Tanya Jawab Seputar UU ITE

Umum : Materi dan cakupan UU ITE

1. **Apa saja Materi dan Cakupan UU ITE?**

   Cakupan UU ITE dapat dilihat dari struktur UU ITE, yaitu :

   BAB I : Ketentuan UMUM
   BAB II : Asas dan Tujuan
   BAB III : Informasi, Dokumentasi, dan Tanda Tangan Elektronik
   BAB IV : Penyelenggara Sertifikasi Elektronik dan Sistem Elektronik
   BAB V : Transaksi Elektronik
   BAB VI : Nama Domain, HAKI, dan Perlindungan Hak Pribadi
   BAB VII : Perbuatan Yang Dilarang
   BAB VIII : Penyelesaian Sengketa
   BAB IX : Peran Pemerintah dan Peran Masyarakat
   BAB X : Penyidikan
   BAB XI : Ketentuan Pidana
   BAB XII : Ketentuan Peralihan
   BAB XIII : Ketentuan Penutup

2. **Mengapa ada banyak materi yang diakomodir dan diatur dalam UU ITE? Hal ini terkesan bahwa UU ITE tidak fokus. Bagaimana tanggapan pemerintah?**

   Cakupan cyberlaw luas, karena meliputi transaksi elektronik, alat bukti elektronik, privasi, yurisdiksi, intelectual property, termasuk tindak pidana

   Ada beberapa kelebihan yang diperoleh dengan menyatukan materi-materi tersebut dalam satu undang-undang. Pertama, penyatuan ini menghemat waktu karena jika tiap materi diatur dalam undang-undang sendiri, akan membutuhkan waktu lama untuk dibahas di DPR. Kedua, tim dapat dapat melihat keseluruhan materi secara holistik dan mengatur agar keterkaitan materi-materi tersebut secara komprehensif.

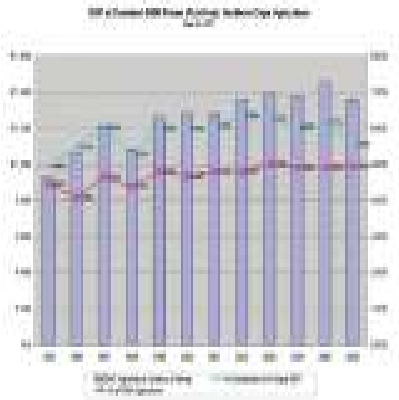
3. **Apakah ketentuan dalam UU ITE telah mengikuti ketentuan-ketentuan yang berlaku secara internasional?**

   UU ITE merujuk ketentuan-ketentuan dan prinsip-prinsip:

   - *UNCITRAL Model Law on Electronic Commerce;*
   - *UNCITRAL Model Law on Electronic Signature;*
   - *EU Directives on Electronic Commerce;*
   - *EU Directives on Electronic Signature;dan*
   - *Convention on Cybercrime;*

   Ketentuan-ketentuan tersebut adalah regulasi internasional yang banyak diterapkan oleh negara-negara Eropa, Amerika dan Asia.

4. **Apakan tujuan dari pembentukan UU ITE?**



Tujuan dari pembentukan UU ITE tercermin dari Pasal 4 UU ITE, yaitu untuk:

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

5. **Secara keseluruhan, apakah UU ITE telah menjawab kebutuhan dalam melakukan kegiatan atau aktivitas di dunia cyber (cyberspace)?**

   Secara garis besar, UU ITE telah cukup menjawab kebutuhan orang-orang dalam melakukan kegitan di dunia cyber. UU ITE telah mengakomodir ketentuan material dan juga prosedural. Dengan demikian UU ITE memberikan dan menjamin kepastian hukum dalam melaksanakan aktivitas melalui Sistem Elektronik.

6. **Manfaat apa saja yang didapat pemerintah melalui pemanfaatan Teknologi Informasi?**

   Teknologi Informasi bagi pemerintah bermanfaat dalam banyak hal. eGovernment

adalah salah satu bentuk pemanfaatan TI dalam penyelenggaraan pemerintah yang bermanfaat untuk,antara lain:

- *meningkatkan diseminasi infirmasi dan akses kepada informasi;dan*
- *meningkatkan akuntabilitas, transparansi, efisiensi dan efektivitas penyelenggaraan pemerintah.*

7. **Manfaat apa yang didapat oleh pelaku usaha melalui pemanfaatan Teknologi Informasi?**

   Beberapa manfaat melakukan transaksi secara elektronik yang dapat diperoleh pelaku usaha dengan memanfaatkan Teknologi Informasi adalah:

   1. *meningkatkan profit;*
   2. *memotong biaya;*
   3. *memperluas jaringan usaha;dan*
   4. *meningkatkan value chain;*

8. **Lembaga-lembaga apa saja yang telah dimiliki oleh Indonesia yang diperluklan dalam menjalankan dan menegakkan UU ITE?**

   Lembaga-lembaga yang telah dimiliki oleh Indonesia dalam menjalankan dan menegakkann UU ITE, antara lain:

   0. *ID-SIRTII : Indonesia - Security Incident Response Team on Internet Infrastructure;*
   1. *ID-CERT : Indonesia - Computer Emergency Response Team;*
   2. *PANDI : Indonesia Domain Name Registry;dan*
   3. *Cyber Crime Unit- Indonesia National Police;*

9. **Menyikapi berbagai kekurangan UU ITE apa yang harus dilakukan agar tidak mengganggu aktivitas/transaksi di dunia cyber dan dapat melindungi pengguna serta menjaga budaya bangsa?**

Kita belum bisa menilai apakah UU ITE ini "kurang".Kita membutuhkan waktu untuk melihat bagaimana pelaksanaan dan penegakkan undang-undang ini . Yang pasti secara spesifikdiatur dalam UU ITE akan diatur lebih lanjut dalam Peraturan Pemerintah dan peraturan pelaksanaannya. JIka dirasa masih kurang, dilengkapiu dan disempurnakan melalui praktek hukum atau yurisprudensi.

10. **Ada beberapa Peraturan Pemerintah yang diamanatkan oleh UU ITE? Bagaimana pemerintah melaksanakn amanat tersebut?**

UU ITE mengamanatkan sembilan Peraturan Pemerintah (PP) :

0. *Lembaga Sertifikasi Keandalan(Pasal 10 ayat (2));*
1. *Tanda Tangan Elektronik (Psal 11 ayat (2));*
2. *Penyelenggara Setifikasi Elektronik (Pasal 13 ayat (6));*
3. *Penyelenggara Sistem Elekronik (Pasal 16 ayat (2));*
4. *Transaksi Elektronik (Pasal 17 ayat (3));*
5. *Agen Elektronik (Pasal 22 ayat(2));*
6. *Nama Domain (Pasal 24 ayat (4));*
7. *Tata Cara Intersepsi (Pasal 31 ayat (4));dan*
8. *Peran Pemerintah dalam memfasilitasi pemanfaatan teknologi informasi, khususnya dalam hal data strategis (Pasal 40 ayat (6)).*

11. **Pemerintah akan membuat UU Tindak Pidana Teknologi Informasi (TiPiTI). Apakah UU diperlukan? Karena UU tersebut bisa merupakan duplikasi dari UU ITE?**

RUU TiPiTI akan melengkapi UU ITE. UU ITE telah menerapkan prinsip-prinsip dari UNCITRAL Model Law on eCommerce dan eSignature; EU Directives on eCommerce dan eSignature; dan juga Convention on Cybercrime. RUU TiPiTI merupakan implementasi dari Convention on Cybercrime. Dalam konvensi ini ada dua hal besar yang dibicarakan: (i) hukum materil (substantive law), dan (ii) prosedur (procedural law). RUU TiPiTI akan mengakomodir ketentuan-ketentuan yang belum diatur dalam UU ITE, khususnya mengenai prosedur. Oleh karena itu, kehadiran UU TiPiTI sangat dibutuhkan dan akan melengkapi UU ITE.

Ada dua alternatif, apakah membuat undang-undang sendiri tentang UU Tindak Pidana Teknologi Informasi atau menyempurnakan ketentuan pidana yang dimuat dalam UU ITE. Pilihan diantara keduanya, tergantung kepada gelagat perkembangan tindak pidana di bidang ITE (kejahatan siber).

12. **Berdasarkan Pasal 2 UU ITE tersebut, apakah aparat penegak hukum dapat langsung menindak WNA atau badan hukum asing yang melakukan kejahatan di luar wilayah Indonesia tetapi memiliki akibat hukum di Indonesia?**

    Salah satu keunikan tindak pidana siber adalah bahwa satu tindak pidana yang dilakukan di suatu negara dapat menimbulkan akibat yang dilarang di negara lain. Ketika hal ini terjadi, permasalahan mengenai yurisdiksi yang dapat melakukan law enforcement terhadap tindak pidana tersebut. Tiap negara memiliki kedaulatan penuh terhadap wilayahnya.

    Oleh karena itu sangat penting bagi aparat penegak hukum untuk melakukan kerja sama (mutual assistance) dengan aparat penegak hukum negara lain dalam mengungkap satu tindak pidana. Kepentingan tersebut harus dijustifikasi dengan peraturan perundang-undangan di negara Indonesia.

13. **Banyak situs porno yang diakses oleh pengguna internet di Indonesia berdomisili di luar negeri (meskipun dimungkinkan sebagian gambarnya berasal dari Indonesia). Apakah secara hukum pemerintah Indonesia dapat menegakkan UU ITE ke situs yang lokasi *servernya* berada diluar negara Indonesia?**

    Berdasarkan Pasal 2 UU ITE, pemerintah Indonesia memiliki kewenangan untuk menegakkan hukum sepanjang ada pelanggaran terhadap UU ITE dan/atau ada kepentingan bangsa Indonesia yang dirugikan.

    Mengingat locus delicti dan server tersebut berada di wilayah Negara lain dan tidak ada maksud secara khusus ditujukan kepada masyarakat Indonesia atau dengan maksud khusus untuk merugikan kepentingan masyarakat Indoneisa, maka perbuatan tersebut tidak dapat dikenakan hukum pidana Indonesia. Pemerintah Indonesia hanya bisa mencegah disebarluaskannya pronografi yang di unduh dari situs porno tersebut atau memproteksi situs agar tidak bisa dibuka di Indonesia.

    Masing-masing Negara memiliki hukum yang berbeda-beda, bagi Negara yang tidak melarang pornografi, maka hukum Indonesia tidak bisa diterapkan kepada pelaku yang berada di negeri lain. Kecuali, jika Negara yang bersangkutan melarang pornografi seperti hukum Indonesia dan keduanya Negara kemudian mengadakan kerjasama.

14. **Bagaimana kewenangan aparat penegak hukum dalam melakukan penegakan hukum *(law enforcement)* terhadap pelanggaran UU ITE? Misalnya terjadi kejahatan kartu kredit yang dilakukan oleh Orang asing dari luar negeri?**

    UU ITE menganut asas extra territorial jurisdiction. Hal ini termaktub dalam pasal 2 UU ITE. UU ITE berlaku untuk setiap Orang yang melakukan perbuatan melawan hukum sebagaimana diatur dalam UU ITE ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia (umumnya juga melarang penyalahgunaan/kejahatan dengan menggunakan kartu kredit), yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

    Dengan demikian, perbuatan hukum yang dilakukan baik oleh WNI maupun WNA di luar wilayah Indonesia; atau baik oleh badan hukum Indonesia maupun badan hukum asing, sepanjang memiliki akibat hukum di Indonesia, dapat ditindak sesuai dengan UU ITE.

<u>Perdata dan Hukum Acara Perdata</u>

15. **Apabila suatu situs memberikan peringatan agar berhati-hati ketika bertransaksi dengan Orang Indonesia, apakah pengelola situs ini dapat dikenal dan digugat sesuai dengan UU ITE?**

    Peringatan tersebut belum tentu merupakan tindakan penghinaan atau pencemaran nama baik karena peringatan tersebut dapat berupa fakta. Jadi pengelola situs bisa saja hanya memberitahukan fakta agar orang lain berhati-hati.Seperti yang ditanyakan oleh seorang pengguna
    situs alibaba.com di bawah ini.

