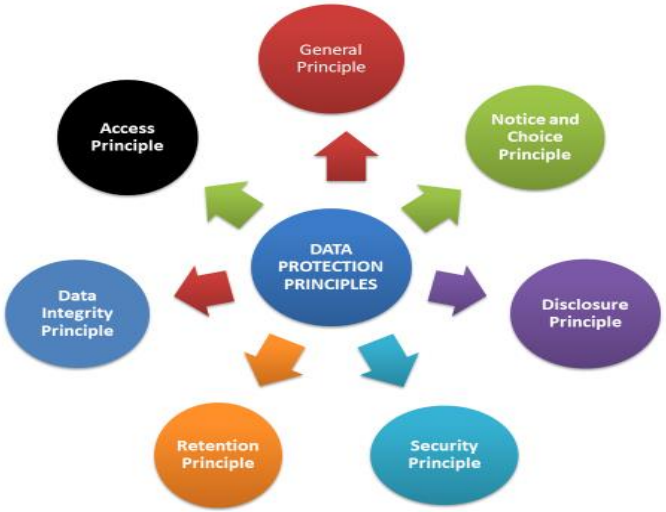
PSE Lingkup Privat

PSE yang diselenggarakan oleh Orang, Badan Usaha dan masyarakat.

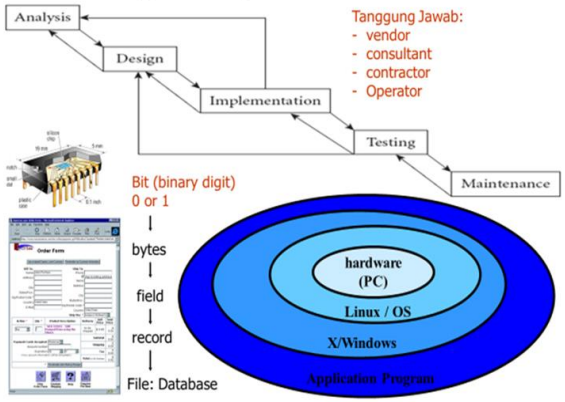
Baik PSE publik maupun privat harus terdaftar sebelum pengguna dapat menggunakan sistemnya. Prosedur pendaftaran mengacu kepada Peraturan Kominfo Nomor 36/2014 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik

Engineering process seluruh PSE harus sesuai dengan ketentuan keandalan Kominfo dan ketentuan keamanan dari BSSN.

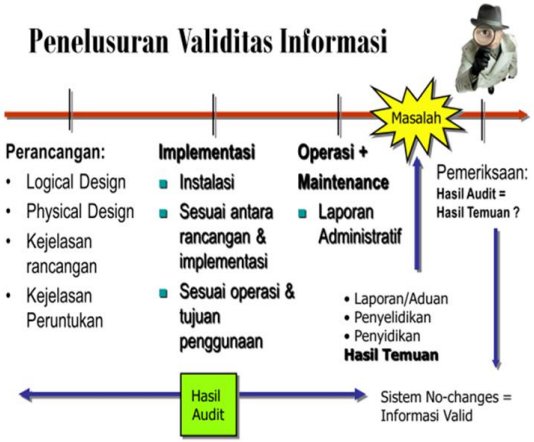
Seluruh PSE harus memastikan penyelenggaraannya *comply* dengan ketentuan mengenai Perlindungan Data Pribadi yang diatur dalam UU ITE dan Peraturan Kominfo Nomor 20/2014 tentang Perlindungan Data Pribadi dalam Sistem Elektronik



Pengembangan Sistem Informasi



Penelusuran Validitas Informasi



UU ITE + PP 82/2012 => 71/2019, PSTE => Akuntabilitas

- Handal, Aman dan Bertanggung jawab
- IE/DE merupakan alat bukti yang sah
- Standar Minimum Penyelenggaraan, khusus utk pelayanan publik perlu Sertifikasi Kelaikan => menjamin pelaksanaan IT Governance
  - mencakup Komponen2 IS => H/W, S/W, procedure, B/W dan Content
  - Mencakup Fungsi-fungsi => I,P, O, S, C
  - BCP, DRC, Back-up data,
  - Personal Data Protection
  - Penggunaan e-sign + CSP/CA
  - dsb.
- SE utk non-pelayanan publik => Pendaftaran + Sertifikasi Keandalan (optional/fakultatif).

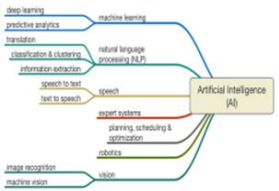
Big Data + Analytics + Artificial Intelligence in Law

- A **legal expert system** is a domain-specific expert system that uses artificial intelligence to emulate the decision-making abilities of a human expert in the field of law.[1]:172 Legal expert systems employ a rule base or knowledge base and an inference engine to accumulate, reference and produce expert knowledge on specific subjects within the legal domain. <wikipedia>, Example Chatbot, AI lawyers, etc.

(+): penetration of the legal services to the poor people equal righs and justice

(-) disruptive to the the existing legal services/lawyers

How about the liability in case of the mailfunction/not working properly => incorrect answer (no warranties)

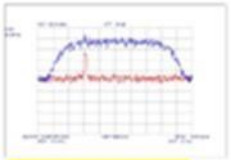


Conventional vs AI Computing

Dimension	Conventional Programming	Artificial Intelligence
Processing	Primarily algorithmic	Includes symbolic conceptualization
Nature of input	Must be complete	Can be incomplete
Search Approach	Frequently based on algorithms	Frequently use rules and heuristics ("rules of thumb")
Explanation	Usually not provided	Provided
Focus	Data, information	Knowledge
Maintenance and update	Usually difficult	Relatively easy changes can be made in self-contained modules
Reasoning capability	No	Yes

- Rule driven based
- data driven based

Alat Bukti Yang Sah + Kekuatan Pembuktian
Ps. 5 + 6 + 11 UU ITE



Perluasan Alat Bukti

Paradigma KUHAP & UU Tipikor

UU-ITE

Alat Bukti Lain

Paradigma UU Pencucian Uang, Terorisme, Narkotika, dst.

Petunjuk

Writing, signed & original

Confidentiality, Integrity, Authorization, Authenticity, Non-Repudiation

Autentik & Terpercaya

Suatu Informasi Elektronik harus diakui bernilai secara Hukum sejak dalam bentuk originalitasnya secara elektronik sepanjang berasal dari sistem elektronik yang layak dipercaya => lihat ps.16 UU ITE

Tanda Tangan Elektronik + Sertifikat Elektronik ⇔ Autentik + Terpercaya
(penggunaan produk Kriptografi dalam pengamanan informasi)

Apakah Fungsi Tanda Tangan ?

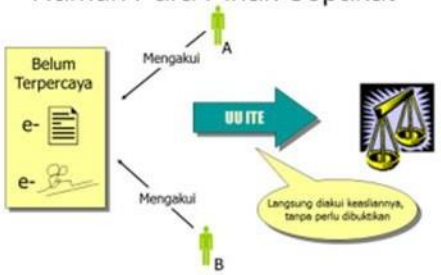
- Representasi Simbolik
- Autorisasi dan Autentikasi
- Persetujuan
- pengamanan Informasi

Tanda Tangan Elektronik
- Verikasi
- Autentikasi

- Tanda tangan tanpa sertifikat
- Tanda tangan dengan **Sertifikat**

- Terdaftar
- Tersertifikasi
- Berinduk

Jika SE "Belum Terpercaya": Namun Para Pihak Sepakat



Informasi Elektronik = Autentik ?

- Suatu tulisan dibwh tangan yg diakui oleh org 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

Jika SE "Belum Terpercaya" dan Terjadi Perselisihan

Jika SE "Terpercaya" dan telah Terakreditasi

Public Key Infrastructure

1887 BW

National Root CA ?

Government Root CA

Non Gov't/ Private CA

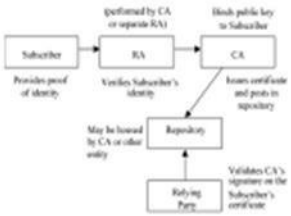
Community CA

Private CA Asing ???

