Hukum Dan Telematika

Bidang-bidang hukum positif di Indonesia yang menerima dampak langsung dari perkembangan teknologi informasi dan memang perlu mendapatkan penyikapan yang memadai dalam waktu dekat adalah sebagai berikut :

- Kerahasiaan dan Perlindungan Data
- Hak atas Kekayaan Intelektual
- Transaksi secara Elektronik
- Kejahatan yang Terkait dengan Komputer
- Media, Telekomunikasi, dan Penyiaran
- Konflik antar Tata Hukum
- Pembuktian Data Elektronik

Sumber hukum Indonesia dapat dibedakan dalam dua macam, yaitu tertulis dan tidak tertulis. Yang termasuk dalam sumber hukum tertulis ialah undang-undang, traktat, dan yurisprudensi. Sedangkan sumber hukum tidak tertulis ialah kebiasaan masyarakat atau adat, dan perjanjian-perjanjian tidak tertulis.

Undang-undang dapat diartikan dalam dua macam, yaitu undang-undang sebagai aturan-aturan hukum tertulis yang disebut sebagai undang-undang, dan undang-undang sebagai aturan-aturan hukum tertulis yang dikeluarkan untuk menyelenggarakan tugas-tugas negara atau kerap disebut sebagai peraturan perundang-undangan.

Terdapat beberapa asas dalam sistem perundang-undangan Indonesia, antara lain:

- *Lex Specialis Derogat Lex Generalis*, yaitu suatu produk perundang-undangan yang pengaturannya bersifat khusus mengenyampingkan perundang-undangan yang bersifat umum.

- *Lex Superiori Derogat Lex Inferiori*, yaitu suatu produk perundang-undangan yang lebih tingkatannya akan mengenyampingkan produk perundang-undangan yang ada dibawahnya.

- *Lex Posteriori Derogat Lex Priori*, yaitu suatu produk perundang-undangan yang baru akan mengenyampingkan perundang-undangan yang terdahulu.

Namun, dalam sistem perundang-undangan Indonesia tidak dikenal adanya undang-undang induk, atau undang-undang yang lebih tinggi tingkatannya dari undang-undang yang lain yang keberlakuannya dapat mengenyampingkan undang-undang lain.

Materi muatan undang-undang dapat bersumber dari UUD secara langsung maupun tidak langsung. Apabila terdapat sebuah fenomena baru di masyarakat dan mempunyai pengaruh jangka panjang terhadap masyarakat, maka hal tersebut dapat menjadi materi muatan undang-undang walaupun tidak secara tegas diatur dalam UUD.

· Kerahasiaan dan Perlindungan Data

Kemudahan dalam menyampaikan dan mengakses informasi yang diakibatkan oleh perkembangan dan konvergensi teknologi informasi sekaligus memperbesar kemungkinan penyalahgunaan data. Dengan terjadinya konvergensi teknologi informasi, *transborder data flows* atau penyebaran data melintasi batas-batas negara menjadi semakin cepat namun demikian juga menjadi sangat bebas dan semakin sulit untuk dikontrol. Bentuk informasi apapunapakah itu berupa teks, gambar, suara, bahkan gambar hidupdengan demikian menjadi sangat mudah untuk disebarluaskan. Kenyataan ini menimbulkan berbagai permasalahan hukum baru di sekitar kerahasiaan dan perlindungan data, yang dalam hal ini, apabila dirujukkan dengan peraturan perundang-undangan yang berlaku di Indonesiaterkait dengan peraturan mengenai sistem kearsipan, dokumen perusahaan, hukum pidana materiil, dan hak asasi manusia.

Ketentuan mengenai informasi publik diatur dalam UU No. 7 tahun 1971 Tentang Sistem Kearsipan. Dalam UU tersebut yang dimaksud dengan arsip ialah:

- Naskah-naskah yang dibuat dan diterima oleh lembaga-lembaga negara dan badan-badan pemerintahan dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan tugas pemerintah.

- Naskah-naskah yang dibuat dan diterima oleh badan-badan swasta dan/ atau perorangan, dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan kehidupan kebangsaan.

Dengan adanya ketentuan bahwa arsip dapat dirupakan dalam bentuk corak apapun, maka dalam hal ini dapat termasuk pula data elektronik. Mengenai keamanan data, UU tersebut juga mencantumkan ancaman pidana terhadap siapa saja yang melawan hukum dan/atau menyimpan dan dengan sengaja memberitahukan hal-hal tentang isi arsip tersebut kepada pihak ketiga yang tidak mengetahuinya.