    WARNING -World of Warcraft Scammers - Indonesia

Hi, PLEASE BEWARE OF INDONESIAN SCAMMERS! We are a reseller of online game gards, and we tried to get some contacts trough Alibaba.com. Unfortunately many offers we found on Alibaba.com are probably set by scammers. (http://resources.alibaba.com/topic/292264/WARNING_World_of_Warcraft_Scammers_Indonesia.htm,diakses 1 Februari 2009)

16. **Dalam satu transaksi yang dilakukan melalui internet konsumer akan diminta untuk mengkonfirmasi transaksi dengan mengklik ikon "yes". Bagaimana UU ITE melindungi konsumer yang melakukan transaksi elektronik seperti itu?**

    Dengan mengklik ikon "yes", konsumen dianggap telah menyetujui persyaratan dan kondisi (terms and condition) yang diatur dalam kontrak elektronik karena ikon "yes" tersebut sama halnya dengan tanda tangan konsumen. Dengan mengklik ikon tersebut, konsumen menjadi terikat secara hukum terhadap transaksi yang dilakukannya.

    UU ITE telah mengimplementasikan prinsip-prinsip perlindungan konsumen dalam pasal-pasalnya yang tujuannya memberikan kepastian hukum perlindungan bagi para konsumen dalam melakukan transaksi elektronik.

    Pasal 9 UU ITE telah mengatur bahwa pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

    Salah satunya, dalam Pasal 23 ayat (3) jo. penjelasan pasal tersebut menentukan setiap Orang dilarang menggunakan nama domain yang menyesatkan konsumen.

    Lebih lanjut, perlindungan konsumen juga semakin dikuatkan dengan pemberian sanksi pidana terhadap pihak yang merugikan konsumen.
    Dalam Pasal 28 ayat (1) UU ITE telah diatur bahwa setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dapat dipidana dengan oidana penjara maksimal enam tahun dan/atau denda maksimal satu miliar rupiah.

    Akan tetapi, konsumen memiliki tanggung jawab untuk bertindak dengan itikad baik dan hati-hati. Oleh karena itu, sebelum mengklik ikon "yes" konsumen seharusnya membaca dengan baik tawaran penjual barang/jasa di internet, kehati-hatian ini adalah salah satu prinsip yang diatur dalam pasal 3 UU ITE.

17. **Apabila penjual dan pembeli melakukan transaksi melalui internet. Komunikasi dilakukan melalui email dan menyetujui harga dan barang. Kemudian pembeli tidak menerima barang sesuai dengan kesepakatan atau penjual tidak menerima pembayaran sesuai dengan yang diperjanjikan. Apa yang harus dilakukan oleh para pihak tersebut? Karena pada faktanya, tidak ada hitam di atas putih.**

    Sepanjang telah memenuhi syarat-syarat sahnya suatu perjanjian maka Email yang dimaksud dapat dikategorikan sebagai kontrak Elektronik, yaitu perjanjian antara para pihak yang dibuat melalui Sistem Elektronik. (Pasal 1 butir 17 UU ITE).

Ketika telah terjadi kesepakatan mengenai barang dan harga maka telah ada perjanjian antara penjual dan pembeli tersebut. Oleh karena itu pihak yang merasa dirugikan dapat menggugat pihak yang lain itu dengan dasar wanprestasi. Email tersebut dapat dijadikan alat bukti sebagaimana dimaksud dalam pasal 5 UU ITE.

Lebih lanjut lagi, sepanjang terdapat dugaaan penipuan, pihak yang dirugikan dapat melaporkan adanya tindak pidana penipuan.

18. **Bagaimana jika tanda tangan kita di-*scan* dan digunakan dalam satu transaksi yang tidak kita ketahui dan setujui?**

Dalam prakteknya, tanda tangan dapat di-scan untuk kepentingan transaksi melalui elektronik. Pada prinsip jika kedua belah pihak menerima bahwa tanda tangan yang di-scan tersebut adalah representasi dari pihak yang melakukan hubungan hukum maka selayaknya dapat diakui sebagai bukti yang sah.

Sesuai dengan Pasal 1 butir 12, Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang digunakan sebagai alat vertifikasi dan autentikasi. Oleh karena itu, sepanjang tanda tangan yang di-scan dalam penggunaannya dapat menjelaskan adanya proses vertifikasi dan autentikasi maka dapat dikatakan sebagai Tanda Tangan Elektronik. Jika ada keraguan, pihak yang meragukan dapat melakukan alat bukti lain sebagai pendukung agar meyakinkan kebenarannya.

Pihak lain tidak boleh menggunakan tanda tangan orang lain atas nama dirinya, perbuatan tersebut termasuk kategori tindak pidana pemalsuan tanda tangan, akibatnya hubungan hukum menjadi batal dengan sendirinya. Oleh sebab itu, kedua belah pihak harus memiliki itikad baik dan saling percaya atau membuat kode-kode lainnya sebagai bukti orisinalitasnya.

Hakim akan melakukan pembuktian terhadap keotentikan tanda tangan terebut dan juga terhadap persetujuan penggunaan tanda tangan itu. Dalam pembuktian hakim akan memanggil saksi-saksi termasuk pihak yang merasa tanda tangannya dipalsukan dan juga para ahli untuk memberikan keterangan.

"On the Internet, nobody knows you're a dog."

19. **Bagaimana sebaiknya pengguna kartu kredit menggunakan kartunya dalam bertransaksi secara elektronik agar aman?**

Berikut beberapa masukan dalam melakukan transaksi elektronik:

1. *Usahakan agar Anda menggunakan komputer pribadi ketika melakukan transaksi elektronik. Penggunaan komputer publik seperti di warnet memberikan resiko lebih tinggi dari penggunaan komputer pribadi. Saat ini sudah ada banyak hardware khusus yang dihubungkan pada kabel keyboard yang akan mencatat semua yang Anda ketikkan melalui keyboard tersebut (keyloger).*
2. *Perhatikan dengan seksama kredibilitas situs yang menawarkan barang dan/atau jasa pada Anda. Situs yang memiliki trust mark atas situs yang meiliki sistem pengamanan komunikasi (contoh:Secure Socket Layer(SSL)) tentunya memberikan kenyamanan bertransaksi yang lebih daripada situs yang tidak memilikinya.*
3. *Jangan berikan tanda tangan elektronik anda (PIN atau tanda tangan digital) pada orang lain.*
4. *Simpan faktur transaksi yang dilakukan dengan menggunakan kartu kredit.*
5. *Pembersihan terhadap script Trojan dan cookies harus dilakukan secara rutin.*
6. *Matikan atau awasilah modem anda jika tidak sedang dalam keadaaan online. Anda perlu waspada jika lampu indikator send/receive data pada modem anda berkedip-kedip. Hal tersebut dapat merupakan tanda-tanda kerusakan modem, atau ada yang berusaha mengirim data anda pada saat tidak online.*
7. *Biasakanlah mengklik tombol logout, logoff atau sign out pada account internet banking atau account keuangan online anda lainnya.*
8. *Bila memungkinkan, mintalah jaminan dari pihak bank penerbit kartu kredit anda untuk selalu melakukan konfirmasi secara real time (langsung kepada anda melalui telepon) apabila ada transaksi pembelanjaan melalui kartu kredit.*

20. **Bagaimanakah pengaturan UU ITE mengenai perlindungan hak-hak pribadi?**

Menurut UU ITE hak pribadi mengandung pengertian:

1. *hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan;*
2. *hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan diawasi atau dimata-matai;*
3. *hak untuk memiliki dan menyimpan informasi atau data pribadi tanpa ada intersepsi dari Orang lain. (Penjelasan Pasal 26 ayat (1) UU ITE)*

21. **Pengiriman jasa premium seperti SMS berhadiah menimbullkan banyak masalah karena layanan seperti itu sering dikirimkan kepada konsumen tanpapersetujuan yang bersangkutan. Terkadang konsumen tidak menyadari dampak yang ditimbulkan layanan tersebut. Bagaimana Pemerintah, khususnya Departemen Komunikasi dan Informatika menyikapi hal tersebut?**

Pentingya perlindungan terhadap privasi seseorang telah diakomodir oleh UU ITE. Dalam Pasal 26 ayat (1) UU ITE diatur bahwa penggunaan setiapinformasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

Lebih jauh, UU ITE telah memberikan hak bagi konsumen yang merasa haknya diganggu oleh pengguna data pribadi tanpa persetujuannya. (Pasal 26 ayat (2)) Pasal 26 UU ITE ini telah di implementasikan lebih konkrit lagi dengan dikeluarkannya Menteri Nomor : 01/PERM/M.KOMINFO/01/2009 tentang PEnyelenggaraan Jasa Pesan Premium dan Pengiriman Jasa Pesan Singkat (Short Messaging Services/SMS) ke banyak Tujuan (Broadcast)

Beberapa aturan penting yang melindungi para konsumen yang diatur dalam Permen tersebut adalah :

1. *Jasa premium dan SMS Broadcast hanya dapat dikirimkan kepada konsumennya yang menyatakan niatnya untuk menerima jasa tersebut, baik melalui aktivitas maupun permintaan.*
2. *Ada mekanisme untuk berhenti dari jasa premium dan SMS Broadcast.*
3. *Adanya sanksi bagi penyedia jasa premium dan SMS broadcast bila melanggar privasi konsumen.*

22. **Apa yang dimaksud dengan tanda tangan elektronik?**

Berdasarkan Pasal 1 butir 12 UU ITE, Tanda Tangan adalah Tanda Tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terakit dengan

Informasi Elekronik lainya yang digunakan sebagai alat verifikasi dan autentifikasi.

Tanda tangan elektronik dapat dibuat atu diperoleh dari berbagai macam metode dan teknologi sepanjang verifikasi dan autenfikasi.

23. **Apa fungsi tanda tangan elektonik?**

Seperti tanda tangan biasa , tanda tangan elektronik berfungsi sebagai alat verifikasi dan autentifikasi. Maksudnya tangan elektronik dapat digunakan untuk mengidentifikasi si penandatangan terkait dengan Informasi dan/atau Dokumen Elektronik, dan untuk mengindikasikan persetujuan Penandatangan atas Informasi Elektronik tersebut.

24. **Apa bentuk tanda tangan elektronik itu?**

Berdasarkan pengertian dan fungsi tanda tangan elektronik, tanda tangan elektronik dapat berupa :

1. *Tindakan menekan ikon "yes" atau "i accept";*
2. *Tanda tangan basah yang yang dipidai(scan);*
3. *Pengunaan personal identification (PIN);*
4. *Tanda tangan yang menggunakan teknik kritografy;*
5. *Tanda tangan yang menggunakan teknik biometrik;*

25. **Apa perbedaan tand tangan elektronik dengan tanda tangan digital?**

Tanda tangan digital adalahh tangda tangan elektronik yang menggunakan teknik kriptografi. Dengan kata lain, tanda tangan digital merupakan bagian dari tanda tangan elektronik.

Tanda tangan digital dibuat dan diverifikasi dengan menggunakan teknik ini, pesan ditransformasikan ke dalam bentuk yang tidak terbaca dan dapat dikembalikan menjadi bentuk semula jika pesan itu dibuka dengan kunci yang tepat.

26. **Apa yang dimaksud dengan tanda tangan biometrik?**

Biometrik bersal dari kata Yunani: (bio=hidup) dan (metrik=ukuran). Karateristik unik tersebut dapat berua: (I)sidik jari, (ii)retina, (iii)iris, (iv)wajah, (v)tangan, (vi)wajah.
Tanda tangan biometrik adalah tanda tangan elektronik yang menggunakan karakteristik unik seseorang dalam melakukan verifikasi dan autenfikasi.

27. **Mengapa UU ITE tidak mengfokuskan pada pengaturan salah satu jenis tanda tangan elektronik (misalnya tanda tangan digital)?**

Prinsip yang diterapkan dalam UU ITE adalah teknolgi netral. Hal ini di tegaskan

dalm pasal 3 UU ITE. Teknologi selalu berkembang dan oleh karena itu pemerintah memberikan ruang bagi teknologi yang ada dan akan ada untuk memberikan layanan yang terbaik bagi pengguna tanda tangan elektronik

28. **Prisip teknologi netral yang diterapkan pemerintah adalm UU ITE dapat menimbulkan resiko dalam Transaksi Elektronik karena ada tanda tangan Elektronik yang aman dan ada yang tidak aman. Bagaimana Pemerinatah meraspon hal ini?**

Pemerintah memberikan kebebasan kepada masyarakat untuk memilih tanda tangan elekronik yang sesuai dengan kebutuhannya.