Gov't Administration

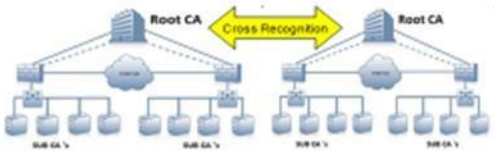
E-Public Services

Mesh PKI



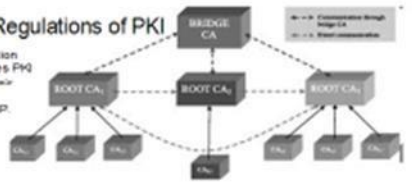
Permen Kominfo 11/2018 P.Sert.Elektronik

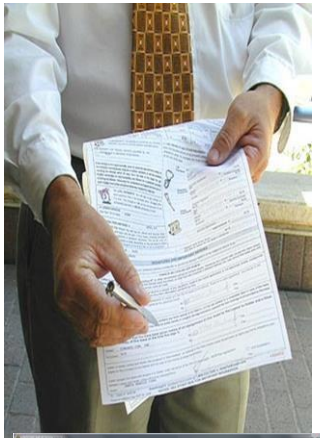
Perpres 95/2018 SPBE

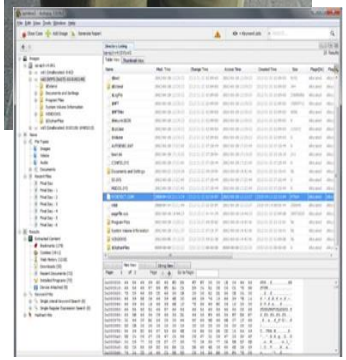


Models Regulations of PKI

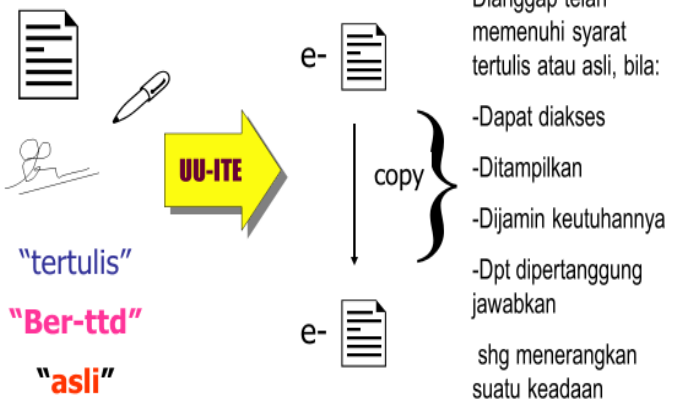
- Self-Regulation
- communities PKI
- "Mesh" PKI
- Peer-to-peer
- "bridge" CSP







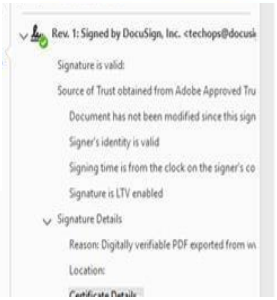
Informasi Elektronik = Informasi di atas Kertas (*functional-equivalent-approach*) => ps.6 UU ITE

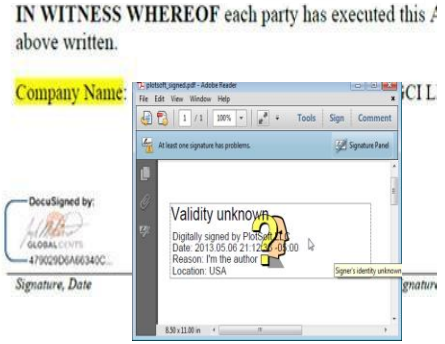


Dianggap telah memenuhi syarat tertulis atau asli, bila:

- -Dapat diakses
- -Ditampilkan
- -Dijamin keutuhannya
- -Dpt dipertanggung jawabkan

shg menerangkan suatu keadaan

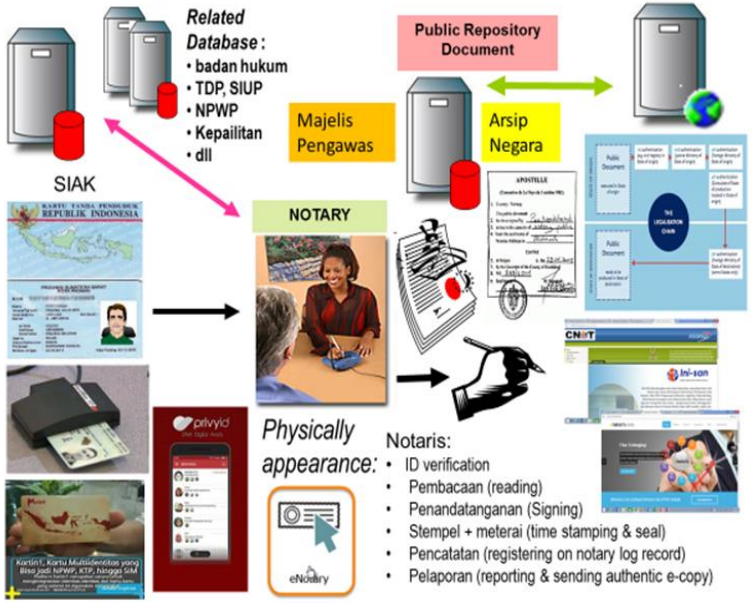




Pelayanan Publik (UU 25/2009)	UU 30/2014 Administrasi Pemerintahan
Pasal 24 Dokumen, akta, dan sejenisnya yang berupa produk elektronik atau nonelektronik dalam penyelenggaraan pelayanan publik dinyatakan sah sesuai dengan peraturan perundang-undangan.. Penjelasan: Cukup Jelas	Pasal 1 1. Administrasi Pemerintahan adalah tata laksana dalam pengambilan keputusan dan/atau tindakan oleh badan dan/atau pejabat pemerintahan. 2. Fungsi Pemerintahan adalah fungsi dalam melaksanakan Administrasi Pemerintahan yang meliputi fungsi pengaturan, pelayanan, pembangunan, pemberdayaan, dan pelindungan. 11. **Keputusan Berbentuk Elektronis** adalah Keputusan yang dibuat atau disampaikan dengan menggunakan atau memanfaatkan media elektronik. 12. **Legalisasi** adalah pernyataan Badan atau Pejabat Pemerintahan tentang keabsahan suatu salinan surat atau dokumen administrasi pemerintahan yang dinyatakan sesuai dengan aslinya; 13. Sengketa Kewenangan adalah klaim penggunaan Wewenang yang dilakukan oleh 2 (dua) Pejabat Pemerintahan atau lebih yang disebabkan oleh tumpang tindih atau tidak jelasnya Pejabat Pemerintahan yang berwenang menangani suatu urusan pemerintahan. 14. Konflik Kepentingan adalah kondisi Pejabat Pemerintahan yang memiliki kepentingan pribadi untuk menguntungkan diri sendiri dan/atau orang lain dalam penggunaan Wewenang sehingga dapat mempengaruhi netralitas dan kualitas Keputusan dan/atau Tindakan yang dibuat dan/atau dilakukannya. 15. Warga Masyarakat adalah seseorang atau badan hukum perdata yang terkait dengan Keputusan dan/atau Tindakan.

Pasal 7 UU 14/2008 KIP

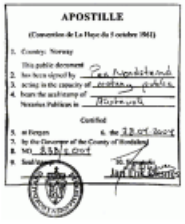
1. Badan Publik wajib menyediakan, memberikan dan/atau menerbitkan Informasi Publik yang berada dibawah kewenangannya kepada Pemohon Informasi Publik, selain informasi yang dikecualikan sesuai dengan ketentuan
2. Badan Publik wajib menyediakan Informasi Publik yang akurat, benar, dan tidak menyesatkan.
3. Untuk melaksanakan kewajiban sebagaimana dimaksud pada ayat (2), Badan Publik harus membangun dan mengembangkan sistem informasi dan dokumentasi untuk mengelola Informasi Publik secara baik dan efisien sehingga dapat diakses dengan mudah.
4. Badan Publik wajib membuat pertimbangan secara tertulis setiap kebijakan yang diambil untuk memenuhi hak setiap Orang atas Informasi Publik.
5. Pertimbangan sebagaimana dimaksud pada ayat (4) antara lain memuat pertimbangan politik, ekonomi, sosial, budaya, dan/atau pertahanan dan keamanan negara.
6. Dalam rangka memenuhi kewajiban ayat (1) sampai dengan ayat (4) Badan Publik dapat memanfaatkan sarana dan/atau media elektronik dan nonelektronik.



