

KULIAH ONLINE HUKUM TELEMATIKA  
PERTEMUAN KE-8  
UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK 2  
Dosen Koordinator : MEN WIH WIDIATNO

**I. PENJELASAN UMUM**

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau cyber law, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (law of information technology), hukum dunia maya (virtual world law), dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya

manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi input, process, output, storage, dan communication.

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelian di Internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik (electronic commerce) telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi. Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (cyber space), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.

Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang dibuat di atas kertas. Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di *cyber space*, yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

## II. ISTILAH DALAM UU ITE

Istilah yang dipergunakan dalam Undang-Undang ITE :

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.
3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6. Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.
7. Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.
8. Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.
9. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
10. Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
11. Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.
12. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
13. Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.
14. Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.

15. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16. Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.
17. Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18. Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.
19. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
20. Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

### **III. ASAS DAN TUJUAN**

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas-asas sebagai berikut :

1. kepastian hukum,  
landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.
2. manfaat,  
asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat.
3. kehati-hatian,  
landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik
4. iktikad baik,  
asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.
5. kebebasan memilih teknologi atau netral teknologi.  
pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

- a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
- b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
- c. meningkatkan efektivitas dan efisiensi pelayanan publik;
- d. membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
- e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

#### IV. MATERI UU ITE

Secara umum, materi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dibagi menjadi dua bagian besar, yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang. Pengaturan mengenai informasi dan transaksi elektronik mengacu pada beberapa instrumen internasional, seperti UNCITRAL Model Law on eCommerce[1] dan UNCITRAL Model Law on eSignature[2]. Bagian ini dimaksudkan untuk mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat umumnya guna mendapatkan kepastian hukum dalam melakukan transaksi elektronik.

Beberapa materi yang diatur, antara lain:

- pengakuan informasi/dokumen elektronik sebagai alat bukti hukum yang sah (Pasal 5 & Pasal 6 UU ITE);
- tanda tangan elektronik (Pasal 11 & Pasal 12 UU ITE);
- penyelenggaraan sertifikasi elektronik (certification authority, Pasal 13 & Pasal 14 UU ITE); dan
- penyelenggaraan sistem elektronik (Pasal 15 & Pasal 16 UU ITE)
- perbuatan yang dilarang (cybercrimes).

Beberapa cybercrimes yang diatur dalam UU ITE, antara lain:

- a. konten ilegal, yang terdiri dari, antara lain: kesusilaan, perjudian, penghinaan/pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, Pasal 28, dan Pasal 29 UU ITE);
- b. akses ilegal (Pasal 30);
- c. intersepsi ilegal (Pasal 31);
- d. gangguan terhadap data (data interference, Pasal 32 UU ITE);
- e. gangguan terhadap sistem (system interference, Pasal 33 UU ITE);
- f. penyalahgunaan alat dan perangkat (misuse of device, Pasal 34 UU ITE);

## V. ALAT BUKTI dalam UU ITE

Dalam Pasal 5 UU ITE menegaskan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ITE

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.

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.

Pengecualian dokumen elektronik 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 notaris atau akta yang dibuat oleh pejabat pembuat akta.

Dalam hal terdapat ketentuan lain selain diatas, 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.

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.

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.

Setiap Orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan.

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

- a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
- b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

## VI. TANDA TANGAN ELEKTRONIK

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 Penandatanganannya; dan
- f. terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

Ketentuan lebih lanjut tentang Tanda Tangan Elektronik diatur dengan Peraturan Pemerintah.

Pengamanan Tanda Tangan Elektronik sekurang-kurangnya meliputi:

- a. sistem tidak dapat diakses oleh Orang lain yang tidak berhak;
- b. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;
- c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh PenandaTangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:
  1. Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau
  2. keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan
- d. dalam hal Sertifikat Elektronik digunakan untuk pendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

Setiap Orang yang melakukan pelanggaran ketentuan tersebut diatas bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

Pasal 11 Undang-Undang ITE 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.

### **Penyelenggaraan Sertifikasi Elektronik**

- Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.
- Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.
- Penyelenggara Sertifikasi Elektronik terdiri atas:
  1. Penyelenggara Sertifikasi Elektronik Indonesia; dan Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.
  2. Penyelenggara Sertifikasi Elektronik asing. Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
- Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

## **VII. PERBUATAN YANG DILARANG**

- Yang dimaksud dengan "mendiskibagikan" adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/ atau Dokumen Elektronik kepada banyak Orang atau berbagai pihak melalui Sistem Elektronik.
- Yang dimaksud dengan "mentransmisikan" adalah mengirimkan Informasi Elektronik dan/ atau Dokumen Elektronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik.
- Yang dimaksud dengan "membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik.

Beberapa cybercrimes yang diatur dalam UU ITE, antara lain:

### **a. konten ilegal**

#### **Pasal 27**

1. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
2. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
3. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik

dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

- Ketentuan pada ayat ini mengacu pada ketentuan pencemaran nama baik dan/ atau fitnah yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).
  - Ketentuan ini merupakan delik aduan.
4. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.
- Ketentuan pada ayat ini mengacu pada ketentuan pemerasan dan/ atau pengancaman yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).

Pasal 28

1. Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2. Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi.

#### **b. Akses ilegal**

- Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:
  - a. melakukan komunikasi, mengirimkan, memancarkan atau
  - b. Sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah
- Sistem pengamanan adalah sistem yang membatasi akses Komputer atau melarang akses ke dalam Komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

Pasal 30

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

### **c. Intersepsi**

Yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

Pasal 31

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
3. Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.
4. Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang.