Pemerintah juga telah mengatur, dalam UU ITE, adanya sertifikasi elektronik. Berdasarkan Pasal 1 butir 9 UU ITE, Sertifikasi Elektronik adalah sertifikasi yang bersifat elektronik yang memuat TAnda Tangan Elektronik dan Identitas yang menunjukan status subjek hukum para pihak dalam Transaksi yang di keluarkan oleh Penyelenggara Sertifikasi Elektonik.

Tujuan sertifikasi elektronik ini adalah untuk mengenali atau menumnjukan atau mengkkonfirmasi suatu keterkaitan (link) antara data pembuatan tanda tangan dengan penanda tangan itu sendiri. Link itu di buat ketika data pembuatan tanda tangan di hasilkan. Oleh karena itu, dalam proses sertifikasi elektronik ini, selayaknya ada pihak ketga yang terpercaya (trusted third party) yang dilibatkan dalam pembuatan tanda tangan.

Pihak ketiaga ini dapat melakukan identifikasi, veritifikasi dan autentifikasi terhadap penanda tangan. Dengan adanya pihak ketiga dan sertifikasi elektronik, maka transaksi elektronik menjadi lebih aman.

29. **Siapa saja yang dapat menyelenggarakan Sertifikasi Elektronik?**

Sertifikasi Elektronik dapat di selenggarakan oleh :

1. *Penyelenggaraan Sertifikasi Elektronik Indonesia, yaitu harus berbadan hukum dan berdomisili di Indonesia; dan*
2. *Penyelenggaraan Sertifikasi Elektronik Asing yang harus terdaftar di Indonesia.*

30. **Bagaimana seorang konsumen tahu bahwa Sertifikasi Keandalan Yang ada di dalam website terpercaya?**

Pada prinsipnya, satu Sertifikasi Keandalan dinyatakan terpercaya jika diterbitkan oleh Penyelenggara Sertifikasi Keandalan yang di akui, disahkan dan di awasi oleh instasi yang berwenang.

Untuk mendapatkan pengakuan dan pegesahan tersebut, Penyelenggara Sertifikasi

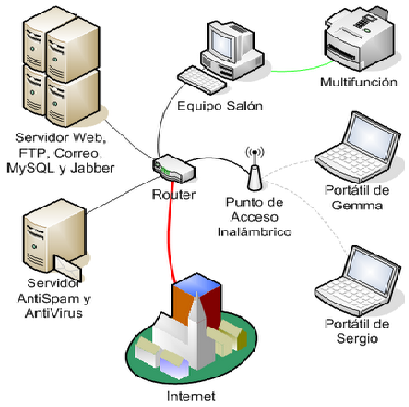
Keandalan itu dan SIstem Elektronik yang di selenggarakannya harus sesuai dengan PEraturan perundang-undangan, termasuk harus memnuhi standar-standar yang terkait.

31. **Siapa yang dapat membentuk Lembaga Sertifikat Keandalan?**

Lembaga Sertifikasi dapat dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah. (Pasal 1 butir 11 UU ITE).

32. **Kapankah Transaksi Elektronik terjadi?**

UU ITE menentukan bahwa Transaksi ELektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima. Persetujuan penawaran Transaksi Elektronik harus dilakukan dengan pernyataan penerimaansecara elektronik. Akan tetapi ketentuan ini dapat disimpangi oleh para pihak, sesuai dengan asas kebebasan dalam berkontrak. (Pasal 20 UU ITE)



33. **Siapa yang bertanggung jawab terhadap transaksi yang dilakukan secara elektronik?**

UU ITE telah mengatur bahwa:

1. Jika Transaksi Elektronik dilakukan oleh paran pihak sendiri, maka merekalah yang bertanggung jawab terhadap segala akibat hukum dalam pelaksanaan Transaksi Elektronik;
2. Jika Transaksi Elektronik dilakukan melalui seorang kuasa, maka segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa;
   aknan tetapi jika Transaksi Elektronik dilakukan melalui agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.(Pasal 21 UU ITE)

34. **Apa yang dimaksud dengan Kontrak Elekronik?**

Berdasarkan Pasal 1 butir 17 UU ITE,KOntrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik. Jika dihubungkan dengan BAB V tentang Transaksi Elektronik, khususnya Pasal 18, Kontrak Elektronik dibuat oleh para pihak karena adanya Transaksi Elektronik.

35. **Bagaimana persyaratan sahnya perjanjia yang dibuat melalui media elektronik?**

Pada prinsipnya syarat sahnya perjanjian didasarkan pada 1320 KUHPerdata, yaitu:
a. adanya kesepakatan antara para pihak;
b. para pihak cakap melakukan perjanjian;
c. adanya hal tertentu yang diperjalankan;
d. adanya sebab yang halal;

Selain persyaratan -persyaratan tersebut, UU ITE juga menambahkan beberapa persyaratan lain, misalnya:
a. beritikad baik (Pasal 17 ayat (2) UU ITE, syarat ini juga telah ada dalam KUHPerdata);
b. ketentuan mengenai waktu pengiriman dan penerimaan Informasi dan/atau Transaksi Elektronik (Pasal 8);
c. menggunakan Sistem Elektrpnik yang andal dan aman serta bertanggung jawab jawab (Pasal 15);

36. **Apakah UU ITE memperbolehkan adanya kontrak baku (standar)?**

UU ITE tidak secara tegas menentukan boleh tidaknya kontrak baku (standar). Akan tetapi, berdasarkan UU No.8 Tahun 1999 Pasal 9 UU ITE, maka kontrak baku diperbolehkan, sepanjang tidak merugikan konsumen atau memenuhi syarat berdasarkan undang-undang perlindungan konsumen.

37. **Apa saja informasi yang penting untuk disediakan oleh Penyelenggara Agen Elektronik?**

Agen Elektronik sepatutnya menyediakan,memuat atau menyampaikan informasi tentang, antara lain:
a. Penyelenggara Agen Elektronik;
b. obyek yang ditransaksikan;
c. syarat kontrak dan prosedur bagaimana mencapai kesepakatan;
d. jaminan privacy dan/atau proteksi data personal;dan
e. kelayakan atau keamanan sistem.

38. **Apakah Sistem Administrator/sysadmin (Administrator Sistem Elektronik dalam suatu perusahaan diperbolehkan mengakses komputer karyawan perusahaan itu>?**

Pada prinsipnya sesuai dengan kewenangannya, sysadmin boleh mengakses komputer karyawan dalam rangka melaksanakan tugas dan tanggung jawab atau dalam kondisi yang mengharuskan untuk melakukan tindakan tersebut.

Tugas dan tanggung jawab seorang Sysadmin yang utama adalah memastikan Sistem Elektronik yang ditanganinya dapat beroperasi dengan aman dan andal; hal ini sesuai dengan Pasal 15 UU ITE,bahwa Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab. Oleh karena itu, dalam hal timbul masalah pada Sistem Elektronik dan mengharuskan sysadmin mengakses komputer karyawan dalam rangka memperbaiki masalah tersebut, maka sysadmin dapat melakukannya. DEnag kata lain, dalam kondisi tersebut sysadmin memiliki hak dan tidak melawan hukum.

Peranan seorang sysadmin sangat vital. Sysadmin memiliki tanggung jab dalam menjaga kerahasiaan data enggotanya karena seorang sysadmin juga bertugas : (i) mengumpulkan data dan informasi anggotanya, (ii) meng-up-date informasi account pengguna, dan (iii) membuat cadangan data (backups). Selama tidak berkaitan dengan tanggung jawabnya, maka sysadmin tidak boleh mengakses komputer karyawan tanpa ijin dari karyawan tersebut.

Berdasarkan Pasal 30 UU ITE, adalah suatu tindakan pidana apabila setiap orang dengan sengaja dan tanpa hak atau melawan hukum

1. *mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun;dan*
2. *mengakses KOmputerdan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi Elektronik dan/atau Dokumen Elektronik.*

Mencerminkan ketentuan ini, Sysadmin perlu menerapkansistem fleksibel bagi para karyawan. MIsalnya sysadmin juga dapat suatu sistem bahwa dalam Sistem Elektronik yang diselenggarakan dibagi menjadi dua bagisn besar:(i) yang dapat diakses oleh siapa saja, dan (ii) yang hanya dapat diakses oleh karyawan yang bersangkutan. Sistem ini dapat diterapkan pada, misalnya dalam perusahaan atau kantor yang membutuhkan akses kekomputer karyawan lain secara cepat untuk mencari atau mengambil dokumen lain.

Kewenangan sysadmin dan anggotanya sebaiknya dideklarasikan dalam bentuk IT Policy yang diterapkan oleh pimpinan organisasi yang bersangkutan.

Pidana dan Hukum Acara Pidana

39. **Bagaimana penerapan sanksi pidana pornografi apabila pengaturan tindakan pornografi dalam UU ITE berbeda dengan dalam UU pornografi?**

Pengaturan UU ITE dalam pornografi, khusunya ketentuan mengenai pornografi dan sanki pidananya perlu disinkronasikan.

UU ITE dan UU Pornografi pada dasarnya saling melengkapi. Pasal 27 UU ITE melarang adalah Orang untuk mendistribusikan, mentransmisikan, dan/atau membuat dapat diakses muatan yang melanggar kesusilaan. SEdangkan UU Anti Pornografi mengatur batasan pornografi yang merupakan bagian dari "hal yang melanggar kesusilaan"yang diatur dalam UU ITE.

Pasal 1 butir 1 UU Pornografi mendefinisikan Pornografi sebagai "gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui komunikasi dan/atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat."

Kemudian, Pasal 44 UU Pornografi menyatakan bahwa peraturan perundang-undangan yang mengatur tindak pidana pornografi dinyatakan tetap berlaku sepanjang tidak bertentangan denagn undang-undang tersebut.

40. **Bagaimanakah kewenangan Aparat Penegak Hukum seperti Polisi, Jaksa, KPK dalam melakukan penyadapan (intersepsi) komunikasi yang diatur dalam UU ITE?**

Pada prinsipnya komunikasi antara para pihak adalah hak privasi. Oleh karena itu Pasal 31 UU ITE menentukan bahwa pada prinsipnya intersepsi dari sistem elektronik merupakan satu tindak pidana, kecuali jika dilakukan secara legal oleh parat penegak hukum berdasarkan peraturan perundang-undangan.

UU ITE telah memberikan pengecualian bagi Aparat Penegak Hukum untuk melakukan intersepsi hanya apabila Aparat Penegak Hukum tersebut memiliki kewenangan untuk itu sebagaimana yang diatur menurut undang-undangnya masing-masing.Misalnya UU tentang Korupsi memberikan kewenangan bagi KPK untuk melakuakn intersepsi, demikian juga dalam UU Narkotika dan Psitropika

memberikan kewenangan bagi kepolisian dan kejaksaan untuk melakukan intersepsi.

Kewenangan untuk melakukan intersepsin diberika oleh undang-undang tesebut karena tindak pidana yang diatur dalam undang-undang itu adalah tindak pidana yang dinilai sarat menggunakan teknologi informasi dalam me;lakukan transaksi.

41. **Apakah semua hasil intersepsi (pembicaraan) akan diungkapkan dalam persidangan satu tindak pidana?**

    Prinsip bahwa komunikasi yang dilakukan para pihak adalah privasi mereka sendiri, tetap dipertahankan dalam pengungkapan satu tindak pidana. Oleh karena itu, aparat penegak hukum hanya akan mengungkap informasi yang terkait erat dengan tindak pidana yang dilakukan. Sedangkan informasi yang bersifat pribadi dan tidak relevan tidak akan diungkap.

42. **Akhir-akhir ini pihak Aparat Penegak Hukum (APH) melakukan pemeriksaan laptop di bandara. Sejauh mana pemerintah dapat memastikan bahwa software yang ada di dalam laptop tersebut original dan bagaimana memastikannya?**

    Tindakan APH tersebut dilakukan dalam rangka penegakan Hak Kekayaan atas Intelektual (HAKI); untuk mengetahui apakah piranti lunak yang digunakan dalam laptop tersebut asli atau tidak. Dalam memeriksa keaslian itu, APH menggunakan alat dan piranti lunak khusus yang telah tersertifikasi. Hanya aparat yang telah dilatih untuk menggunakannya lah yang dapat melakukannya. Oleh karena itu, APH juga harus meningkatkan kapabilitas TIK personalnya.