Hague Agreement 1961

(*The Convention Abolishing the Requirement of Legalization for Foreign Public Documents*) => *Electronic Apostile.*

Article 2
Each Contracting State shall exempt from legalisation documents to which the present Convention applies and which have to be produced in its territory. For the purposes of the present Convention, ***Legalisation*** *means only the formality by which the diplomatic or consular agents of the country in which the document has to be produced certify the authenticity of the signature, the capacity in which the person signing the document has acted and, where appropriate, the identity of the seal or stamp which it bears.*



- *Valitas Subyek => identitas (org & lembg), kapasitas, autorisasi.*
- *Validitas Obyek => keutuhan*

In April 2006, the HCCH and the National Notary Association of the USA officially launched the electronic Apostille Pilot Program (e-APP). Under the e-APP, the HCCH and the NNA are, together with any interested State, (or any of its internal jurisdictions), developing, promoting and assisting in the implementation of low-cost, operational and secure software for (i) the issuance and use of electronic Apostilles (**e-Apostilles**) and, (ii) the creation and operation of electronic Registers of Apostilles (**e-Registers**).

The e-APP modernises the operation of the Apostille Convention by extending it into the electronic medium without changing its nature and without having to change its content; the e-APP makes the overall operation of the Convention much more effective, dramatically enhances security and offers a very powerful and effective deterrent to fraud. The two main components of the e-APP consist of:

1) comprehensive explanatory material as to how Competent Authorities may use out-of-the-box PDF technology and digital certificates to issue e-Apostilles, and how third parties can use such e-Apostilles and,

2) open-source software for the creation and operation of e-Registers by Competent Authorities, and an explanation as to how third parties can use such e-Registers. An e-Register under the e-APP allows for easy online queries by third parties to verify the origin of an Apostille without Competent Authorities having to answer these queries individually by phone, email or otherwise. This being said, an e-Register as suggested under the e-APP does not allow for "fishing expeditions" – persons do not have unlimited access to all the information stored in an e-Register but can only verify whether or not an Apostille they have been presented with has really been issued by the Competent Authority whose name appears on the Apostille. To access the relevant e-Register, a person must provide the date and the number of the Apostille he or she has been presented with.

E-authentication = E-signatures ?

[OECD]

- **Authentication in Context**
- Authentication can mean a variety of things depending on the context in which the term is used. An Internet search on the term "authentication" yields a very broad range of definitions, some addressing authentication of persons or other entities, others addressing things, documents and systems. Across these definitions, authentication is accomplished through processes that have various degrees of detail and technical specificity. These processes are aimed at determining whether someone or something is, in fact, who or what it claims to be. As such, effective authentication is a key contributor to the establishment of a trust relationship in a digital environment. For the purposes of this guidance, authentication is defined as:
  - *A function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system.*
- This definition implies two processes and one result:
  - A claim related to a person, other entity or thing is presented (claiming process).
  - That claim is substantiated (substantiation process).
  - As a result, a degree of confidence, or lack thereof, in the claim is generated.

[UNCITRAL]

In some cases, the expression "electronic authentication" is used to refer to techniques that, depending on the context in which they are used, may involve various elements, such as:
- identification of individuals,
- confirmation of a person's authority (typically to act on behalf of another person or entity) or
- prerogatives (for example, membership in an institution or subscription to a service) or
- assurance as to the integrity of information.

- In some cases, the focus is on identity only, but sometimes it extends to authority, or a combination of any or all of those elements.

Procedures for signatures ?

- Most legal systems have special procedures or requirements that are intended to enhance the reliability of handwritten signatures. Some procedures may be mandatory in order for certain documents to produce legal effects. They may also be optional and available to parties that wish to act to preclude possible arguments concerning the authenticity of certain documents. Typical examples include the following:
- (*a*) Notarization. In certain circumstances, the act of signing has a particular formal significance due to the reinforced trust associated with a special ceremony. This is the case, for instance, with notarization, i.e. the certification by a notary public to establish the authenticity of a signature on a legal document, which often requires the physical appearance of the person before the notary;
- (*b*) Attestation. Attestation is the act of watching someone sign a legal document and then signing one's name as a witness. The purpose of attestation is to preserve evidence of the signing. By attesting, the witness states and confirms that the person whom he or she watched sign the document in fact did so. Attesting does not extend to vouching for the accuracy or truthfulness of the document. The witness can be called on to testify as to the circumstances surrounding the signing;
- (*c*) Seals. The practice of using seals in addition to, or in substitution of, signatures is not uncommon, especially in certain regions of the world. Signing or sealing may, for example, provide evidence of the identity of the signatory; that the signatory agreed to be bound by the agreement and did so voluntarily; that the document is final and complete; or that the information has not been altered after signing. It may also caution the signatory and indicate the intent to act in a legally binding manner.

[*Sources: UNCITRAL, Promoting Confidence in E-commerce: Legal issues on international use of electronic authentication & signature methods., 2009*]

Traditional authenticity vs e-Authentication

Paperbased *(keautentikan formil & material)*	**Electronic-based** *(functional equivalent approach)*
• Writing (Tertulis) • Signed (Bertanda-tangan) • Original (asli, tak berubah)	• Apa yang telah dituliskan/disimpan dpt ditemukan kembali • Terdapat informasi yang menemukan Subyek Hukum Yang bertgg-jawab • Apa yang tersimpan dan ditemukan tidak ada perubahan (terjamin keutuhannya).

• Pandangan Awam
  • Ditandatangani di atas meterai (kewajiban untuk pembuktian)
• Dokumen Publik
  • Bentuk fisik/cetak dan ditandatangani pejabat public yang bersangkutan
  • Double Legalization (oleh konsuler) vs Apostille
	Terjamin keterpercayaan (*trust*) terhadap keamanannya ➔ eIDAS (Electronic Identification and Authentication System)
	• Access to e-ID vs Credential system
	• e-registry + e-filing
	• Public Document Repository
	• Automated Clearing House
	• **UU Arsip => autentik, utuh dan terpercaya** ...???

• **Formal Requirement**
• kehadiran fisik pihak secara langsung penghadap dengan notaris (ps. 16 ayat (1) huruf l)
• pembacaan akta dihadapan para pihak dan para pihak mengerti, kecuali bila para pihak tidak minta untuk dibacakan (ps. 16 ayat (7))
• kehadiran dan tanda tangan para saksi-saksi yang tidak mempunyai hubungan darah atau perkawinan, kecuali bila ditentukan lain oleh UU (ps.39 dan 40)
• paraf para pihak, saksi dan notaris pada setiap halaman sebagai tindakan persetujuan.
	• **Material/Substantial Requirement:**
	  • C.I.A.N.A.
	  • Mendukung bukti bahwa aspek formal telah dilakukan
	  • Jaminan tidak adanya perubahan (teramankan)
	  • Ditunjang oleh rantai keautentikan (baik secara vertical maupun horizontal)
	  • Didukung oleh jaminan penyimpanan ketersediaan dokumen yang bersangkutan

Konvensional	Elektronik
Dokumen Yang Diterima sd akhir proses persidangan berbentuk kertas dan kemudian dialihkan ke bentuk elektronik	Dokumen Yang Diterima dari awal bentuk original nya adalah elektronik (harus dapat ditelusuri siapa orang yg bertgg jwb dan dokumen valid secara elektronik => terkonfirmasi secara elektronik)
Dlm hal transformasi dilakukan oleh para pihak, maka Pengadilan tentu memerlukan kepastian/ konfirmasi bahwa bukti adalah sah dan mengikat (diperoleh secara sah, relevan dan valid)	Semua bukti digital yang dihadirkan harus teramankan dengan baik ; - Jika dikirimkan secara elektronik harus melalui secured communication - Jika dikirimkan secara offline maka harus terenkripsi sesuai kebijakan kriptografi nasional
1. Jika dokumen pejabat maka menggunakan CA pemth 2. Jika dokumen privat maka hrs menggunakan TTE yang Tersertifikasi dan Berinduk ke pemth	1. Jika dokumen pejabat maka menggunakan CA pemth 2. Jika dokumen privat maka hrs menggunakan TTE yang Tersertifikasi dan Berinduk ke pemth
Jika dilengkapi meterai seharusnya menjadi pendukung sistem keautentikan	Meterai adalah sama dengan e-seal, harus dipastikan sbg pendukung rantai keautentikan
Meta data menjelaskan proses terakhir dari transformasi kertas menjadi digital	Idealnya, meta data dari berkas ybs menjelaskan semua proses yang telah dilalui.