Ketentuan mengenai data perusahaan terdapat dalam UU No.8 Tahun 1997 Tentang Dokumen Perusahaan. Yang dimaksud dengan dokumen perusahaan dalam UU tersebut ialah data, catatan, dan atau keterangan yang dibuat dan atau diterima oleh perusahaan dalam rangka pelaksanaan kegiatannya, baik tertulis diatas kertas atau sarana lain maupun terekam dalam bentuk corak apapun yang dapat dilihat, dibaca atau didengar.

Kedua peraturan tersebut masih harus disempurnakan karena metode-metode pembuatan, penyimpanan, dan penyebarluasan data telah berkembang dengan sangat pesat dan melampaui batas-batas penegakan hukum secara konvensional. Dalam hal ini berbagai perihal yang dapat menimbulkan permasalahan hukum ialah:

- Pengertian dan ruang lingkup data elektronik.
- Pengertian dan ruang lingkup kerahasiaan.
- Ketentuan pengaksesan data elektronik.
- Ketentuan mengenai subjek.
- Penggunaan data elektronik.
- Kekuatan data elektronik dalam pembuktian.

Perlindungan atas data pribadi merupakan aspek yang paling minimal pengaturannya, sehingga harus segera diatur lebih lanjut. Hukum pidana Indonesia telah memiliki ketentuan mengenai penyebaran informasi yang bertujuan sebagai fitnah, dan yang mengandung unsur pornografi. Dalam UU No.39 Tahun 1999 tentang Hak Asasi Manusia terdapat ketentuan mengenai kebebasan untuk berkomunikasi dan mendapatkan informasi secara pribadi sekaligus pula jaminan terhadap privasinya. Namun demikian, ketentuan-ketentuan tersebut belum memberikan batasan yang tegas mengenai kedudukan dan nilai hukum dari informasi pribadi tersebut. Sebagai perbandingan, Amerika Serikat telah mengeluarkan sebuah peraturan untuk mengantisipasi hal tersebut yaitu *The Electronic Communications Privacy Act.* Kanada, khususnya Quebec, telah memberlakukan *Act Respecting The Protection of Personal Information in The Private Sector* dan *Act Respecting Acces to documents held by Public Bodies and The Protection of Personal Information*. Di Inggris dikenal adanya *Data Protection Act*. Sementara suatu usaha untuk mengharmonisasikan regulasi mengenai *Data Protection* di Eropa dimulai sejak OECD mengeluarkan *Guidelines on The Protection of Privacy and Transborder Data Flows of Personal Data.*

Merujuk kepada U.K *Data Protection Act* 1984, ketentuan mengenai kerahasiaan dan perlindungan data setidaknya mengatur mengenai ruang lingkup dari pengguna data, subjek data, dan kaitannya dengan perkembangan teknologi komputer. Prinsip-prinsip yang ada dalam Undang-undang tersebut ialah:

- Data pribadi dapat diperoleh secara adil dan berdasarkan hukum.
- Disimpan hanya untuk tujuan yang terdaftar.
- Digunakan atau dibuka hanya jika sesuai dengan tujuan terdaftar.
- Cukup, relevan, dan tidak melebihi batas.
- Atau tujuan terdaftar.
- Akurat, dan diperbaharui jika diperlukan.
- Tidak disimpan lebih lama dari kebutuhan tujuan semula.
- Disediakan untuk subyek data yang diminta.
- Diamankan seperlunya dari kehilangan atau keterbukaan.

· Hak atas Kekayaan Intelektual (HaKI)

Kemajuan-kemajuan yang dicapai oleh teknologi informasi tidak dapat lepas dari keberadaan HaKI. Secara umum HaKI adalah perlindungan hukum yang berupa hak yang diberikan oleh negara secara eksklusif terhadap karya-karya yang lahir dari suatu proses kreatif pencipta/ penemunya. *Cyberspace* yang ditopang oleh dua unsur utama, komputer dan informasi, secara langsung bersentuhan dengan obyek-obyek pengaturan dalam HaKI, yaitu cipta, paten, merek, desain industri, rahasia dagang, dan tata letak sirkit terpadu. HaKI mendapatkan sorotan khusus karena hak tersebut dapat disalahgunakan dengan jauh lebih mudah dalam kaitannya dengan fenomena konvergensi teknologi informasi yang terjadi. Tanpa perlindungan, obyek yang sangat bernilai tinggi ini dapat menjadi tidak berarti apa-apa, ketika si pencipta/ penemu tidak mendapatkan penggantian biaya yang telah dikeluarkannya selama proses penciptaan ketika orang lain justru yang memperoleh manfaat ekonomis dari karyanya.