43. **Apabila seseorang merasa ditipu dalam menggunakan kartu kredit; dia ditagih untuk transaksi yang ia tidak lakukan. Tindak pidana apa yang dapat dikenakan kepada penipu tersebut?**

    Untuk menentukan tindak pidana yang terjadi maka harus dilakukan penyelidikan dan penyidikan. Penyelidikan dan penyidikan tersebut dapat dilakukan apabila ada laporan kepada kepolisian. Jika kejadian itu terjadi maka pemilik kartu kredit dapat mengkonfirmasikan kepada penyelenggara kartu kreditnya dan meminta bukti. Pelaku penggunan kartu kredit orang lain untuk melakukan transaksi dapat dikenakan tindak pidana pemalsuan dokumen atau ilegal access.

44. **Apa yang dimaksud dengan Cybercrime itu?**

Cybercrime dalam arti sempit (computer crime) adalah "any ilegal behavior directed by means of electronic operation that target the security of compiter system and the data processed by them" Sedangkan cybercrime dalam atri luas (Computer related crimes) adalah "any ilegal behavior comitted by means on relation to, a computer system offering or system or network, including such crime as ilegal possession in, offering or distributing information by means of computer system or network.

45. **Bagaimana Convention on Cybercrime mengatur hukum pidana materil?**

Convention on cybercrime telah mengatur tindak-tindak pidana siber, yaitu:

1. *illegal acess;*
2. *illegal interception;*
3. *data interference;*
4. *sytem interference;*
5. *misuse of device;*
6. *computer-related forgery;*
7. *computer-related fraud;*
8. *offence related to child pornography;*
9. *offences related to infringments of cppyright abn related rights;*
10. *attempt and and aiding or abetting;*

46. **Bagaimana pengaturan perbuatan yang dilarang dalam UU ITE?**

UU ITE telah mengatur beberapa perbuatan yang dilarang, antara lain:

1. *Distribusi, transmisi, membuat dapat diaksesnya konten tertentu yang ilegal (Pasal 27 s.d Pasal 29 UU ITE);*
2. *illegal access (Pasal 30);*

3. *illegal interception (Pasal 31);*
4. *data interference (Pasal 32);*
5. *system interference (Pasal 33);*
6. *misuse of device (Pasal 34);*
7. *computer related forgery (Pasal 35);*

47. **Apa saja perbedaan antara cybercrime dengan kejahatan konvensional?**

Perbedaan antara cybercrime dengan kejahatan konvensional dapat dilihat sebagai berikut.

Cybercrime	Kejahatan Konvensional
Terdapat penggunaan IT.	Tidak ada penggunaan TI secara langsung.
Alat bukti; digital evidnce.	Alat bukti fisik (terbatas menurut Pasal 184 KUHP).
Pelaku dan korban komputer berada dimana saja.	Pelaku dan korban biasanya terdapat dalam satu tempat
Pelaksana kejahatan: non fisik (cyberspace).	Pelaksana kejahatan: fisik (dunia "nyata").
Proses penyidikan melibatkan laboratorium forensik komputer.	Proses sidik tidak melibatkan laboratorium forensik komputer.
Sebagian proses sidik dilakukan di cyberspace; virtual undercaver.	Proses sidik dilakukan di dunia nyata.
Penanganan komputer sebagai TKP (crime scence).	Tidak ada penanganan komputer sebagai TKP.
Dalam proses persidangan, keterangan ahli menggunakan ahli TI	Dalam proses persidangan, keterangan ahli tidak menggunakan ahli TI

48. **Pengaturan Pasal 43 ayat(6) UU ITE kerja sama antara penyidik dan penuntut umum terlalu kompleks. Mengapa aparat tidak menggunakan KUHAP saja?**

Ketentuan sebagaimana diatur Pasal 43 ayat(6) UU ITE penting karena, antara lain: (i)adanya koordinasi antara aparat penegak hukum (polisi, jaksa dan hakim) dalam rangkaian proses pidana mulai dari penyidikan, penuntutan, hingga pembacaan vonis; dan (ii)hak asasi tersangka lebih terjamin. DPR lebih menyetujui konstruksi penangkapan dan penahanan seperti ini. Petunjuk pelaksanaan pasal ini akan diatur lebih lanjut.

49. **Dalam penanganan tindak pidana yang menggunakan sistem elektronik seperti korupsi, kehadiran pusat data menjadi sangat penting. Bagaimana UU ITE mengakomodir kepentingan ini?**

    Pasal 40 ayat(6) UU ITE telah mengamanatkan agar pemerintah mengatur lebih lanjut mengenai data strategis. Pengaturan ini akan mengakomodir kepetingan tersebut dalam penanganan tindak pidana yang menggunakan Sistem Elektronik.

50. **Adanya pengaturan tindak pidana mengenai penyiaran kabar bohong menimbulkan permasalahan sendiri. Dimanakah locus delicti tindak pidana tersebut?**

    Penentuan locus delicti (dan juga tempus delicti) terkait dengan jenis tindak pidana: apakah tindak pidana tersebut adalah tindak pidana:
    a. Formil. Penentuan tempus dan locus delicti dari tindak pidana yang jenisnya formil berada dalam tempat dimana dan waktu ketika tindak pidana itu dilakukan. Misalnya pencurian 362 KUHP sedangkan,
    b. Materil. Penentuan tempus dan locus delicti dari tindak pidana yang jenisnya materil berada pada tempat dimana dan waktu ketika akibat yang dilarang itu timbul. (Misalnya, pembunuhan biasa pasal 338 KUHP).

    Literatur hukum yang digunakan di Indonesia (doktrin) mengenal adanya tiga teori locus delicti, yaitu:

    1. *Teori perbuatan fisik (de leer van de lichamelijke daad);*
    2. *Teori bekerjanya alat yang digunakan (de leer van het instrumen);*
    3. *Teori akibat (de leer van het gevolg);*
    4. *Teori tempat yang jamak (de leer van de meervoudige tijd)*
    5. *Kombinasi dari teori tersebut.*

    Akan tetapi ketentuan Pasal 84 ayat(2) KUHAP yang merupakan legislasi di Indonesia mengatur bahwa pada prinsipnya locus delicti suatu tindak pidana adalah tempat dimana tindak pidana itu dilakukan.

KUHAP juga membuka kemungkinan bahwa terhadap beberapa perkara pidana yang satu sama lain ada sangkut pautnya dan dilakukan oleh seorang dalam daerah hukum pelbagai pengadilan negeri maka masing-masing pengadilan negeri dapat mengadili perkara pidana dengan dibuka kemungkinan penggabungan perkara. (Pasal 84 ayat(4) KUHAP).

Penentuan locus delicti dalam satu perkara tindak pidana adalah hal yang kompleks. Dalam tindak pidana, seorang pelaku tindak pidana dapat melakukan niat jahatnya di satu tempat dan tujuan dari niat jahatnya itu terjadi di tempat lain. Dalam proses pelaksanaan tindak pidana tersebut mungkin saja terjadi tindak-tindak pidana yang lain. Oleh karena itu, peran dan kerja sama pakar dalam hukum materil pidana dan prosedural pidana beserta ahli TI sangat dibutuhkan dalam menentukan locus delicti tersebut.

Akan tetapi, secara konkrit dapat digambarkan bahwa yang menjadi concern pihak kepolisian adalah lokasi hard disc berada. Dengan atau melalui hard disc ini diduga bahwa pelaku telah melakukan satu tindak pidana.]

51. **Bagaimana Penyidik menentukan locus delicti di lapangan?**

Penyidik dapat menentukan locus delicti dengan berdasrkan :

1. *Dimana pelaku meng-upload data ke internet/ melakukan serangan terhadap korbannya melaui jaringan internet; dan/atau*
2. *Server tempat jaringan di mana website tersebut berada dan dimana saja sepanjang web sites dapat diakses melalui internet serta termasuk akibat yang ditimbulkan.*

52. **Bagaimana Penyidik dapat menentukan tempus delicti dalam satu perkara cybercrime?**

Salah satu acuan bagi Penyidik dalam menentukan tempus delicti tindak pidana tersebut adalah dengan melihat pada log file.

53. **Bagaimana bentuk identitas dalam dunia siber?**

Identitas dapat berupa :

1. *Attributed Identity: Atribut yang diberikan (nama, tempat dan tanggal lahir);*
2. *Biometic Identity: Atribut yang unik (iris, sidik jari, retina, DNA);*

54. **Apa fungsi identitas dalam dunia siber?**

Sama seperti dalam dunia nyata, identitas sangat penting dalam berkomunikasi, yaitu berfungsi untuk autentifikasi dan veritifikasi.

55. **Apa yang dimaksud dengan identity theft?**

Yang di maksud dengan identity theft adalah seseorang sengaja dan tanpa hak atau melawan hukum menggunakan identitas orang lain untuk :

1. *Melakukan perbuatan melawan hukum lain; dan/ atau*
2. *Mengambil keuntungan atas nama orang tersebut. identity theft adalah salah satu bentuk dari Cybercrime: Ilegal dan Intentional.*

56. **Bagaimana bentuk perbuatan melawan hukum lain, atau bentuk mengambil keuntungan atas identitas orang yang di curi?**

Identitas yang dicuri dapat digunakan untuk melakukan teror atau penipuan, bahkan pemerasan. Selain itu, identitas yang di curi dapat digunakan untuk mengambil tanpa hak uang orang lain dari bank dengan menggunakan kartu kredit orang tersebut atau mentransfer uang dari bank ke bank lain.

57. **Bagaimana Identity theft dilakukan?**

Identity theft dapat dilakukan dengan :

1. *Ilegal access;*
2. *Ilegal interception;*
3. *Data interference;*
4. *System Interfernce;*
5. *Misuse of device;*
6. *Computer related forgery;*

58. **Bagaimana para pelaku identity theft dapat mendapatkan akses untuk mencuri identitas orang lain?**

Para pelaku dapat mencuri akses dengan melakukan, misalkan :

1. *Email Interception;*
2. *Email Spoofing;*
3. *Web data interception;*
4. *Network & volume Invasion;*
5. *Viruses, worms, trojan horses;*
6. *Password cracking;*

59. **Bagaimana mencegah identitas seseorang dicuri?**

Ada banyak cara yang dapat di lakukan untuk mencegah identitas di curi oleh orang lain, antara lain :

1. *Menggunakan anti virus dan pengamanan komputer lainnya yang terus di perbaharui (up to date), khususnya ketika akan melakukan transaksi elektronik;*
2. *Mengunjungi situs-situs yang dipercaya . Salah satu ciri situs yang dapat dipercaya adalah situs tersebut memilki trust mark.*
3. *Menghapus data-data pribadi setelah transaksi elektronik dilakukan.*

60. **Tantangan apa saja yang dihadapi oleh Penyindik dalam mengungkapkan satu tindak pidana di bidang teknologi informatika?**

Beberapa tantangan yang dihadapi oleh penyidik adalah :

1. *Perbedaan sistem hukum;*
2. *Tindak pidana terlambat;*
3. *Kebanyakan korban berasal dari luar negeri; dan*
4. *Korban tidak bersedia diperiksa sebagai saksi korban.*

61. **Apa yang dimaksud dengan *digital evidence?***

Digital evidence merupakan istilah untuk menjelaskan Informasi atau Dokumen Elektronik yang bisa dijadikan sebagai alat bukti yang disimpan dalam dan bisa di ambil kembali dari penyompanan data disebuah komputer atau media penyimpanan lainnya.