Draft UNCITRAL Model LAW on eIDAS

* dlm konteks e-communication for international contract

Article 19. Electronic archiving

Where the law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement is met in relation to a data message if a method is used:

(a) To make the information contained in the data message accessible so as to be usable for subsequent reference;

(b) To indicate the time and date of archiving and associate that time and date with the data message;

(c) To retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and

(d) To retain such information, if any, as enables the identification of the origin and destination of a data message and the time and date when it was sent or received.

UU 30/2014 Administrasi Pemerintahan

- Pasal 1 angka (11) => Keputusan Berbentuk Elektronis adalah Keputusan yang dibuat atau disampaikan dengan menggunakan atau memanfaatkan media elektronik.

- BAB VII PENYELENGGARAAN ADMINISTRASI PEMERINTAHAN Bagian Keempat Keputusan Berbentuk Elektronis (Pasal 38)

(1) Pejabat dan/atau Badan Pemerintahan dapat membuat Keputusan Berbentuk Elektronis.
(2) Keputusan Berbentuk Elektronis wajib dibuat atau disampaikan apabila Keputusan tidak dibuat atau tidak disampaikan secara tertulis.
(3) Keputusan Berbentuk Elektronis berkekuatan hukum sama dengan Keputusan yang tertulis dan berlaku sejak diterimanya Keputusan tersebut oleh pihak yang bersangkutan.
(4) Jika Keputusan dalam bentuk tertulis tidak disampaikan, maka yang berlaku adalah Keputusan dalam bentuk elektronis.
(5) Dalam hal terdapat perbedaan antara Keputusan dalam bentuk elektronis dan Keputusan dalam bentuk tertulis, yang berlaku adalah Keputusan dalam bentuk tertulis.
(6) Keputusan yang mengakibatkan pembebanan keuangan negara wajib dibuat dalam bentuk tertulis.

Pasal 38
Ayat (1) Prosedur penggunaan Keputusan Berbentuk Elektronis berpedoman pada ketentuan peraturan perundangundangan yang mengatur tentang informasi dan transaksi elektronik.
Ayat (2) Untuk proses pengamanan pengiriman Keputusan, dokumen asli akan dikirimkan apabila dibutuhkan penegasan mengenai penanggung jawab dari Pejabat Pemerintahan yang menyimpan dokumen asli. Jika terdapat permasalahan teknis dalam pengiriman dan penerimaan dokumen secara elektronis baik dari pihak Badan dan/atau Pejabat Pemerintahan atau Warga Masyarakat, maka kedua belah pihak saling memberitahukan secepatnya.
Ayat (3) Cukup jelas.
Ayat (4) Cukup jelas.
Ayat (5) Cukup jelas.
Ayat (6) Cukup jelas.

Bab IV bagian ke VI- Legalisasi Dokumen:

Legalisasi (UU AdPem)

Pasal 73
(1) Badan dan/atau Pejabat Pemerintahan yang menetapkan Keputusan berwenang untuk melegalisasi salinan/fotokopi dokumen Keputusan yang ditetapkan.
(2) Legalisasi salinan/fotokopi dokumen sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh Badan dan/atau Pejabat Pemerintahan lain yang diberikan wewenang berdasarkan ketentuan peraturan perundang-undangan atau pengabsahan oleh notaris.
(3) Legalisasi Keputusan tidak dapat dilakukan jika terdapat keraguan terhadap keaslian isinya.
(4) Tanda Legalisasi atau pengesahan harus memuat:
a. pernyataan kesesuaian antara dokumen asli dan salinan/fotokopinya; dan
b. tanggal, tanda tangan pejabat yang mengesahkan, dan cap stempel institusi atau secara notarial.
(5) Legalisasi salinan/fotokopi dokumen yang dilakukan oleh Badan atau Pejabat Pemerintahan tidak dipungut biaya.

Pasal 74
(1) Keputusan wajib menggunakan bahasa Indonesia.
(2) Keputusan yang akan dilegalisasi yang menggunakan bahasa asing atau bahasa daerah terlebih dahulu diterjemahkan ke dalam bahasa Indonesia.
(3) Penerjemahan wajib dilakukan oleh penerjemah resmi.

Pasal 73
Ayat (1) Yang dimaksud dengan "salinan/fotokopi" adalah termasuk juga copy collationee.
Ayat (2) Yang dimaksud dengan "**dokumen**" adalah setiap informasi yang terdokumentasi dalam bentuk tertulis atau bentuk elektronik yang dikuasai oleh Badan dan/atau Pejabat Pemerintahan yang berkaitan dengan aktivitas penyelenggaraan pemerintahan dan/atau pelayanan publik.
Kewenangan notaris untuk mengesahkan dokumen dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.
Ayat (3) Yang dimaksud dengan "**terdapat keraguan**" adalah karena robek, penghapusan kata, angka dan tanda, perubahan, kata-kata yang tidak jelas terbaca, penambahan atau hilangnya lembar halaman yang merupakan bagian tidak terpisahkan dari dokumen.
Ayat (4) Cukup jelas.
Ayat (5) Cukup jelas.
Pasal 74 Cukup jelas.

UU Kearsipan	Penjelasan
Pasal 1 angka (3) Arsip adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa, dan bernegara. Pasal 3 Penyelenggaraan kearsipan bertujuan untuk: a. menjamin terciptanya arsip dari kegiatan yang dilakukan oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan, serta ANRI sebagai penyelenggara kearsipan nasional; b. menjamin ketersediaan arsip yang **autentik** dan **terpercaya** sebagai alat bukti yang sah;	Pasal 3 Huruf a Cukup jelas. Huruf b Yang dimaksud dengan "menjamin ketersediaan arsip yang autentik dan terpercaya sebagai alat bukti yang sah" adalah bahwa penyelenggaraan kearsipan harus dapat menjamin arsip sebagai rekaman kegiatan atau peristiwa yang dapat disediakan atau disajikan dalam kondisi autentik dan terpercaya, sehingga dapat berfungsi sebagai alat bukti yang sah maupun dapat menjadi sumber informasi dalam pelaksanaan kegiatan pada masa yang akan datang. Yang dimaksud dengan "arsip yang autentik" adalah arsip yang memiliki struktur, isi, dan konteks, yang sesuai dengan kondisi pada saat pertama kali arsip tersebut diciptakan dan diciptakan oleh orang atau lembaga yang memiliki otoritas atau kewenangan sesuai dengan isi informasi arsip. Yang dimaksud dengan "arsip terpercaya" adalah arsip yang isinya dapat dipercaya penuh dan akurat karena merepresentasikan secara lengkap dari suatu tindakan, kegiatan atau fakta, sehingga dapat diandalkan untuk kegiatan selanjutnya.