Ketentuan mengenai Hak atas Kekayaan Intelektual telah ada di Indonesia, namun terdapat beberapa permasalahan yang perlu dicermati, yaitu:

- Apakah Program Komputer dapat dikategorikan sebagai Hak Cipta ?
- Bagaimana kedudukan Nama Domain dalam hukum mengenai Merk ?
- Apakah hak eksklusif dalam Hak atas Kekayaan Intelektual tidak bertentangan dengan ketentuan mengenai larangan praktek monopoli dan persaingan usaha tidak sehat ?
- Apakah internet dapat dikategorikan sebagai media untuk mempublikasikan suatu objek paten ?
- Penyebaran informasi yang terkait dengan rahasia dagang semakin mudah dengan adanya teknologi kriptografi, bagaimana mengantisipasi hal tersebut ?

Untuk menghadapi perubahan-perubahan yang terjadi tersebut, Amerika Serikat telah memperbaharui perangkat hukum mengenai HaKI dan salah satunya mengeluarkan *Digital Millenium Copyright Act*, dalam mengantisipasi hal tersebut.

· Transaksi secara Elektronik

Internet telah berkembang sebagai media untuk melakukan kegiatan-kegiatan bisnis. Kegiatan bisnis pada dasarnya adalah rangkaian transaksi-transaksi. Pada dunia nyata, hal tersebut tidaklah menjadi masalah, karena para pihak yang bertransaksi dapat dengan mudah mengetahui identitas pribadi-pribadi yang melakukannya dan memastikan keberadaan hal yang ditransaksikan. Pada dasarnya ketentuan perundang-undangan Indonesia telah menjamin bahwa transaksi yang dilakukan melalui internet adalah sebuah perikatan yang mengikat para pihak yang membuatnya. Namun, transaksi yang dilakukan dengan menggunakan media internet validitasnya sangat rentan.

Hal tersebut disebabkan sulitnya mengetahui identitas para pihak yang bertransaksi dan hal yang ditransaksikan. Selain itu, perubahan media dari kertas menjadi elektronik menjadi permasalahan dalam hal kekuatan hukumnya. Pada beberapa negara, teknologi tanda tangan digital dapat digunakan untuk menggantikan fungsi tandatangan dalam perjanjian tertulis konvensional.

Keberadaan tanda tangan digital dengan menggunakan sistem kriptografi ini menyelesaikan (paling tidak) beberapa hal yang menjadi permasalahan dalam proses komunikasi via internet:

- *Authenticity*, menunjuk pada keaslian (otentitas) asal pengirim data suatu data.
- *Confidentiality*, menunjuk pada unsur kerahasiaan dari suatu data.
- *Integrity*, menunjuk pada integritas terhadap isi suatu data:
  - Apakah isi suatu data utuh atau hanya sebagian?
  - Apakah isi suatu data telah dirubah oleh pihak lain?
  - Apakah data yang dikirim sama dengan data yang diterima? Tanda t digital mengakibatkan data tidak dapat dibaca oleh pihak lain sehingga b bentuk perubahan pada data tersebut secara sengaja oleh pihak lain mengakibatkan data tersebut tidak dapat dibaca.

- *Non-repudiation,* berarti seorang pengirim tidak dapat menyangkal telah mengadakan suatu hubungan komunikasi, atau menyatakan bahwa bahwa isi dari data yang diterima tidak sama dengan data yang dikirim.Dalam manajemen pemanfaatan tanda tangan digital tersebut melahirkan sebuah lembaga yang disebut sebagai otoritas sertifikasi (*Certification Authority/CA*).

Beberapa negara telah mengeluarkan peraturan-peraturan yang berkaitan dengan hal tersebut, yaitu :

A.S	:	Uniform Electronic Transaction Act 1998
Singapura	:	Electronic Transaction Act 1996
Malaysia	:	Digital Signature Act 1997
Kanada	:	Electronic Transaction Act 1999
Irlandia	:	Electronic Commerce Bill 1999

Pada umumnya ketentuan yang diatur dalam peraturan negara-negara tersebut ialah :