62. **Apakah pengaturan *digital evidence* merupakan pengaturan baru berdasarkan UU ITE?**

Sebenarnya sebelum ada UU ITE, telah ada undang-undang lain yang telah mengatur alat bukti digital, misalnya:

1. *Pasal 26 A UU20/2001 tentang Perubahan atas UU 31/1999 tentang pemberantasan Tipikor;*
2. *Pasal 15 ayat (1) UU 8/1997 tentang Dokumen Perusahaan;*
3. *Pasal 38 UU 15/2002 tentang Tindak Pidana Pencucian uang;*
4. *Pasal 27 Perpu 1/20002 tentang Pemberantsan Tindak Pidana Terorisme sebagaimana telah ditetapkan menjadi UU 15/2003;*
5. *Pasal 29 UU 21/2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang;*

63. **Bagaimana karakteristik Informasi atau Dokumen Elektronik sebagai *digital evidence*itu?**

Informasi atau Dokumen Elektronik sebagaimana dimaksud dalam UU ITE memiliki karakteristik, antara lain:

1. *tidak mudah rusak;*
2. *mudah diperbanyak;*
3. *mudah hilang;*

64. **Melihat karakteristik alat bukti digital tersebut. Bagaimana Penyidik menangani alat-alat bukti digital yang ditemukan dilapangan.**

Menurut ACPO, dalam menangani digital evidence, prinsip-prinsip yang harus dijalankan adalah sebagai berikut.

1. *tindakan penyidik tidak boleh mengubah data yang ada dalam sebuah media elektronik sebagai media penyimpanan;*
2. *dalam hal penyidik harus mengakses data pada komputer atau media penyimpanan yang akan menjadi bukti, penyidik yang melakukan harus dapat memberikan penjelasan yang relevan atas tindakan yang dilakukan dan implikasi dari tindakannya tersebut.*
3. *Penyidik harus membuat catatan atas segala tindakan yang dilakukan terhadap bukti digital.*
4. *Apabila pihak lain yang independen mau menguji alat bukti digital maka harus menggunakan metode yang sama yang disepakati sehingga menghasilkan hasil yang sama juga.*
5. *Penyidik bertanggung jawab penuh atas dipenuhinya aturan hukum dan prinsip penanganan bukti digital.*

65. **Bagaimana pembagian *digital evidence*?**

Menurut Shinder (2002) digital evidence dapat diklarifikasikan menjadi:

- *bukti digital asli (original digital evidence) yaitu barang secara fisik dan objek data yang berkaitan dengan barang-barang tersebut pada saat bukti disita;dan*
- *bukti digital duplikat (duplicate digital evidence), yaitu reproduksi digital yang akurat dari seluru objek data yang tersimpan didalam benda mati yang asli.*

66. **Darimana saja alat bukti digital itu dapat ditemukan atau diambil?**

Alat bukti digital dapat ditemukan atau diambil dari media penyimpanan informasi tersebut, seperti:

0. *perangkat keras (hardware) misalnya dari CPU, yaitu hard drives dan volatile memory;*
1. *media yang bisa dilepas, misalnya floppy diskettes, SC/VCD, data tapes, zipdisks,atau memory cards.*
2. *Personal digital assistants (PDA);*
3. *Kamera digital;*
4. *Perekam video;*
5. *MP3 PLayer;*
6. *Printer;*
7. *Log0log penggunaan, seperti ID jaringan.*

67. **Tahap-tahap apa saja yang harus dilakukan penyidik dalam melakukan forensik komputer?**

Tahap-tahap dalam menyajikan forensik komputer adalah:

0. *pengumpulan (collection);*
1. *penyimpanan (preservation);*
2. *penyaringan (filtering);dan*
3. *pernapasan (presentation).*

68. **Pengumpulan *digital evidence* harus dilakukan oleh aparat penegak hukum, khususnya kepolosian yang mengerti TIK. Sayangnya belum semua kepolisian di Indonesia yang mengerti hal ini. Langkah-langkah apa yang dilakukan oleh aparat penegak hukum menyikapi permasalahan tersebut?**

Sangat tepat dikatakan bahwa pengumpulan digital evidence harus dilakukan oleh aparat penegak hukum yang mengerti TIK. Oleh karena itu aparat penegak hukum harus meningkatakan kemampuan personil dan finansial.

Finansial sangat dibutuhkan untuk memingkatakan kemampuan personil dan membeli baik hardware dan software yang digunakan untu pengumpulan digital evidence. Sedangkan kemampuan personil sangat dibutuhkan dalam menggunakan software dan hardware tersebut.

Sosialisasi UU ITE dan peraturan pelaksanaanya adalah strategi lain yang harus dilakukan. Sosisalisasi ini diharapakan dapat menyamakan penafsiran dan persepsi aparat penegak hukum.

69. **Dimanakah *locus delicti* suatu tindak pidana teknologi informasi?**

Locus delicti maksudnya tempat kejadian perkara suatu tindakan pidana. UU ITE tidak menentukan secara khusus mengenai penentuan locus delicti tindak pidana tersebut karena prinsip-prinsip hukum yang berlaku dalam hukum acara.

70. **Kendala-kendala apa yang dihadapai aparat penegak hukum dalam menegakkan UU ITE?**

Beberapa kendala yang dihadapi oleh aparat penegak hukum penegakan UU ITE:

a. belum adanya single identity number indonesia;
b. banyak korban yang tidak melapor;
c. masih terbatasnya infrastruktur serta alat dan perangkat di bidang Teknologi Informasi yang dibutuhkan.

71. **Apa yang dimaksud dengan perluasan alat bukti dalam Pasal 5 UU ITE**

Dalam hukum acara pidana, Informasi dan/atau Dokumen elektronik dan/atau hasil cetaknya merupakan perluasan alat bukti lain selain yang telah diatur dalam Pasal 184 KUHAP. Hal ini juga ditegaskan dalam Pasal 44 huruf b UU ITE. Dengan kata lain, maksudnya adalah upaya untuk menghadirkan bukti Informasi Elektronik dalam memenuhi kategorisasi sebagai alat bukti yang dikenal dalam Pasal 184 KUHAP.

72. **Apakah hasil dari Imaging file bisa menjadi alat bukti dalam pengadilan?**

Informasi Elektronik adalah suatu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, elektronic 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 (Pasal 1 butir 1)
Imaging adalah proses penyalinan satu informasi tanpa ada perubahan meta data. Sesuai dalam UU ITE Bab III Pasal 5, Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Dalam UU ITE juga disebutkan bahwa 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. Tentunya suatu informasi dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE.

73. **Apakah alat bukti elektronik yang diatur dalam UU ITE berlaku hanya untuk tindak pidana yang diatur dalam ITE atau semua tindak pidana?**

Ketentuan mengenai alat bukti elektronik yang diatur dalam UU ITE berlaku terhadap semua tindak pidana:

0. *Tindak pidana yang diatur dalam UU ITE; dan*
1. *Tindak pidana selain yang diatur dalam UU ITE, termasuk tindak pidana konvensional.*

74. **Dalam KUHAP ada pembedaan antara barang bukti dengan alat bukti. Apakah informasi Elektronik dan/atau Dokumen Elektronik dapat menjadi barang bukti?**

Berdasarkan Pasal 39 KUHAP, yang dimaksud dengan barang bukti adalah:
a. benda yang seluruh atau sebagian diduga diperoleh dari tindak pidana atau sebagai hasil dari tindak pidana;
b. benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk persiapannya;
c. benda yang dipergunakan untuk menghalang-halangi penyelidikan tindak pidana;
d. benda yang harus dibuat atau diperuntukkan melakukan tindak pidana;
e. benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan;

Hakim akan menentukan apakah suatu Informasi atau dokumen elektronik tersebut adalah barang bukti atau alat bukti.
Menurut Pasal 5 ayat(1), (2) dan (3) UU ITE, informasi Elektronik dan/atau dokumen elektronik dapat menjadi alat bukti hukum yang sah, maka informasi elektronik dan atau dokumen elektronik sejauh memenuhi kriteria Pasal 39 KUHAP adalah barang bukti.

75. **Mengapa Pasal 43 ayat(6) UU ITE mengharuskan penyidik untuk meminta penetapan dari Pengadilan Negeri ("PN") setempat melalui Penuntut Umum? Hal tersebut tidak efektif dan dapat membuat aparat penegak hukum kesulitan dalam mengumpulkan alat bukti>**

Adanya keharusan bagi penyidik untuk meminta surat penetapan PN melalui penuntut umum dimaksudkan untuk:

0. melakukan koordiansi sejak awal antara aparat penegak hukum (penyidik, penuntut umum, dan hakim) dalam rangkaian proses penegakan hukum dan;

1. memastikan bahwa penangkapan dan penahanan tersebut adalah tindakan yang dibuthkan;
2. mengikat tindak pidana di bidang ITE termasuk kategori kejahatan yang lunak (soft crimes) dan lebih menekankan kepada konten informasi dan/atau dokumen elektronik daripada perbuatannya seperti pada kejahatan biasa (street crimes)

Selain itu,ketentuan ini telah sesuai dengan prinsip dalam Convention on CVybercrime.

76. **Jika dalam melakukan penahanan dan penangkapan, penyidik harus meminta penetapan dari PN Melalui penuntut umum, siapakah yang bertanggung jawab atas penangkapan dan penahanan tersebut?**

Sesuai dengan prinsip KUHAP, pihak yang bertanggung jawab adalah pihak yang melakukan penahanan, walaupun harus ada penatapan dari PN.

77. **Prinsip-prinsip apa yang terkandung dalam UU ITE yang harus dilaksanakan oleh aparat penegak hukum dalam mengumpulkan alat bukti elektronik?**

Pasal 43 ayat(2) UU ITE menentukan bahwa dalam penyidikan termasuk pengumpulan alat bukti elektronik, penyidik harus memperhatikan perlindungan terhadap:
- *privasi;*
- *kerahasiaan;*
- *kelancaran layanan publik;*
- *integritas data atau keutuhan data;*

Dengan demikian, dalam mengumpulkan alat bukti elektronik tersebut:

4. *tindakan penyidik untuk mengamankan dan megumpulkan alat bukti elektronik tidak boleh menggunakan integritas alat bukti tersebut;*
5. *penyidik yang melakukan pengamanan dan pengumpulan alat bukti serta penganalisaan terhadap alat bukti elektronik tersebut adalah orang yang ahli dibidangnya;*
6. *tindakan atau aktivitas yang berkaitan dengan pengamanan, pengumpulan.*

78. **Ada banyak istilah dalam cybercrime, misalnya (i) spamming, (ii) phissing, (iii) hacking. Apa maksudnya?**

Yang dimaksud dengan:

0. *spamming adalah pengiriman email promosi tanpa persetujuan pemilik email, termasuk pengiriman email borongan (bulk email) atau email sampah (junk mail);*
1. *phissing yaitu salah satu bentuk penipuan dengan menggunakan media elektronik untuk mendapatkan informasi sensitif, seperti password dan informasi kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi.*
2. *hacking adalah kegiatan menyusup atau memasuki satu Sistem Elektronik tanpa hak, yang biasanya bertujuan untuk menyalahgunakan ataupun merusak sistem tersebut;*

79. **Bagaimana cara pemerintah Indonesia melakukan *block* terhadap konten-konten yang dilarang berdasarkan UU ITE dan juga UU lain yang terkait?**

Pada dasarnya, sebelum melakukan blocking, Pemerintah menggali partisipasi publik terlebih dahulu dengan melakukan take-down notice terlebih dahulu, baru kemudian menempuh upaya bersama melakukan blocking terhadap penyebaran konten ilegal

Pemerintah melihat pentingnya empat strategi yang harus dilakukan secara simultan.

0. *pelaksanaan self cencoring terhadap konten-konten yang dilarang. Setiap orang dapat melakukan ini: dengan tidak mengunjungi situs-situs tersebut atau memilah-milih Informasi yang diterima. Diharapkan juga orang tua menggunakan parental control untuk membatasi atau menjaga anak-anaknya mengunjungi situs-situs yang memuat konten-konten yang dilarang.*
1. *technical approach. Strategi ini dilakukan dengan cara melakukan blocking terhadap IP address atau konten yang dilarang.*
2. *kerja sama. Para pemangku kepentingan (staka holders) bekerja sama dengan pemerintah untuk mengurangi masuknya konten-konten yang dilarang. sosialisasi atau advokasi mengenai bahaya pornografi merupakan beberapa cara yang dapat dilalksanakan bersama-sama*

3. *peran serta masyarakat juga sangat dibutuhkan dalam menghadirkan konten-konten yang positif. Dengan semakin banyaknya konten positif tersebut maka pilihan bagi masyarakat akan semakin banyak.*

   Law enforcement. Penegakan hukum ini dilakukan dengan memberikan sanksi terhadap pihak yang melanggar peraturan perundang-undangan tersebut. Tentunya tindakan ini, khususnya sanksi pidana, merupakan tindakan terakhir.