UU Kearsipan	Penjelasan
c. menjamin terwujudnya pengelolaan arsip yang andal dan pemanfaatan arsip sesuai dengan ketentuan peraturan perundang-undangan; d. menjamin pelindungan kepentingan negara dan hak-hak keperdataan rakyat melalui pengelolaan dan pemanfaatan arsip yang autentik dan terpercaya; e. mendinamiskan penyelenggaraan kearsipan nasional sebagai suatu sistem yang komprehensif dan terpadu; f. menjamin keselamatan dan keamanan arsip sebagai bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara; g. menjamin keselamatan aset nasional dalam bidang ekonomi, sosial, politik, budaya, pertahanan, serta keamanan sebagai identitas dan jati diri bangsa; dan h. meningkatkan kualitas pelayanan publik dalam pengelolaan dan pemanfaatan arsip yang autentik dan terpercaya.	Huruf c Yang dimaksud dengan "pengelolaan arsip yang andal" adalah pengelolaan arsip yang dilaksanakan berdasarkan sistem yang mampu menampung dan merespons kebutuhan perkembangan zaman. Sistem pengelolaan arsip yang andal memiliki kemampuan: menjaring atau menangkap (capture) semua arsip dari seluruh kegiatan yang dihasilkan organisasi; menata arsip dengan cara yang mencerminkan proses kegiatan organisasi; melindungi arsip dari pengubahan, pengurangan, penambahan, atau penyusutan oleh pihak yang tidak berwenang; menjadi sumber utama informasi secara rutin mengenai kegiatan yang terekam dalam arsip; dan menyediakan akses terhadap semua arsip berikut beserta metadatanya. Huruf d Yang dimaksud dengan hak-hak keperdataan rakyat meliputi: hak sosial, hak ekonomi, dan hak politik dan lainlain yang dibuktikan dalam arsip misalnya sertifikat tanah, ijazah, surat nikah, akte kelahiran, kartu penduduk, data kependudukan, surat wasiat, dan surat izin usaha. Huruf e Yang dimaksud dengan "mendinamiskan penyelenggaraan kearsipan nasional" adalah bahwa dengan adanya sistem yang komprehensif dan terpadu penyelenggaraan kearsipan menjadi lebih dinamis dan terarah. Huruf f Yang dimasud dengan "menjamin keselamatan dan keamanan arsip" adalah bahwa arsip baik secara fisik maupun informasinya harus dijaga keselamatan dan keamanannya, sehingga tidak mengalami kerusakan atau hilang. Arsip perlu dijaga kerahasiaanya dari pengaksesan oleh pihak yang tidak berhak, karena arsip merupakan bukti pertanggungjawaban dalam kehidupan bermasyarakat, berbangsa dan bernegara. Huruf g Yang dimaksud dengan "aset nasional" adalah kekayaan negara dan masyarakat baik secara ekonomi, sosial, politik, budaya, maupun aspek kehidupan lain yang terekam dalam arsip seperti daftar kekayaan negara maupun bukti-bukti kepemilikan yang harus dilindungi dan dijaga keselamatannya. Huruf h Yang dimaksud dengan "meningkatkan kualitas pelayanan publik" adalah penyelenggaraan kearsipan yang komprehensif dan terpadu dengan dukungan sumber daya manusia yang profesional serta prasarana dan sarana yang memadai akan meningkatkan kualitas pelayanan publik dalam memanfaatkan arsip yang dibutuhkan melalui ketersediaan arsip yang faktual, utuh, sistematis, autentik, terpercaya, dan dapat digunakan.

24.Sistem Informasi Kearsipan Nasional yang selanjutnya disingkat SIKN adalah sistem informasi arsip secara nasional yang dikelola oleh ANRI yang menggunakan sarana jaringan informasi kearsipan nasional. => SIKD + SIKS
25.Jaringan Informasi Kearsipan Nasional yang selanjutnya disingkat JIKN adalah sistem jaringan informasi dan sarana pelayanan arsip secara nasional yang dikelola oleh ANRI.

BAB VI AUTENTIKASI

Pasal 68

(1) Pencipta arsip dan/atau lembaga kearsipan dapat membuat arsip dalam berbagai bentuk dan/atau melakukan alih media meliputi media elektronik dan/atau media lain.
(2) Autentikasi arsip statis terhadap arsip sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh lembaga kearsipan.
(3) Ketentuan mengenai autentisitas arsip statis yang tercipta secara elektronik dan/atau hasil alih media sebagaimana dimaksud pada ayat (1) harus dapat dibuktikan dengan persyaratan yang diatur dengan peraturan pemerintah.

Pasal 69

(1) Lembaga kearsipan berwenang melakukan autentikasi arsip statis dengan dukungan pembuktian.
(2) Untuk mendukung kapabilitas, kompetensi, serta kemandirian dan integritasnya dalam melakukan fungsi dan tugas penetapan autentisitas suatu arsip statis, lembaga kearsipan harus didukung peralatan dan teknologi yang memadai.
(3) Dalam menetapkan autentisitas suatu arsip statis, lembaga kearsipan dapat berkoordinasi dengan instansi yang mempunyai kemampuan dan kompetensi.

Pasal 68
Ayat (1) Cukup jelas.
Ayat (2)
Yang dimaksud dengan "autentikasi arsip statis" adalah **pernyataan tertulis atau tanda** yang menunjukkan bahwa arsip statis yang bersangkutan adalah **asli atau sesuai dengan aslinya.**
Ayat (3) Cukup jelas.

Pasal 69
Ayat (1)
Yang dimaksud dengan "dukungan pembuktian" adalah usaha-usaha **penelusuran dan pengungkapan serta pengujian** terhadap arsip yang akan diautentikasi.
Ayat (2)
Yang dimaksud dengan "kemandirian dan integritasnya" adalah lembaga kearsipan harus menjaga **netralitasnya** dalam penetapan autentisitas dan tidak menyandarkan pembuktian pada instansi dan/atau pihak yang mempunyai kepentingan tertentu yang dapat menciderai kualitas pembuktian.
Ayat (3) Cukup jelas.

PP28/2012 Arsip (Bagian Keempat Autentikasi)

Pasal 106

(1) Autentikasi arsip statis dilakukan terhadap arsip statis maupun arsip hasil alih media untuk menjamin keabsahan arsip.
(2) Autentikasi terhadap arsip hasil alih media sebagaimana dimaksud pada ayat (1) dilakukan dengan memberikan tanda tertentu yang dilekatkan, terasosiasi atau terkait dengan arsip hasil alih media.
(3) Kepala lembaga kearsipan menetapkan autentisitas arsip statis sebagaimana dimaksud pada ayat (1) dengan membuat surat pernyataan.

Pasal 107

Kepala lembaga kearsipan menetapkan autentisitas arsip statis sebagaimana dimaksud dalam Pasal 106 ayat (3) berdasarkan persyaratan:

a. pembuktian autentisitas didukung peralatan dan teknologi yang memadai;
b. pendapat tenaga ahli atau pihak tertentu yang mempunyai kemampuan dan kompetensi di bidangnya; dan
c. pengujian terhadap isi, struktur, dan konteks arsip statis.

Pasal 108

(1) Dalam rangka pembuktian autentisitas arsip statis sebagaimana dimaksud dalam Pasal 107 huruf a, lembaga kearsipan menyediakan prasarana dan sarana alih media serta laboratorium.
(2) Ketentuan lebih lanjut mengenai prasarana dan sarana, laboratorium serta tata cara penggunaan dan metode pengujian dalam rangka autentikasi diatur dengan Peraturan Kepala ANRI.

Pasal 106
Ayat (1)
Yang dimaksud dengan "autentikasi arsip statis" adalah pernyataan terhadap autentisitas arsip statis yang dikelola oleh lembaga kearsipan setelah dilakukan proses pengujian.
Ayat (2) Cukup jelas.
Ayat (3) Cukup jelas.

Pasal 107
Huruf a Cukup jelas.
Huruf b
Yang dimaksud dengan "pihak tertentu" antara lain laboratorium forensik, laboratorium kimia maupun perseorangan (seperti ahli di bidang teknologi informasi dan telekomunikasi, sejarah, kertas, tinta, dan film).
Huruf c
Pengujian terhadap isi, struktur dan konteks arsip statis untuk memastikan reliabilitas dan autentisitas arsip statis.

Pasal 108
Ayat (1) Yang dimaksud dengan "laboratorium" adalah unit yang melaksanakan pengujian terhadap autentisitas dan reliabilitas arsip yang dilengkapi dengan peralatan untuk pengujian.
Ayat (2) Cukup jelas

PERKA-ANRI

- PerKa No.20/2011 tentang Pedoman Autentikasi Arsip Elektronik;
- PerKa No.14/2012 Tentang Pedoman Penyusunan Kebijakan Umum Pengelolaan Arsip Elektronik
- PerKa No.15/2012 Tentang Petunjuk Pelaksanaan Pengelolaan Surat Elektronik Di Pencipta Arsip.
- PerKa No.2 Tahun 2014 Tentang Pedoman Tata Naskah Dinas

Digital archiving is a curation activity, ensures that

- Data is properly selected
- Data is properly stored
- Data can be accessed
- The logical and physical integrity of the data is maintained over time
- Data is secure and authentic *

* Lord & MacDonald, e-Science Data Curation Report, 2003

- **Arsip Elektronik** adalah arsip yang diciptakan (dibuat atau diterima dan disimpan) dalam format elektronik.
- **Identitas** adalah keseluruhan karakteristik suatu dokumen yang unik mengidentifikasinya serta membedakannya dengan dokumen atau arsip lainnya.
- **Integritas** adalah kualitas lengkap dan tidak berubah dalam setiap komponen pentingnya.
- **Autentisitas** adalah kualitas suatu arsip yang sebagaimana adanya dan tidak mengalami perubahan.
- **Autentik** adalah layak diterima atau dipercaya berdasarkan fakta dan ini identik (tidak berbeda sedikit pun) dengan asli serta bonafide (dapat dipercaya dengan baik).
- **Arsip asli** adalah arsip yang memiliki karakter sesungguhnya, yang tidak dipalsukan, diimitasikan, atau tercemar, serta dipastikan berasal dari sumber tertentu yang diketahui.
- **Arsip orisinal** adalah arsip yang lengkap dan efektif yang merupakan manifestasi pertama saat arsip tersebut diterima atau dikaptur dan dinyatakan sebagai arsip.