### **d. Gangguan terhadap data (data interference)**

Pasal 32

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
3. Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

### **e. Gangguan terhadap sistem (system interference)**

Pasal 33

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

f. penyalahgunaan alat dan perangkat (misuse of device)

Pasal 34

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
  - a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
  - b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
2. Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

g. Pemalsuan Dokumen Elektronik

Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

## VIII. KETENTUAN PIDANA

Pasal 45

- Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
- Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).
- Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman

sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling

- lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

#### Pasal 45A

- Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
- Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

#### pasal 45B

- Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

#### Pasal 46

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

#### Pasal 47

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

#### Pasal 48

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Pasal 49

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

#### KETENTUAN PIDANA PEMBERATAN

Pasal 52

- Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.
- Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.
- Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.
- Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

#### IX. URGENSI PERUBAHAN UU NO. 11 TAHUN 2008

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang pertama di bidang Teknologi Informasi dan Transaksi Elektronik sebagai produk legislasi yang sangat dibutuhkan dan telah menjadi pionir yang meletakkan dasar pengaturan di bidang pemanfaatan Teknologi Informasi dan Transaksi Elektronik.

Akan tetapi, dalam kenyataannya, perjalanan implementasi dari UU ITE mengalami persoalan-persoalan.

Pertama,

- terhadap Undang-Undang ini telah diajukan beberapa kali uji materiil di Mahkamah Konstitusi dengan Putusan Mahkamah Konstitusi Nomor 50 / PUU-VI / 2008, Nomor 2 I PUU -VII I 2009, Nomor S / PUU-UII / 20 I O, dan Nomor 20IPUU-X.IV /2016.
- Berdasarkan Putusan Mahkamah Konstitusi Nomor SO/PUU-VII2008 dan Nomor 2/PUU-VII2009, tindak pidana penghinaan dan pencemaran nama baik dalam bidang Informasi Elektronik dan Transaksi Elektronik bukan semata-mata sebagai tindak pidana umum, melainkan sebagai delik aduan. Penegasan mengenai delik aduan dimaksudkan agar selaras dengan asas'kepastian hukum dan rasa keadilan masyarakat.
- Berdasarkan Putusan Mahkamah Konstitusi Nomor s/PUU-Vfil I 2OLO, Mahkamah Konstitusi berpendapat bahwa kegiatan dan kewenangan penyadapan merupakan hal

yang sangat sensitif karena di satu sisi merupakan pembatasan hak asasi manusia, tetapi di sisi lain memiliki aspek kepentingan hukum. Oleh karena itu, pengaturan (regulation) mengenai legalitas penyadapan harus dibentuk dan diformulasikan secara tepat sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

- Di samping itu, Mahkamah berpendapat bahwa karena penyadapan merupakan pelanggaran atas hak asasi manusia sebagaimana ditegaskan dalam Pasal 28J ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, sangat wajar dan sudah sepatutnya jika negara ingin menyimpangi hak privasi warga negara tersebut, negara haruslah menyimpanginya dalam bentuk undang-undang dan bukan dalam bentuk peraturan pemerintah. Selain itu, berdasarkan Putusan Mahkamah Konstitusi Nomor 20IPUU-xrv 12oL6, Mahkamah Konstitusi berpendapat bahwa untuk mencegah terjadinya perbedaan penafsiran terhadap Pasal 5 ayat (1) dan ayat (2) UU ITE, Mahkamah menegaskan bahwa setiap intersepsi harus dilakukan secara sah, terlebih lagi dalam rangka penegakan hukum.
- Oleh karena itu, Mahkamah dalam amar putusannya menambahkan kata atau frasa "khususnya" terhadap frasa "Informasi Elektronik dan/atau Dokumen Elektronik". Agar tidak terjadi penafsiran bahwa putusan tersebut akan mempersempit makna atau arti yang terdapat di dalam Pasal 5 ayat (1) dan ayat (2) UU ITE, untuk memberikan kepastian hukum keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti perlu dipertegas kembali dalam Penjelasan Pasal 5 UU ITE.

Kedua,

- ketentuan mengenai penggeledahan, penyitaan, penangkapan, dan penahanan yang diatur dalam UU ITE menimbulkan permasalahan bagi penyidik karena tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik begitu cepat dan pelaku dapat dengan mudah mengaburkan perbuatan atau alat bukti kejahatan.

Ketiga,

- karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/ atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja.
- Dalam rangka melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik, diperlukan penegasan peran Pemerintah dalam mencegah penyebarluasan konten ilegal dengan melakukan tindakan pemutusan akses terhadap Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum agar tidak dapat diakses dari yurisdiksi Indonesia serta dibutuhkan kewenangan bagi penyidik untuk meminta informasi yang terdapat dalam Penyelenggara Sistem Elektronik untuk kepentingan penegakan hukum tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

Keempat,

- penggunaan setiap informasi melalui media atau Sistem Elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
- Untuk itu, dibutuhkan jaminan pemenuhan perlindungan diri pribadi dengan mewajibkan setiap Penyelenggara Sistem Elektronik untuk menghapus Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan.

Berdasarkan pertimbangan tersebut, perlu membentuk Undang- Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menegaskan kembali ketentuan keberadaan Informasi Elektronik dan/atau Dokumen Elektronik dalam Penjelasan Pasal 5, menambah ketentuan kewajiban penghapusan Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak relevan dalam Pasal 26, mengubah ketentuan Pasal 31 ayat (4) mengenai pendelegasian penJrusunan tata cara intersepsi ke dalam undang-undang, menambah peran Pemerintah dalam melakukan pencegahan penyebaran dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang dalam Pasal 40, mengubah beberapa ketentuan mengenai penyidikan yang terkait dengan dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dalam Pasal 43, dan menambah penjelasan Pasal 27 ayat (1), ayat (3), dan ayat (4) agar lebih harmonis dengan sistem hukum pidana materiil yang diatur di Indonesia.