80. **Apa dasar keberadaaan aturan pasal tentang penghinaan dan/atau pencemaran nama baik sebagaimana tercantum dalam Pasal 27 ayat(3) UU ITE?**

Pengaturan Pasal 27 ayat(3) UU ITE didasarkan pada: (i) karakteristik internet, dan (ii) kebutuhan perlindungan hak asasi warga negara Indonesia.
Pertama karakteristik internet. Anonymity atau pseudonimity adalah salah satu karakteristik dari internet. Maksudnya adalah setiap orang dapat menggunakan nama lain selain nama diri yang sebenarnya. Oleh karena itu, sangat besar kemungkinan subyek hukum yang melakukan transaksi dan/atau iteraksi yang dilakukan dalam dunia maya sulit untuk diketahui. Dengan kata lain, setiap orang dapat menyalahgunakan kebebasan yang diperolehnya secara sistematis sebagai konsekuensi pola komunikasi di internet yang tidak dapat mewajibkan setiap orang mencantumkan identitas dirinya secara benar.

Dengan demikian, perbuatan penghinaan dan/atau pencemaran nama baik melalui Sistem Elektronik (internet) dapat dengan mudah dilakukan, sementara pelakunya sangat sulit untuk diketahui dan ditelusuri. Jika seseorang melakukan penelusuran sendiri terhadap hal tersebut maka ia telah melanggar hukum karena bertentangan dengan perlindungan privasi.

Karakteristik lainnya adalah internet bersifat obiquitous dimana penyampaian informasi dapat dilakukan secara instan ('seketika'), borderless (tidak terbatas ruang dan waktu), multiplicative (berlipat ganda), dan tersimpan permanen, sehingga internet dapat menjadi sarana penyebaran informasi yang menimbulkan dampak yang sangat luas dan tidak terbatas. Hal ini tentunya sangat merugikan bagi setiap orang yang dihina atau yang nama baiknya dicemarkan. Untuk menelusuri, mengungkapkan, atau mencari siapa pelakunya hanya merupakan kewenangan dan tanggung jawab aparat penyidik. Dalam hal ini proses penelusuran untuk menemukan siapa pelaku tersebut juga memerlukan keahlian dan kemampuan tertentu, khususnya keahlian dan kemampuan dalam hal perolehan dan penanganan bukti digital (digital evidence).

Kedua, berdasarkan amanat UUD NRI 1945, Pasal 28 G ayat(1) UUD NRI 1945 telah di tegas dinyatakan bahwa "setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Oleh karena itu, pengaturan Pasal 27 ayat(3) UU ITE mutlak dibutuhkan.

Dengan demikian, berdasarkan karakteristik internet dan amanat Pasal 28 G ayat(1) UUD NRI 1945 tersebut diatas, maka Pasal 27 ayat(3) UU ITE mutlak diperlukan untuk melindungi semua orang dari penyalahgunaan hak kebebasan orang lain yang dilakukan melalui Sistem Elektronik (internet).

81. **Apakah pengaturan Pasal 27 ayat (3) UU ITE sesusai dengan UUD NRI 1945?**

Konstitusionalitas Pasal 27 ayat(3) UU ITE telah di uji oleh Mahkamah Konstitusi dan Mahkamah Konstitusi telah memutuskan, berdasarkan Putusan MK Nomor 50/PUU-VII/2008 dan Putusan MK Nomor 2/PUU-VII/2009 tertanggal 5 Mei 2009, bahwa Pasal 27 ayat (3) UU ITE adalah konstitusional, dan juga telah sesuia dengan Universal Declaration of Human Right serta tidak bertentangan dengan nilai-nilai demokrasi, hak asasi manusia, dan prinsip-prinsip negara hukum.

Beberapa dasar pertimbangan dari Mahkamah Konstitusi mengenai konstitusionalitas Pasal 27 ayat (3) UU ITE, antara lain :

0. *Bahwa penghargaan terhadap harkat dan martabat kemanusiaan tidak boleh tercederai oleh tindakan-tindakan yang mengusik nilai-nilai kemanusiaan melalui tindakan penghinaan dan/atau pencemaran nama baik.*

1. *Bahwa masyarakat internasional juga menjunjung tinggi nilai-nilai yang memberikan jaminan dan perlindungan kehormatan atas diri pribadi, seperti dalam pasal 12 Universal Declaration of Human Right (UDHR), Pasal 17 dan Pasal 19 International Covenant on Civil and Political Right(ICCPR).*
   Pasal 12 Universal Declaration of Human Right (UDHR) mengatur : "Tidak seorang pun dapat di ganggu dengan sewenang-wenang urusan pribadinya, keluarganya, rumah tangganya atau hubungan surat-menyurat, juga tidak diperkenankan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapatkan perlindungan hukum terhadap gangguan atau pelangaran separti itu".

   Pasal 17 International Covenant on Civil and Political Right (ICCPR) :

   1. *"Tidak ada seorang pun yang boleh dicampuri secara sewenang-wenang atau secara tidak sah masalh pribadinya, keluarganya, atau hubungan surat menyurat, demikian pula secara tidak sah diserang kehormatan atau nama baiknya."*
   2. *"Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan demikian".*

Pasal 19 International Covenant on Civil and Political Right (ICCPR) :

3. *"Setiap orang berhak untuk mempunyai pendapat tanpa diganggu";*
4. *"setiap orang berhak atas kebebasan untuk menyatakan pendapat; hak ini termasuk kebebasan untuk mencari, menerima dan memberi informasi dan ide apapun, tanpa memperhatikan medianya, baik secara lisan, tertulis atau dalam bentuk cetakan, dalam bentuk seni, atau melalui media lainnya sesuai dengan pilihannya".*
5. *Pelaksanaan hak yang diatur dalam ayat 2 Pasal ini menimbulkan kewajiban dan tanggung jawab khusus. Oleh karena itu hak tersebut dapat dikenai pembatasan tertentu, namun pembatasan tersebut hanya diperbolehkan apabila diatur menurut untuk :*

   a. Menghormati hak atau nama baik orang lain.
   b. Melindungi keamanan nasional atau ketertiban umum atau kesehatan atu moral masyarakat.

2. *Berdasarkan putusan Nomor 14/PUU-VI/2008 Mahkamah Konstitusi telah berpendirian bahwa nama baik, martabat, atau kehoramatan seseorang adalah salah satu kepentingan hukum yang dilindungi oleh hukum pidana karena merupakan bagian dari hak konstitusional setiap orang yang dijamin baik oleh UUD 1945 maupun hukum internasional. Dengan demikian, apabila hukum pidana memberikan sanksi pidana tertentu terhadap perbuatan yang menyerang nama baik, martabat, atau kehoramatan seseorang, hal itu tidaklah bertentangan dengan konstitusi.*

3. *Bahwa rumusan KUHP dinilai belum cukup karena unsur "di muka umum" sebagaimana diatur dalam Pasal 310 KUHP kurang memadai sehingga perlu rumusan khusus yang bersifat ekstensif yaiti "mendistribusikan, mentransmisikan dan/atau membuat dapat diakses". Rumusan Pasal 27 ayat(3) UU ITE telah memberikan perlindungan dengan mengatur unsur "dengan sengaja" dan "tanpa hak".*

4. *Bahwa unsur dengan sengaja dan tanpa hak merupakan satu kesatuan yang dalam tataran penerapan hukum harus dapat dibuktikan oleh penegak hukum. Unsur "dengan sengaja " dan "tanpa hak" berarti pelaku "menghendaki" dan "mengetahui" secara sadar bahwa tindakannya dilakukan tanpa hak. Dengan kata lain, pelaku sadar menghendaki dan mengetahui bahwa perbuatan "mendistribusikan" dan/atau "mentranmisikan" dan/atau "membuat dapat*

diaksesnya Informasi Elektronik dan/atau Dolumaen Elektronik" adalah memiliki muatan penghinaan dan/ atau nama baik. Adapun unsur "tanpa hak" meruapakan unsur melawan hukum. Pencantuman uunsur tanpa hak di maksudkan untuk mencegah orang melakukan perbuatan mendistribusikan dan/atau mentransmisikan dan/atau mambuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memilikim muatan penghinaan dan/atau pencemaran nama baik.

5. *Bahwa penafsiran norma yangmuatan dalam Pasl 27 ayat(3) UU ITE mengenai penghinaan nama baik, tidak bisa dilepaskan dari norma hukum pidana yang termuat dalam Bab XVI tentang Penghinaan yang termuat dalam Pasal 310 dan Pasal 311 KUHP, sehingga konstitusionalitas Pasl 27 ayat(3) UU ITE harus dikaitkan dengan Pasal 310 dan PAsal 311 KUHP.*

6. *Meskipun setiap orang mempunyai hak untuk berkomunikasi dan memperoleh informasi, tetapi ketentuan konstitusi (Pasal 28 G UUD 1945 dan Pasal 28 J UUD 1945) menegaskan dan menjamin bahwa bahwa dalam menjalankan kebebasan berkominikasi dan memperoleh informasi tidak boleh melanggar hak-hak orang lain untuk mendapatkan perlindungan diri pribadi, keluarga, kehormatan ,martabat, dan nam baiknya.*
7. *Penghinaan yang di atur dalam KUHP (penghinaan off line) tidak dapat menjangkau delik penghinaan dan pencemaran nama baik yang di lakukan di dunia siber (penghinaan on line) karena ada unsur "di muka umum".*

82. **Apakah pengaturan Pasal (3) UU ITE mengancam kebebasan pers atau kebebasan berekspresi, termasuk menyampaikan keluhan dari seorang konsumen?**

Menurut doktrin ada dua jenis penghinaan, yaitu: (i)penghinaan formil(formele belediging) dan (ii)penghinaaan mateil(mateliel belediging); penghinaan formil adalah pernyataan yang konten dan esensinya jelas dan tegas merupakan penghinaan karena, antara lain, menggunakan bahasa yang kasar dan tidak sopan. Sedangkan penghinaan materil adalah pernyataan yang konten esensinya adalah bentuk penghinaan yang di lakukan secara halus. Konten dan esensinya dari pernyataan tersebut harus dinlai secara keseluruhan baik dari segi bahasa amupaun dari segi hukum pidana serta pandangan objektif kebanyak orang. Dengan kata lain, suatu pernyataan tidak dapat dilihat secara garamatiakl yang parsial.

Yang dapat di pidana adalah penghinaan formil. penghinaan materil tidak daapt dipidana karena hal tersebut ,merupakan bentuk wujud dari kebeebasan berpendapat yang harus dilindungi. Dalm kasus Prita tidak ada penghinaan formil.

Ketentuan pasal 27 ayat (3) UU ITE sama sekali

tidak mengancam kebebasan pers atau kebebasan berekspresi karena kebaebasan pers dan kebebasan berekspresi tentunya tidak di tujukan untuk melakukan penghinaan atau pencemaran nama baik. Kebebasan berekspresi , dan tindakan penghinaan adalah dua hal yang secara normatif berbeda (tidak dapat dicampur baurkan).

Terkait dengan kebebasan pers, sesuai dengan Peraturan Dewan Pers Nomor: 6/Peratuaran DP/V/2008 tentang Pengesahan Surat Keputusan Dewan Pers Nomor 03/SK-DP/III/2006 tentang Kode Etik Jurnalistik sebagai Peraturan Dewan Pers (kode jurnalistik-KEJ) Pasal 1 dan Pasal 4 KEJ perlu diperhatikan dalam mengekspresikan kebebasan pers.

Pasal 1 KEJ menyatakan bahwa wartawan Indonesia bersikap independen, menghasilkan berita akurat, berimbang, dan tidak beritikad buruk. Sedangkan PAsal 4 KEJ mengatur wartawan Indonesia tidak membuat beriat bohong, fitnah, sadis, dan cabul.

Kemudian, Psal 27 ayat (3) UU ITE juga memuat unsur "dengan sengaja" dan unsur "tanap hak". Unsur dengan sengaja memiliki makna "tahu dan menghendaki" dilakukannya tindak pidana.