Permen Kominfo 11/2018 P.Sert.Elektronik

- Bab 1: Ketentuan Umum
- Bab 2: Penyelenggara Sertifikasi Elektronik
  - Lokal dan Asing
  - Instansi dan Non-Instansi
- Bab 3: Tata Cara Memiliki Sertifikat Elektronik
  - Pemeriksaan sendiri atau
  - Dengan notaris sbg RA
- Bab 4: Pengawasan Penyelenggaraan Sertifikasi Elektronik
- Bab 5: Sanksi
- Bab 6: Ketentuan Lain-Lain
- Bab 7: Ketentuan Peralihan
- Bab 8: Ketentuan Penutup

Perpres 95/2018 SPBE

Bab 1: Ketentuan Umum
- Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
- Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset TIK dengan tujuan untuk menetapkan tingkat kesesuaian antara TIK dengan kriteria dan/atau standar yang telah ditetapkan.

Bab 2: Tata Kelola Sistem Pemerintahan Berbasis Elektronik
Bab 3: Manajemen Sistem Pemerintahan Berbasis Elektronik
Bab 4: Audit Teknologi Informasi Dan Komunikasi
Bab 5: Penyelenggara Sistem Pemerintahan Berbasis Elektronik
Bab 6: Percepatan Sistem Pemerintahan Berbasis Elektronik
Bab 7: Pemantauan Dan Evaluasi Sistem Pemerintahan Berbasis Elektronik
Bab 8: Ketentuan Peralihan
Bab 9: Ketentuan Penutup

UU ITE	
Pasal 5 (1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. (2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan **perluasan** dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. (3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini. (4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk: a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan b.surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.	*Penjelasan Pasal 5* (perubahan dalam UU ITE 19/2016 sebagai konsekuensi dari Putusan MK 20/PUU-XIV/2016) Ayat (1) Bahwa keberadaan Informasi Elektronik dan/atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan melalui Sistem Elektronik. Ayat (2) Khusus untuk Informasi Elektronik dan/atau Dokumen Elektronik berupa hasil intersepsi atau penyadapan atau perekaman yang merupakan bagian dari penyadapan harus dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang. Ayat (3) Cukup jelas. Ayat (4) Huruf a Surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara. Huruf b Cukup jelas.
Pasal 6 Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.	*Penjelasan Pasal 6* Selama ini bentuk tertulis identik dengan informasi dan/atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. Dalam lingkup Sistem Elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab Sistem Elektronik pada dasarnya beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.
Pasal 11 (1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut: a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan; b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan; c.segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui; d.segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui; e. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan f.terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait. (2) Ketentuan lebih lanjut tentang Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.	*Penjelasan Pasal 11* Ayat (1) Undang-Undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum. Persyaratan sebagaimana dimaksud dalam Pasal ini merupakan persyaratan minimum yang harus dipenuhi dalam setiap Tanda Tangan Elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapa pun untuk mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik. Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik. Ayat (2) Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik.

Pepres 82/2022 Infrastruktur Informasi Vital (IIV)

Pasal 4

Sektor IIV meliputi:

a. Administrasi pemerintahan;
b. Energi dan sumber daya mineral;
c. Transportasi;
d. Keuangan;
e. Kesehatan;
f. Teknologi informasi dan komunikasi;
g. Pangan;
h. Pertahanan; dan
i. Sektor lain yang ditetapkan Presiden.

Pasal 6

1) Setiap penyelenggara SE lingkup sektor IIV wajib melakukan identifikasi IIV secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
2) Setiap penyelenggara sektor IIV wajib melaporkan hasil identifikasi IIV beserta informasi yang relevan kepada Kementerian atau Lembaga.
3) Kementerian atau Lembaga melakukan verifikasi thdp laporan hasil identifikasi IIV sebagaimana dimaksud.

4) Kementerian atau lembaga menetapkan:

a. SE menjadi IIV; dan

b. Penyelenggara SE pada lingkup sektor IIV sbg Penyelenggara IIV

Berdasarkan hasil verifikasi laporan identifikasi IIV.

5) Ketentuan lebih lanjut mengenai *identifikasi IIV, pelaporan hasil identifikasi, mekanisme verifikasi, penetapan IIV, dan penetapan penyelenggara IIV* ***diatur dengan Peraturan Badan.***

Pasal 23

1. Badan berkedudukan sebagai koordinator penyelenggaraan pelindungan IIV.
2. Badan tsb bertugas:
   a) Mengevaluasi pelaksanaan penetapan sektor IIV
   b) Mengevaluasi penetapan IIV
   c) Mengusulkan penetapan danperubahan sektor IIV kpd Presiden
   d) Memberikan himbauan keamanan siber IIV kpd K/L berdasarkan data dan informasi yang diperoleh Badan;
   e) Mengevaluasi implementasi kebijakan pelindungan IIV.

Pepres 47/2023 Strategi Keamanan Siber

1. **Keamanan Siber** adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial.
2. **Strategi Keamanan Siber Nasional** adalah arah kebijakan nasional dalam menggunakan seluruh sumber daya siber nasional untuk mewujudkan Keamanan Siber guna mempertahankan dan memajukan kepentingan nasional.
3. **Insiden Siber** adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya sistem elektronik.
4. **Krisis Siber** adalah situasi kedaruratan akibat dari Insiden Siber pada tingkat nasional yang berdampak terhadap keselamatan, keutuhan, dan kedaulatan negara.
5. **Manajemen Krisis Siber** adalah tata kelola penggunaan sumber daya dan langkah penanganan secara efektif yang dilakukan sebelum, saat, dan setelah terjadinya Krisis Siber.
6. **Tim Tanggap Insiden Siber** adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
7. **Instansi Penyelenggara Negara** adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan.
8. **Pemangku Kepentingan** adalah para pihak yang memiliki peran dalam penerapan Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.
9. **Penyelenggara Sistem Elektronik** yang selanjutnya disingkat PSE adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

Pasal 6: Fokus area Strategi Keamanan Siber Nasional sebagaimana dimaksud dalam Pasal 5 huruf a terdiri atas:

a) tata kelola;
b) manajemen risiko;
c) kesiapsiagaan dan ketahanan;
d) penguatan pelindungan infrastruktur informasi vital;
e) kemandirian kriptografi nasional;
f) peningkatan kapabilitas, kapasitas, dan kualitas;
g) kebijakan Keamanan Siber; dan
h) kerja sama internasional.