- Siapa yang berwenang mengeluarkan CA ?
- Sejauhmana ruang lingkup perdagangan atau kegiatan komersial ? Siapa yang berwenang untuk membuat peraturan ?
- Siapa yang berhak untuk mengontrol ?
- Peraturan apa saja yang mungkin disiapkan
- Siapa yang berhak menjadi CA ?
- Apa saja yang menjadi kewenangan CA ?
- Produk-produk apa saja yang memerlukan CA?
- Bagaimana cara membuktikan apabila terjadi pemalsuan identitas *subscriber* ?
- Jaminan dan kewajiban CA ?
- Jaminan terhadap konsumen pada CA ?
- Apakah ada jaminan atau diasuransikan jika terjadi kerugian diantara para pihak?
- Syarat-syarat apa saja yang harus dipenuhi dalam suatu kontrak (standar kontrak)?
- Siapa yang memberikan *time stamping*?
- Apakah dimungkinkan pengaturan mengenai *Tax stamp*?
- Hukum mana yang digunakan apabila timbul perselisihan di kemudian hari (*Choice of Law*)?
- Pilihan forum yang digunakan apabila timbul perselisihan di kemudian hari (*Choice of Forum*)? Pengadilan mana yang dipilih untuk menyelesaikan perkara tersebut?
- Bagaimana pembuktian kontrak yang dibuat dalam transaksi secara elektronik?

Sebagai pembanding, di Singapura ada perlindungan terhadap CA dengan maksud memberikan kepercayaan di mata masyarakat. Kemudian ada yang kontra, yaitu yang menyatakan bahwa pihak yang akan menggunakan CA akan memperoleh garansi atau perlindungan jika dalam prakteknya pelanggan dirugikan yang besarnya ditentukan oleh

para pihak. Mengenai adanya suatu standar yang dapat digunakan sehingga pelanggan akan menikmati dan memanfaatkan CA sebagai pihak ketiga yang dipercaya, UNCITRAL tidak menjelaskannya, namun secara implisit dapat diartikan bahwa digantungkan pada perjanjian sebelumnya.

Kemungkinan penggantian (jaminan) yang diberikan terhadap pelanggan (*subscriber*), seluruhnya dibebankan pada CA, sesuai dengan berapa banyaknya modal atau uang yang disetor.

Pembayaran asuransi pada CA dapat lebih besar, maka CA dapat memberikan suatu janji dimana CA akan mengganti kerugian yang diderita oleh subscriber dengan tujuan melindungi konsumen itu sendiri.

Seperti di Singapura, CA harus mengungkapkan atau mengumumkan deposit atau modal yang dimiliki, sehingga pelanggan akan percaya dan konsumen akan merasa terlindungi jika terjadi hal-hal yang tidak diinginkan, gempa bumi.

Dalam kaitannya dengan perlindungan konsumen, di Irlandia dikenal adanya *liabilities limit*, dimana tanggung jawab berada pada CA. Karena ada perlindungan konsumen maka semua tanggung jawab ada di tangan CA.

· Kejahatan yang Terkait dengan Komputer

Definisi *computer crime* menurut OECD yang didefinisikan dalam kerangka *computer* abuse yakni,

Any illegal, unethical or unauthorized behavior involving authomatic data processing and/or transmissing of data.

Terjemahan bebasnya :

Setiap perilaku yang melanggar/melawan hukum, etika atau tanpa kewenangan yang menyangkut pemrosesan data dan/atau pengiriman data.

Walaupun istilah *computer crime* ataupun *cybercrime* telah populer di masyarakat akan tetapi secara eksistensi *computer crime* secara akademik masih menjadi perdebatan para ahli. Permasalahan yang timbul berkaitan dengan *computer crime* ini antara lain adalah apakah *computer crime* merupakan suatu bentuk kejahatan baru yang berbeda dari kejahatan-kejahatan konvensional tradisional seperti pencurian, pembunuhan dll., sehingga membutuhkan suatu pengaturan hukum yang secara khusus mengatur masalah ini seperti halnya tindak pidana perekonomian, ataukah kejahatan yang dimaksud dalam *computer crime* tersebut hanyalah suatu bentuk lain dari kejahatan-kejahatan biasa yang telah diatur di dalam hukum pidana materil positif sehingga yang diperlukan dalam mengatasi masalah *computer crime* secara hukum hanyalah masalah ekstensifikasi definisi unsur-unsur pasal serta masalah pembuktian di depan pengadilan saja.

Untuk lebih memperjelas masalah-masalah tersebut maka *computer* (*related*) *crime* dapat dilihat dalam ruang lingkup :

- Komputer sebagai instrumen untuk melakukan kejahatan tradisional, seperti

pencurian, penipuan, penggelapan uang, penyalahgunaan creditcard dan pemalsuan.