Unsur "tanpa hak"akan menentukan dapat atau tidaknya seseorang dituntut berdasarkan ketentuan Pasal 27 ayat(3) UU ITE. Dengan demikian, sepanjang seseorang mengekspresikan pendapatnya sesuai denagn peratuar perundang-undangan yang berlaku, termasuk Jurnalis yanng melakukan tugas jurnalistiiknya sesuai dengan kode etiknya, maka jelas Jurnal tidak terkena Pasal 27 ayt(3) UU ITE, Hal ini juga termasuk konsumen yang memiliki hak untuk didengar pendapat dan keluhan atas barang dan/atau jasa yang digunakan (Pasal 4 huruf d UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.)

Unsur "tanpa hak " dalam ketntuan Pasal 27 ayat(3) UU ITE merupakan perumusan uunsur sifat melawan hukum (wederrchtelijk-sebagai unsur konstitutif dari sustu tindak pidana-yng lebih spesifik.)

Perumusan unsur melawan hukum dalam hal ini unsur "tanpa hak" di maksudkan untuk menghindarkan orang yang memiliki hak menjadi dapat dipidana.

Lebih lanjut, aparat penegak hukum juga bisa bertindak sewenang-wenang karena selain telah di atur unsur "tanpa hak" sebagai perlindungan terhadap orang yang berhak, pada dasarnya UU ITE jugatelah memberikan perlindungan lain dengan meminimalisir abuse of power dalam melakukan penangkapan dan penahan, sebagaimana termuat dalam Pasal 43 ayat (6) UU ITE yang berbunyi :

"Dalam hal melakukan penangkapan dan penahan, penyidik melalui penuntut umum ***wajib*** *meminta penentapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam ."*

Dari pasal ini dapat disimpulkan bahwa tiga insittu penegak hukum " (i)kepolisian, (ii)kejaksaan,dan (iii) pengadilan wajib melakukan koordinasi mengenai perlunya atau dasr dilakukan nya penahan. Adanya koordinasi ini di tunjukan untuk mencegah

abuse of power oleh aparat penegak hukum.

Oleh karena itu,pengaturan Pasal 27 ayat(3) UU ITE tidak bertujuan dan tidak menghabat kebebasan pers atau kebebasan berekspresi. Akan tetapi sepatutnyalah pihak yang memiliki hak tersebut tidak menggunakan haknya dengan semena-mena. Mengemukakan pendapat atau menyatakan ekspresi haruslah sesuai dengann etika dan peraturan perundang-undangan.

Unsur "tanpa hak" dalam Pasal 27 ayat (3) UU ITE adalah unsur yang sangat penting. Pers,sebagaimana dengan profesi dokter atau advokat dapat kebal hukum (memiliki hak) apabila memegang teguh: (i)taat pada kode etik, (ii)taat pada SOP (dengan kata lain harus ada SOP), dan (iii)semata-mata untuk menjalankan profesi dengan itikad baik. Jika ada salah satu dari ketiga hal tersebut dilanggar, pintu hukum akan terbuka. Oleh karena itu,baik wartawan maupun para blogger harus memiliki SOP.

83. **Mengapa perbuatan penghinaan dan pencemaran nama baik diselesaikan dengan pidana?**

Disatu sisi, perbuatan penghinaan atau pencemaran nama baik melalui Sistem Elektronik (Internet) dapat dengan mudah dilakukan, sementara pelakunya sangat sulit untuk diketajui dan ditelusuri. Disisi alin, pihak yang terhina atau yang namanya tercemar sulit untuk membuktikan bahwa si pelaku lah yang melakukannya karena terhalang dengan ketentuan privasi yang diatur dalam UU ITE, dan mungkin terhambat dengan teknologi yang dimilikinya. oleh karena itu, hanya aparat penegak hukum lah, dalam hal ini kepolisian, yang memiliki tanggung jawab dan kewenangan dan menulusuri atau mengungkapkan siapa pelaku yang harus bertanggung jawab.

Meskipun demikian, sesuai dengan ketentuan KUHP bahwa penghinaan dan/ atau pencemaran nama baik adalah termasuk delik aduan, maka rindak pidana yang diatur dalam Pasal 27 ayat (3) juga memerlukan panduan. Sifat paduan tersebut tetap melekat. Hal ini ditegaskan dalam Putusan MK No. 50/PUU-VI/2008. Ketentuan ini memberi ruang bagi pihak yang dirugikan (Korban) untuk menyelesaikan perdamaian diluar pengadilan atua menempuh melalui proses perdata. Setelah tindak pidana tersebut diproses dan mendapatkan putusan berkekuatan hkum tetap (in kracth), korban dapat mengajukan gugatan perbuatan melawan hukum berdasarkan pasal 1365 KUHP perdata dengan dasar putusan pidana tersebut.

84. **Mengapa sanksi terhadap penghinaan dan/atau pencemaran nama baik dalam pasal 27 ayat (3) UU ITE sangat berat? (pidana penjara maksimal 6 tahun dan/ atau denda maksimal 1 miliar rupiah?)**

Beratnya sanksi pidana trehadap palenggaran Pasal 27 ayat (3) UU ITE sebagaimana diatur dalam Pasal 45 ayat (1) UU ITE dilihat dari karakteristik internet di atas (annonimity, bordeerless, masive effect). Kemudian, perumusan sanksi pidana yang di atur dalam Pasal 45 ayat (1) UU ITE hanya memberikan batas amksiaml : "...sebanyak-banyaknya..." dan bukan perumusan "...paling singkat...dan paling lama..." seperti perumusan dalm UNdang-Undang Pemberatasan Tindak Pidana Korupsi. berat ringannya pidana yang akan dijatuhkan Hakim tergantung pada kesalahn si terdakwa. Sebagai perbandingan berikut ini beberapa perumusan ancaman meksimal pidana trehadap tindak pidana penyebaran informasi yang bersifat melawan hukum.

*Undang-Undang Nimir 19 Tahun 2002 tentang Hak Cipta dimuat dalam Pasal 17 yaitu **Pengumuman setiap Ciptaan** yang bertentangan dengan kebijaksanaan Pemerintah di bidang **Agama**pertahanan dan keamanan Negara, **kesusilaan,** serta**ketertiban umum**, ancaman pidana maksimal 5 atahun dan / atau denda maksiaml 1 miliyar.*

Undang-Undang Nomor 32 tahun 2002 tentang Penyiaran, dimuat dalam Pasal 57jo. Pasal 36 ayat(5) dan ayat (6) yaitu dilakukan dengan cara menyiarkan :

- *Melalui radio : pidana penjara 5 tahun dan /atau denada 1 miliyar;*
- *Melalui televisi : pidana penjara 5 tahun dan / atau denda 10 milyar.*

85. **Apa yang dimaksud dengan "muatan penghinaan dan/atau pencemaran nama baik" dalam pasal 27 ayat (3) UU ITE?** *"Muatan penghinaan dan/atau pencemaran anma baik" amksudnya memuat penghinaan dan/atau pencemaran nama baik. Oleh karena itu, Pasal 27 ayat (3) UU ITE harus mengacu pada bab XVI tentang PEnghinaan Psal 310 KUHP yang intinya adalah menyerang kehormatan orang lain.*

86. **Apa yang dimaksud dengan mendistribusikan, mentransmisikan atau membuat dapat diakses dalam Pasal 27 ayat (3) UU ITE?**

Yang diamksud dengan mendistribusikanadalah perbuatan menyebarkan secara luas Informasi dan/atau Dokumen Elektronik melalui medi elektronik(misalnya dilakukan melalui web atau mailing list) yang ditujukan dengan sengaja untuk menghina dan/atau mencemarkan nama baik.

Yang dimaksud dengan mentranmisikan adalah kegiatan mengirimkan, memancarkan atau meneruskan informasi melalui media elektronik dan/atau perangkat telekomunikasi yang bertujukan dengan sengaja untuk menghina dan/atau mencemarkan nama baik.

Yang dimaksud dengan membuat dapat diaksesnya adalah kegiatan untuk membuat agar informasi dan/atau Dokumen Elektronik dapat diakses oleh orang alin. misalnya dengan menyediakan link pada satu website yang ditujukan dengan sengaja untuk menghina dan/atau mencemarkan nama baik.

87. **Apakah yang dimaksud dengan muatan perjudian sebagaimana diatur dalam Pasal 27 ayat (2) UU ITE?**

Muatan Perjudian diatur dalm Pasal 303 ayat (3) KUHP yaitu : Tiap-tiap permainan, yang mendasarkan pengharapan buat menang pada umumnya bergantung kepada untung-untungan saja, dan juga kalau pengharapan itu jadi bertambah besar karena kepintaran dan kebiasan pemain. Yang juaga terhitung masuk main judi adalah pertaruhan tentang keputusan perlombaan atua permainan lain, yang tidak diadakan oleh mereka yang turut berlomba atau bermain itu, demikianjuga segala pertaruhan yang lain-lain. Oleh karena itu, yang dilarang adalah dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan membuat dapt diaksesnya muatan perjudian.

Apabila seorang pemain agar dapat memasuki suatu website judi ia perlu terlrbih dahulu memiliki password dahulu (KOde akses). Maka pihak yang mengelolah situs judi dengan memberikan passwod tersebut dapat dikategorikan sebagai membuat dapat diaksesnya.

Menurut UU ITE, Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan. Kedua tersangka telah memberikan Kode Akses, yaitu angka, huruf, simbol, karakter lainya, atau kombinasi diantaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainya.

88. **Apakah ketentuan pidana dalam UU ITE dapat langsung dilaksanakan?**

Berdasarkan Pasal 54 ayat (1) UU ITE, UU ITE mulai berlaku pada tanggal diundangkan, yaitu 21 April 2008. Hal ini sesuai dengan Pasal 50 UU Nomor 10 Tahun 2004 tentang pembentukan Peraturan PErundang-undangan bahwa peraturan perundang-undangan muali berlaku dam mempunyai kekuatan mengikat pada tanggal diundangakan, kecuali ditentukan lain dalam peraturan perundang-undangan yang bersangkutan. Oleh akrena itu, ketentuan pidana dalam UU ITE sudah langsung dapat dijalankan tanpa perlu menunggu Peraturan Pemerintah. Akan tetapi, jika Pasal-psal yang dirujuk oleh Pasal 45 samapi Pasal 51 tersebut memerlukan pengaturan lebih lanjut ke dalam Peraturan Pemerintah, maka Pasal-pasal tersebut menunggu adanya Peraturan Pemerinta, tidak harus emnunggu selama 2 tahun,

melainkan sejak diterbitkannya Peraturan Pemerintah. sebaliknya, jika pasal-pasal yang di rujuk Pasal 45 sampai Pasal 51 tersebut tidak memerlukan pengaturan dalam abentuk Pengaturan Pemerintah,maka tindak pidana dalam UU ITE tersebut dapat langsung dilaksanakan.

89. **Apakah amsyarakat dapat mengajuakn class action berkaitan dengan promosi palsu, undian palsu yang dilakukan oleh provider?**

Sesuai dengan Pasal 28 ayat (1) UU ITE jo Pasal, setiap orang denagn sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik dipidana dengan pidana penjara maksiamal 6 tahun dan/atau denda maksimal satu milyar. Apabila provider ternyata memberikan kabar abohong dan menyesatkan sehingga para konsumen dirugikan maka masyarakat dapa mengajukan class action.

Class action sendiri telah diakui dalam sistem hukum indonesia. Secara sederhana class action dapat dijelaskan sebagai tindakan hukum berupa gugatan yang diajuakam oleh perwakilan dari satu masyarakat. Ketentuan mengenai class actino terdapat dalam Peraturan MA Nomor 1 tahun 2002 tentang Acara Gugatan Perwakilan Kelompok.

90. **Apa yang dimaksud dengan kerugian pada Pasal 23 ayat (3) UU ITE mengenai Nama Domain?**

Pasal 23 ayat (3) UU ITE :
"Setiap penyelenggara negara, Orang, Badan Usaha, atau masyarakat uyang dirugikan karena pengguna Nama Domain secara tanpa hak oleh Orang lain, berhak mengajukan gugatan pembatalan Nama Domain yang di maksud."
Pasal ini terkait dengan masalah perdata. Kerugian yang dimaksud adalah kerugian baik materil maupun imateril. Pihak yang merasa di rugikan dapat mengajukan gugatan.