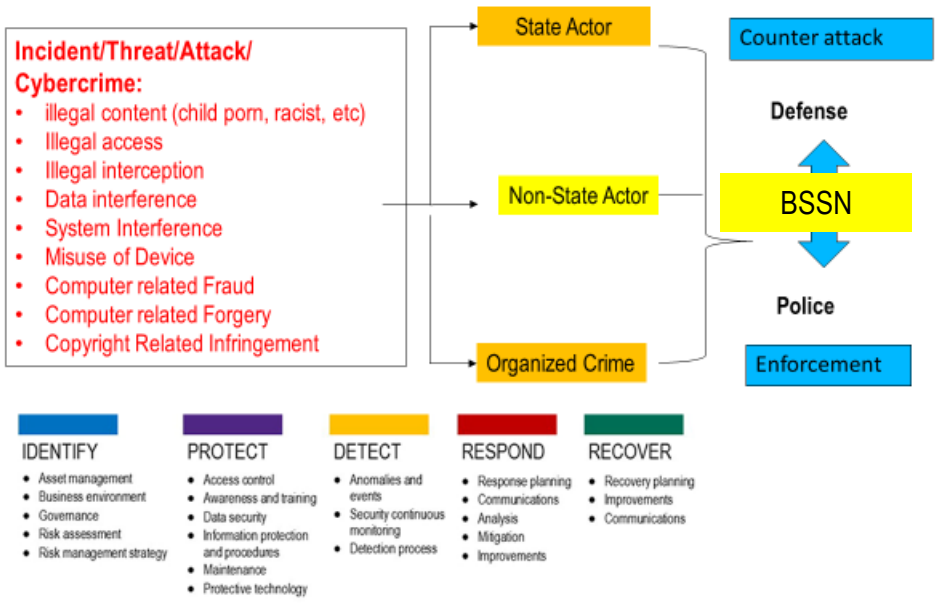
Cybersecurity

Umum	ITU	NATO
Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term *security* implies cybersecurity. Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include: • Application security • Information security • Network security • Disaster recovery / business continuity planning • End-user education.	"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. The Global Cybersecurity Agenda: 1) Legal Measures => cybercrime legislation 2) Technical and Procedural Measures => End users and businesses (direct approach); and Service providers and software companies 3) Organizational Structures => highly developed organizational structures, avoid overlapping, 4) Capacity Building & User's education => public campaigns + open communication of the latest cybercrime threats 5) International Cooperation => Mutual Legal Assistance of the LEA's	**National Cyber Security (NCS):** Defined 'The focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.' **The 5 Mandates** (Different interpretations of NCS & common activities) • Military Cyber • Counter Cyber Crime • Intelligence and Counter-Intelligence • Critical Infrastructure Protection and National Crisis Management • Cyber Diplomacy and Internet Governance + **3 'Cross Mandates'**: o coordination, o Information exchange and data protection, o research & development and education **The 3 Dimensions:** Different stakeholder groups in NCS • Governmental (central, state, local) – 'coordination' • National (CIP/contactors, security companies, civil society) – 'co-operation' • International (legal, political and industry frameworks) – 'collaboration' **The 5 Dilemmas:** • Balancing the cost and benefits of NCS • Stimulate the Economy vs. Improve National Security • Infrastructure Modernisation vs. Critical Infrastructure Protection • Private Sector vs. Public Sector • Data Protection vs. Information Sharing • Freedom of Expression vs. Political Stability

Comparative: Substantive Law of Cyber Crime

CoC	ITU	Indonesia
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems . illegal access, illegal interception, data interference, system interference, misuse of devices, Title 2 – Computer-related offences computer-related forgery, computer-related fraud Title 3 – Content-related offences offences related to child pornography and offences related to copyright and neighbouring rights. Title 4 – Offences related to infringements of copyright and related rights Title 5 – Ancillary liability and sanctions Attempting and aiding or abetting Corporate liability Sanctions & Measures	*Title 2. Substantive Provisions; Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data* sect. 2. Unauthorized Access to Computers, Computer Systems, and Networks sect. 3. Unauthorized Access to or Acquisition of Computer Data, Content Data, Traffic Data sect. 4. Interference and Disruption sect. 5. Interception sect. 6. Misuse and Malware sect. 7. Digital Forgery sect. 8. Digital Fraud, Procure Economic Benefit sect. 9. Extortion sect. 10. Aiding, Abetting, and Attempting sect. 11. Corporate Liability	• Penyalahgunaan Komptr/ Kompt sbg sarana: – Penyebaran Informasi ilegal (Illegal materials) – Pelanggaran Hak Cipta (offences related to copyright) – Pemalsuan atau Penipuan (*computer related fraud & forgery*) • Komputer sebagai sasaran – Akses tanpa hak dan/atau melawan hukum (Illegal Access) – Intersepsi Melawan Hukum (Illegal Interception) – Gangguan/Pengrusakan Data (Data Interference) – Gangguan/Pengrusakan Sistem (System Interference) – Penyalahgunaan Perangkat (Misuse of Device)

Centre for Coordination, Cooperation and Collaboration

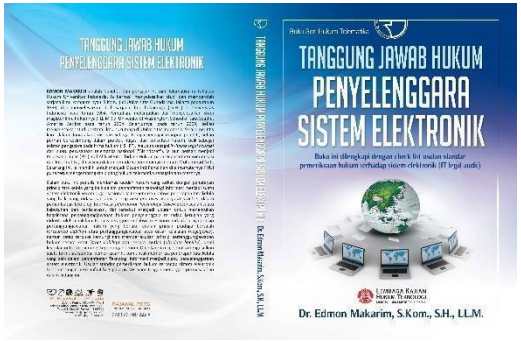


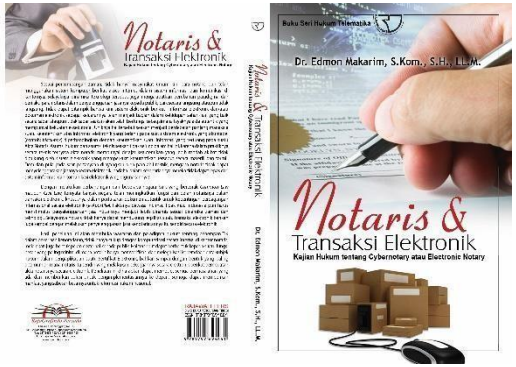
Kesimpulan

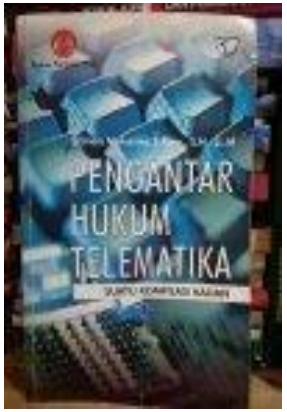
- Paradigma e-justice dan transformasi e-Court tdk dpt dilepaskan dari paradigma keautentikan secara elektronik tidak hanya sekedar Ketersediaan Data saja melainkan juga sistem keautentikan lintas sektor
- Semua komunikasi dan pemberkasan harus jelas rantai keautentikannya dan diperlakukan sebagaimana layaknya Arsip Negara untuk fungsi pembuktian & pembelajaran hukum di belakang hari.
- Sistem arsip perkara secara elektronik harus didukung oleh kejelasan tata-naskah dinas secara elektronik dan *IT policy* di instansi yang bersangkutan. Sesuai UU Kearsipan harus Autentik dan Terpercaya
- Alat bukti yang sah, tetap harus dilihat reliabilitas sistem keamanannya, yang secara teknis akan menentukan sejauhmana kekuatan pembuktiannya. Bobot pembuktikan ditentukan oleh bagaimana penerapan *e-IDAS (e- identitification and authentication system)*, sehingga sepanjang IE/DE berikut Sistem Elektroniknya teraman/terjaga validitasnya dengan baik, maka otomatis tidak dapat disangkal => mempunyai kekuatan hukum yang kuat dan mengikat.
- Perlu reformasi hukum nasional untuk mengkonsistensikan aturan ttg Keautentikan, khususnya thp identitas dan dokumen public guna menghadapi Law 2030.
- Keautentikan, baik secara teknis maupun hukum terhadap dokumen elektronik di Indonesia merujuk pada pasal 5 dan 6 UU-ITE, selayaknya ditunjang dengan Sertifikat Elektronik sesuai dengan PP-PSTE.
- Indonesia perlu memiliki kebijakan tentang Public Document Repository, demi memfasilitasi kejelasan adanya rantai keautentikan terhadap dokumen public dan mengurangi rumitnya legalisasi foreign public document. ANRI perlu membantu MA + KUMHAM dalam hal ini, khususnya terkait Dokumen Perusahaa dan Arsip Negara yang disimpan oleh Notaris.