- Komputer dan perangkatnya sebagai objek penyalahgunaan, seperti *computer sabotage* yang dapat mencakup perbuatan-perbuatan penghancuran atau pengubahan data secara tidak sah.
- Penyalahgunaan yang berkaitan dengan komputer atau data yang dapat berkaitan dengan mengganggu arus data, system komputer maupun penggunaan sistem komputer secara tidak sah (*hacking*).
- *Unauthorized acquisition, disclosure or use of information and data*.

Untuk dapat dengan lebih seksama mengidentifikasikan masalah kejahatan komputer sebagai suatu bentuk kejahatan yang perlu diatur secara khusus maka unsur-unsur yang perlu dikaji adalah:

- Rumusan formal atau materil yang lebih tepat digunakan dalam membatasi ruang lingkup kejahatan yang terkait dengan komputer ?
- Bagaimana permasalahan mengenai *tempus delicti* dan *locus delicti* ?
- Apakah ketentuan mengenai kejahatan yang terkait dengan komputer harus diatur dalam sebuah peraturan khusus?

Beberapa bentuk kejahatan komputer diantaranya ialah :

- Cracking, The act of breaking into a computer system.
- Worm, A sometimes malicious stand-alone program that can propagate to other computers via network.
- Virus, A segment of machine code that will copy its code into one or more larger host program when its activated.
- Trojan Horse, A computer program with an apparently or actually useful function that contains additional (hidden) function that surreptitiously exploit the legitimate authorizations of the involving process to the detriement of security or integrity.
- Logic Bomb, A resident computer program that triggers an unauthorized act when a certain event occurs.

Pengaturan mengenai kejahatan yang terkait dengan komputer di beberapa negara diantaranya:

- Computer Misuse Act 1990 (Inggris)
- US Code Annex Titles 1-26 18 USCA Sec. 1030 (a) Fraud & Related Activity in Connection with Computer (Amerika Serikat)
- Second Law for the Prevention of Economic Crime of 1986 (Jerman)

· Media, Telekomunikasi, dan Penyiaran

Dalam kerangka WTO, sektor Telekomunikasi dikategorikan sebagai sektor perdagangan jasa, yang dalam Kertas Referensi WTO (WTO *Reference Paper*) pada intinya meliputi;

- Anti monopoli
- Interkoneksi tanpa diskriminasi
- Pelayanan universal harus transparan
- Kriteria pemberian lisensi harus terbuka
- Regulator independen (bebas dari ketergantungan penyelenggara)
- Alokasi sumberdaya terbatas transparan dan adil

Ringkasnya, prinsip-prinsip dasar pertelekomukasian dewasa ini adalah bersifat *open*, *compatibility*, *transparancy*, universal, dan pengaturan sendiri (*self regulatory*).

Akibat konvergensi yang terjadi, pemisahan ketentuan antara telekomunikasi dan penyiaran dirasakan sudah kurang tepat lagi. Pada dasarnya, penyiaran dengan telekomunikasi adalah berbicara mengenai hal yang sama, dimana semula Penyiaran dikategorikan sebagai *public means of communication* dan Telekomunikasi sebagai *private communications*. Kini disadari bahwa keduanya berbicara mengenai sistem komunikasi bagi masyarakat yang merupakan infrastruktur untuk pertukaran informasi bagi masyarakat.

Apalagi dengan keberadaan Internet, tumbuh 4 (empat) jenis usaha baru, yaitu

- Internet Services/ Access Provider
- Internet Content Provider
- Commercial/Application Services Provider
- Digital Cyber Communities

Perubahan struktur telekomunikasi akhirnya memerlukan pemisahan antara regulasi ataupun perijinan untuk penyelenggara infrastruktur komunikasi dengan penyedia informasi. Karena walaupun kedua-duanya berinvestasi untuk pembangunan jaringan, namun tentunya objektifnya berbeda.

· Konflik antar Tata Hukum

Globalisasi informasi sebagai akses dari perkembangan teknologi informasi tersebut rentan terhadap munculnya konflik dalam penerapan suatu hukum.

Beberapa isu yang berkaitan dengan hal tersebut diantaranya:

- Jurisdiction, yaitu the power of courts to inquire into facts, apply the law, make decissions, and declare judgement.

- *Choice of Law* atau mengenai pilihan hukum, dalam hal ini jika para pihak telah mengadakan perjanjian sebelumnya, maka masalah ini tidaklah berat, namun jika belum pilihan hukum ini dapat didasarkan pada tempat pembuatan kontrak, negosiasi, domisili, tempat tinggal, nasionalitas, atau tempat kedudukan dari para pihak .

- *Choice influencing factors*, untuk hal ini Amerika Serikat telah mengeluarkan *The American Restatement of Conflict of Laws*, yang dalam kebijakannya meliputi:

  - Coordination of legal systems
  - Justice of the end result
  - Protection of Justified Expectation
  - Predictability and Legal Consequences

Oleh karena itu dengan eskalasi dan semakin intensifnya globalisasi ini dan semakin meningkatnya sengketa yang melibatkan dua atau lebih hukum nasional, usaha yang lebih besar dalam membuat perjanjian bilateral/ multinasional akan menjadi pusat utama.

· Pembuktian Data Elektronik

Perubahan mendasar dalam era digital ini ialah semakin populernya penggunaan data elektronik di masyarakat. Namun kemudian, data elektronik ini dihadapkan pada permasalahan, ketika dihadapkan dengan masalah pembuktian dalam hal penyelesaian suatu sengketa. Tujuan dari pembuktian adalah mencari kebenaran baik secara formal maupun materil. Memang dari segi kekuatan mengikat ada beberapa alat bukti yang punya kekuatan pembuktian sempurna dan ada yang tidak. Surat otentik dalam peradilan perdata memiliki kekuatan pembuktian sempurna sepanjang tidak ada yang dapat membantahnya. Namun, secara materil dalam peradilan pidana, maka kekuatan pembuktian surat belum kuat dan harus didukung oleh alat bukti lainnya.

Namun di *cyberspace* keberadaan data elektronik menjadi penting karena sulitnya mendapatkan saksi yang mengetahui terjadinya pelanggaran hukum tersebut. PBB telah mengeluarkan sebuah rekomendasi, melalui resolusi 40/71, paragraf 5(b) , 11 Desember 1985 sebagai berikut:

- Pada waktu yang bersamaan bahwa tidak ada kebutuhan untuk unifikasi terhadap peraturan dari bukti memperhatikan penggunan rekaman/catatan (*record computer*) pada perdagangan internasional, pengalaman menunjukkan bahwa perbedaan substansial /perbedaan paling penting terhadap peraturan dari bukti sebagaimana yang mereka ajukan untuk sistem berdasarkan tertulis (*paper-based system*) dari dokumentasi sejauh ini telah menyebabkan tidak adanya bahaya yang dapat diperhatikan terhadap pembangunan perdagangan internasional.

- Pembangunan penggunaan *Automated Data Processing* adalah menciptakan sejumlah keinginan sistem hukum untuk sebuah adaptasi peraturan hukum yang

tetap untuk pembangunan ini .

- Rekomendasi untuk Pemerintah.

- Untuk me-*review* peraturan hukum mengenai penggunaan rekaman komputer sebagai bukti dalam litigasi untuk mengurangi rintangan/halangan yang tidak perlu untuk izin mereka, jaminan bahwa peraturannya konsisten dengan pembangunan teknologi, dan untuk menyediakan peralatan yang perlu bagi pengadilan untuk mengevaluasi kredibilitas data yang mengandung rekaman data tersebut.

- Untuk *me-review* persyaratan hukum bahwa transaksi dagang tertentu atau dokumen yang berhubungan dengan perdagangan yang dilakukan secara tertulis, apakah perlu untuk direkam dan ditransmisikan dalam bentuk *computer-readable* (dapat dibaca komputer) atau tidak.

- Untuk *me-review* persyaratan hukum dari tandatangan tertulis atau metode otensifikasi *paper-based* lainnya pada dokumen yang berhubungan dengan perdagangan dengan niat untuk mengizinkan.

- Untuk *me-review* persyaratan hukum bahwa dokumen untuk diserahkan ke pemerintah dalam bentuk tertulis dan tertanda secara manual dengan niat untuk mengizinkan, apabila perlu, beberapa dokumen untuk diserahkan dalam bentuk *computer-readable* kepada pelayanan administrasi tersebut.

Merekomendasikan kepada organisasi internasional untuk mengelaborasikan teks-teks hukum (*legal text*) berkaitan dengan perdagangan untuk memperhatikan rekomendasi yang ada dalam mengadopsi teks tersebut dan, apabila perlu, untuk mempertimbangkan memodifikasi *legal text* sesuai dengan rekomendasi yang ada.