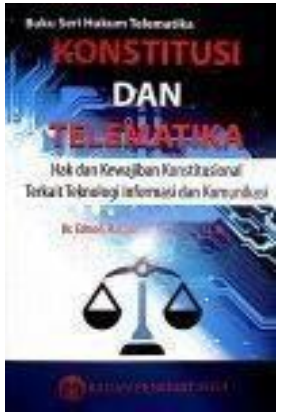
Thank You

- Eyes => horizon
- Lamp => idea
- Smile=> Optimism
- IC/processor => ICT
- Web & Hub => geostrategic Nusantara Islands





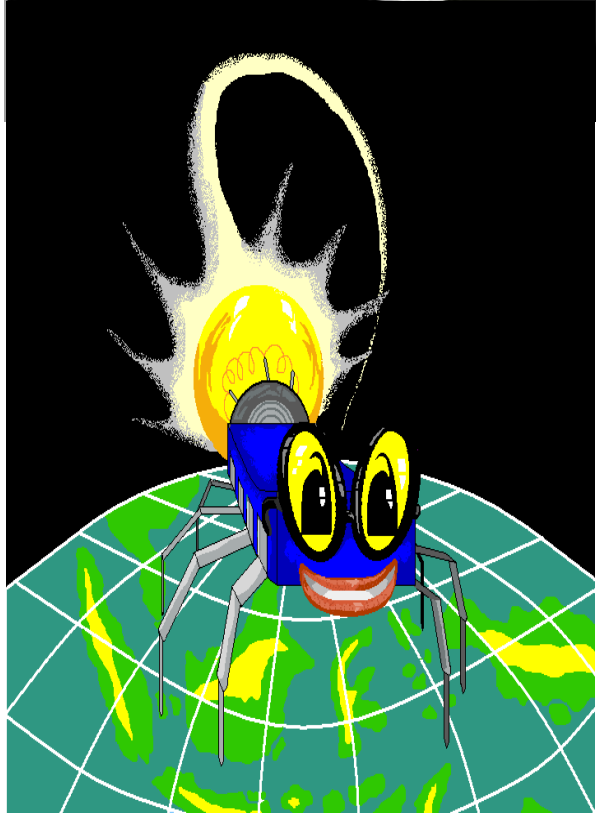




Empowerment
Through Education

Living A Dream,
Building A Future

eCLIS.id



UU 8/1997 Dokumen Perusahaan	PP 88/1999 tentang Tata Cara Pengalihan Dokumen Perusahaan ke Dalam Mikrofilm atau Media Lainnya dan Legalisasi	
Menimbang: … f. Bahwa kemajuan teknologi telah memungkinkan catatan dan dokumen yang dibuat di atas kertas dialihkan ke dalam media elektronik atau dibuat secara langsung dalam media elektronik	**Pasal 1** Dalam Peraturan Pemerintah ini yang dimaksud dengan: 1. Dokumen perusahaan adalah data, catatan, dan atau keterangan yang dibuat dan atau diterima 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 didengar. 2. Mikrofilm adalah film yang memuat rekaman bahan tertulis, dan atau tergambar dalam ukuran yang sangat kecil. 3. Legalisasi adalah tindakan pengesahan isi dokumen perusahaan yang dialihkan atau ditransformasikan ke dalam mikrofilm atau media lain, yang menerangkan atau menyatakan bahwa isi dokumen perusahaan yang terkandung di dalam mikrofilm atau media lain tersebut sesuai dengan naskah aslinya. **Pasal 2** Setiap perusahaan dapat mengalihkan dokumen perusahaan yang dibuat atau diterima baik di atas kertas maupun dalam sarana lainnya ke dalam mikrofilm atau media lainnya. BAB II TATA CARA PENGALIHAN **Pasal 6** (1) Sebelum melakukan pengalihan, perusahaan yang bersangkutan wajib melakukan persiapan dan penelitian dari berbagai aspek atas dokumen perusahaan yang akan dialihkan. (2) Pimpinan perusahaan yang bersangkutan dapat terlebih dahulu menetapkan pedoman intern dalam rangka pengalihan dokumen perusahaan. (3) Pimpinan perusahaan dapat menetapkan pejabat di lingkungan perusahaan yang bersangkutan yang ditunjuk dan bertanggung jawab untuk meneliti dan menetapkan dokumen perusahaan yang akan dialihkan. **Pasal 7** Keputusan mengenai pengalihan dokumen perusahaan hanya dapat dilakukan oleh pimpinan perusahaan atau pejabat yang ditunjuk. **Pasal 8** Dalam dokumen perusahaan yang dibuat perusahaan berbentuk neraca tahunan, perhitungan laba rugi tahunan, atau tulisan lain yang menggambarkan neraca laba rugi, pengalihan hanya dapat dilakukan setelah dokumen perusahaan tersebut dibuat di atas kertas dan ditandatangani oleh pimpinan perusahaan atau pejabat yang ditunjuk di lingkungan perusahaan yang bersangkutan.	**Pasal 9** Pengalihan dokumen perusahaan dapat dilakukan terhadap satu set dokumen tertentu atau sekumpulan dokumen, baik yang sejenis maupun yang tidak sejenis. **Pasal 10** (1) Pengalihan dokumen perusahaan dilakukan dengan menggunakan peralatan dan teknologi yang memenuhi standar ketepatan dan kelengkapan sehingga dapat menjamin hasil pengalihan sesuai dengan naskah asli dokumen yang dialihkan: (2) Dalam pengalihan dokumen perusahaan, pimpinan perusahaan atau pejabat yang ditunjuk wajib menjamin keamanan proses pengalihan agar: a. dokumen perusahaan hasil pengalihan, yang disimpan di dalam mikrofilm atau media lainnya tersebut, merupakan dokumen pengganti yang sepenuhnya sama dengan naskah aslinya; b. mikrofilm atau media lainnya tetap dalam keadaan baik untuk dapat disimpan dalam jangka waktu sekurang kurangnya sesuai dengan ketentuan mengenai daluwarsa suatu tuntutan yang diatur dalam peraturan perundang undangan yang berlaku; dan c. dokumen hasil pengalihan dapat dibaca atau dicetak kembali di atas kertas. **Pasal 11** (1) Perusahaan dapat menunjuk perusahaan lain untuk melaksanakan pengalihan dokumen perusahaan ke dalam mikrofilm atau media lainnya. (2) Perusahaan yang ditunjuk melaksanakan pengalihan dokumen sebagaimana dimaksud dalam ayat (1) wajib memenuhi syarat sebagai berikut: a. berbadan hukum; dan b. memperoleh izin usaha. **Pasal 12** Apabila tempat pemrosesan pengalihan dokumen perusahaan berbeda dari tempat pembuatan dan penyimpanan dokumen perusahaan, proses pengalihan dapat dilakukan melalui media teknik pengalihan yang tersedia.

UU 8/1981 Hukum Acara Pidana	UU 15/2002 Tindak Pidana Pencucian Uang	UU 9/2013 Pencegahan dan Pemberantasan Terorisme	UU 21/2007 Pemberantasan Tindak Pidana Perdagangan Orang
Pasal 184 - Keterangan saksi - Keterangan ahli - Surat - Petunjuk - Keterangan terdakwa	**Pasal 1 angka 7** Dokumen adalah data, rekaman, 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, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada: a. tulisan, suara, atau gambar; b. peta, rancangan, foto, atau sejenisnya; c. huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.	**Pasal 1 angka 14** Dokumen adalah data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas atau benda fisik apa pun selain kertas maupun yang terekam secara elektronik, termasuk tetapi tidak terbatas pada: a. tulisan, suara, atau gambar; b. peta, rancangan, foto, atau sejenisnya; dan c. huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.	**Pasal 29** Alat bukti selain sebagaimana ditentukan dalam Undang-Undang Hukum Acara Pidana, dapat pula berupa: a. informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan b. data, rekaman, 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 apa pun selain kertas, atau yang terekam secara elektronik, termasuk tidak terbatas pada: 1) tulisan, suara, atau gambar; 2) peta, rancangan, foto, atau sejenisnya; atau 3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.
	Pasal 38 Alat bukti pemeriksaan tindak pidana pencucian uang berupa: a. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana; b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan c. dokumen sebagaimana dimaksud dalam Pasal 1 angka 7.	**Pasal 38** Alat bukti yang sah dalam pembuktian tindak pidana pendanaan terorisme ialah: a. alat bukti sebagaimana dimaksud dalam Undang- Undang Hukum Acara Pidana; b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau alat yang serupa optik; dan/atau c. Dokumen.	