91. **Nama Domain akan diliberalisasi. Bagaimana pelaku usaha menyikapi hal ini?**

ICANN kan meliberalisasi domain name systems (DNS) pada kuartal pertama ditahun 2010. Liberalisasi ini akan menimbulkan dampak yang besar bagipemilik brand. Mereka harus melindungi brand mereka di gTLD yang baru dan hal tersebut memerlukan strategi.

Hal yang perlu dipertanyakan adalah apakah membuat brandTLD (dotBrand) adalah hal yang teat ? Penamaan brandTLD akan memberikan segi positif, antara lain posisi yang penting bagi pemilik brand, meningkatkan visibilitas dari brand didunia internet

karena tidak tergantung lagi kepada pemilik TLD. Pemilik TLD dengan demikian dapat membentuk kebijakan untuk mengkontrol dan memonitor TLD.Akan tetapi, brandTLD juga akan menimbulkan dampak dari segi teknis, merketing, operasional,dan finansial.

Selain itu tantangan yang muncul dalam mengaplikasi dotBrad adalah proses aplikasi membutuhkan waktu yang lama dan mendetail. Selain itu, menjalankan posisi sebagai tentunya bukan core business pemilik brand. Mereka juga perlu mengeluarkan usahayang besar dalam bidang merketing untuk memaksimalkan keuntungan.

Secara singkat, pemilik brand yang ingin mengaplikasikan dotBrand perlu mengambillangkah-langkah ini: (i) melakukan feasibility study, (ii) membuat proposal ke ICANN, (iii) mengimplementasikan gTLD baru, (iv) mengeluarkan gLTD baru, dan (v) mengelola gTLD terseut.

92. **Bagaimana Pelaku Usaha dapat melindungi HAKI mereka, khususnya Nama Doamin?**

Perusahaan dapat melindungi HAKI mereka di internet, khususnya NamaDomain, dengan dua strategi. Strategi upstream adalah strategi yang diambil oleh perusahaan sebeleum terjadi konflik, misalnya mendaftarkan Nama Domain.Sedangkan strategi doenstream diambil perusahaan ketika terjadi sengketa atau konflik (enforcements Strategi downstream yang dapat diambil oleh pelaku usaha, yaitu:

0. *tindakan bisnis, pelaku usaha dapat membeli Nama Domain yang di persengketakan.*
1. *tindakan hukum, pelaku usaha dapat menyelesaikan melalui UDRP atau pengadilan. Akan tetapi, biaya yang dikeluarkan oleh pelaku usaha untuk menyelesaikan nama doamin melalui pengadilan jauh lebih besar dibandingkan penyelesaian melalui UDRP.*

Terkait sengketa Nama Domain, ICANN telah mengeluarkan Unifor Domain Name Dispute Resolution Policy (UDRP) tahun 1999. Sengketa yang dapat diselesaikan dengan menggunakanUDRP, Misalnya:

2. *Nama Domain terlapor identik atau sangat mirip engan trademark atau service mark pelapor;*
3. *terlapor tidak berhak atau legitimate interests terhadap Nama Domain yang disengketakan;*
4. *adanya itikad buruk dari pihak yang meregistrasi Nama Domain;*

Strategi enforcement/downstream menimbulkan masalah yang lebih besar daripada strategi upstream karena strategi tersebut membutuhkan biaya dan waktu yang cukup besar dan tidak singkat. Oleh karena itu, perusahaan dianjurkan untuk berinvestasi pada downstream.

93. **Karakteristik internet seperti pedang bermata dua. Bagaimana pelaku usaha dapat melindungi brand dari penyalahgunaan karakteristik ini oleh penipu?**

Karakteristik Internet yang dimanfaatkan oleh fraudsters: (i) global reach, (ii) fast time to market, (iii) low cost per transaction, (iv) annomity, (v) easy to copy e-brand image. (vi) policy limited or non existent. Oleh karena itu, karakteristik ini dapat menjadi ancaman.

Beberapa contoh ancaman terkait dengan brand, antara lain:
a. trademark relate abuse, misalnya: (i) traffict diversion dan (ii) negative association.
b.conterfeit product sales, misalnya dalam e-commerce sites, auction listings , dan spam.
c. financial fraud, seperti bintang dan 419 seconds.

Oleh karena itu, pelaku usaha perlu melindungi brand-nya dengan cara: (i) menentukan geografi yang penting, (ii) brand yang penting (bagi pelaku usaha yang memiliki lebi dari satu brand), dan (iii) menggunakan brandTLD. Selain itu, pelaku usaha juga perlu melibatkan unit yang terkait, antara lain: (i)legal, (ii) marketing, (iii) keamanan, (iv) IT, dan (v) finansial. Setelah itu, pelaku usaha dapat menentukan prioritasyang didasarkan pada (i) highest volume per transaction, (ii) most damaging to reputation.

94. **Apakah Indonesia telah memiliki peralatan forensik yang memadai untuk mengungkap tindak pidana siber?**

Aparat Penegak Hukum telah memiliki peralatan yang cukup memadai untuk menangani perkara siber. Mabes POLRI telah memiliki laboratorium forensik siber.

95. **Pada akhir Desember 2007 lalu, tempat usaha Warnet rekan kami dioperasi polisi dan beberapa perangkatnya disita. Sementara, dalam UU ITE, penyitaan dapat dilakukan hanya dengan Imaging data dalam media penyimpanan.**

Apakah UU ITE berlaku surut, sehingga rekan kami bisa mengambil perangkatnya yang disita untuk keperluan usaha saat ini?

UU ITE tidak berlaku surut. Hal ini diatur dalam Pasal 54 UU ITE. Namun perlu diketahui bahwa dengan berlakunya UU ITE, sepanjang tindak pidana tersebut menyangkut keberadaan Sistem Elektronik, maka selayaknya penyitaan yang dilakukan harus mengikuti ketentuan dalam UU ITE

96. **Sebagai pemilik Warnet, apakah kami akan dikenai hukuman atau sanksi jika pengguna internet mengakses situs porno yang memang dilarang sebagaimana dinyatakan dalam Pasal 27 ayat(1) UU ITE?**

Pada dasarnya yang diancam dengan sanksi pidana terhadap pelanggaran Pasal 27 ayat(1) UU ITE adalah Orang yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat dan dapat diaksesnya Informasi dan/atau Dokumen Elektronik yang memiliki muatan kesusilaan. Dalam konteks ini, pihak warnet tidak melakukan akses. Yang melakukan dengan sengaja adalah pengguna internet, maka terhadap pemilik warnet tidak dapat diterapkan Pasal 27 ayat(1) UU ITE.
Sebaiknya pengelola warnet mencegah situs porno diakses oleh konsumen dengan cara memblokir (menutup) situs yang jelas-jelas porno sebagai bentuk tanggung jawab sebagai warga negara dalam melaksanakan undang-undang ITE.

97. **Sebagai pengelola Warnet, kami berusaha untuk berbisnis sesuai dengan aturan. Pertanyaannya, apakah kami akan menerima hkuman atau sanksi jika pengguna Warnet men-download situs-situs porno atau meng-up load informasi atau Dokumen yang di larang berdasarkan UU ITE dan meletakannya dalam server kami atau menyimpan pada hardisk local kami?**

Pada dasarnya yang diancam oleh UU ITE adalah oarang yang dengan sengaja dan tanpa hak melakukan perbuatan yang dilarang dalam UU ITE. Akan tetapi sistem hukum pidan adalam KUHP, tremasuk UU ITE, mengenal adanya konsep perbuatan turut serta yang juga tetap memperhatikan unsur "dengan sengaja" dan "tanpa hak". Oleh karena itu, sepanjang pengelola Warnet telah melakukan pengamanan atau tindakan pencegahan untuk penyalahgunaan tersebut dan segera menghilangkan dari servernya, maka pengelola tidak terkena sanksi pidana.

98. **Dalam Pasal 43 ayat (3) UU ITE dinyatakan bahwa penggeledahan dan/atau penyiatan harus dilakukan atas izin ketua pengadilan negeri setempat. Bagaimana jika penyidak melakukan operasi penggeledahan dan penyitaan tanpa dilengkapi izin yang dimaksud? Apakah kami dapat menolak?**

Penggeledahan dan penyitaan adalah upaya paksa. Terhadap kedua upaya paksa ini harus mengacu kepada UU ITE dan juga KUHP. Pada prinsipnya, upaya paksa adalah tindakan penyidak yang bersifat memaksa orang lain untuk melakukan hal tertentu sehingga pada hakekatnya upaya paksa tersebut melanggar hak asasi manusia. Akan tetapi penyidaik dapat melakukan hal terssebut sepanjang dilakukan berdasarkan peraturan perundang-undangan.

Keharusan izin dari ketua pengadilan setempat adalah dalam rangka check and balances antara aparat penegak hukum dari eksekutif dengan pengadilan dari yustisi. dengan demikian, kemungkinan penyalahgunaan wewenang dapat di cegah. Kentetuan izin dalam UU ITE harus selaras dengan KUHP. Oleh karena itu, selain izin tersebut, penggeledahandan penyitaan Sistem Elektronik harus dilekukan dengan (i)disaksikan oleh minimal dua orang saksi dan (ii) dibuat berita acara penggeledahan dan/atau penyitaan (pasal 34 ayat (1) KUHAP).

Selain itu,Penyidik juga harus memperhatikan Pasal 43 ayat (2) UU ITE yaitu harus dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan public, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.

Dalam KUHAP telah diatur bahwa dalam keadaan tertantu izin yang dimaksud tidak perlu diperoleh sebelum melakukan upaya paksa. Hal ini dimungkinkan dalan hal (i)dalam keadaan yang sangat perlu dan mendesak, (ii)penyidak harus segera bertindak, (iii)tidak mungkin untuk mendapat izin terlebih dahulu (Pasal 34 ayat (2) dan Pasal 38 ayat (2) KUHAP).

Karena UU ITE tidak mengatur adanya pengecualian tersebut, maka berlakulah ketentuan-ketentuan KUHAP yang dimaksud.

Jika penyidak melakukan penggeledahan dan/atau penyitaan tanpa mematuhi ketentuan-ketentuan dia atas maka tiap pihak yang terkena upya paksa dapat menolak dan dapat mengajukan upaya pra pengadilan, jika aparat penyidak tetap memaksa melakukannya. (Pasal 95 jo. Penjelasan Pasal 95 KUHAP).

99. **Dalam pasal-pasal pada Bab VIII UU ITE tentang Perbuatan yang dilarang,digunakan unsur "setiap orang" padahal perbuatan yang dilarang seperti, spam, craking, fraudulent, virus,flooding, atau tindakn merusak lainya akan dilakukan oleh mesin olah progarm, dan bukan dilakkukan langsung oleh manusia. Apakah hal ini merupakan kelemahan UU ITE?**

Pada prinsipnya pihak yang harus bertanggung jawab adalah the men behind the

machine. Yang dilakukan spam, cracking, kacking, fraudulent, flooding atau tindakan merusak lainnya tetaplah manusianya. Jadi ini bukanlah suatu kelemahan.

100. **Mengacu pada pasal 27 s.d. 37 UU ITE yang dapat ditangkap adalah orang yang menyebarkan virus. Akan tetapi, tampaknya pembuat virus tidak dapat ditangkap dengan UU ITE. Apakah kelemahan UU ITE? Dan bagaimana sebaiknya Pemerinath menyikapinya?**

Virus tidak akan merusak sistem komputer atau Sistem Elektronik jika tidak disebarkan malalui Sistem Elektronik. Artinya jika virus itu tersebar, maka penyebarlah yang akan dikenakan sanksi pidana. tentunya hal ini harus dibuktikan di pengadilan, yaitu apakah penyebaran virus melakukannya dengan sengaj dan tanpa hak.

<u>Peran masyarakat dan Pelaku Usaha</u>

101. **Apa saja bentuk peran masyarakat dan juga pelaku usaha yang dimaksud dalam BAB XI UU ITE?**

Masyarakat dan pelaku usaha dapat memberikan peranan yang sangat besar dalam memajukan Teknologi Informasi di Indonesia. Pemanfaatan Teknologi Informasi melalui penggunaan dan penyelenggaraan Sistem Elektronik dan Transaksi Elektronik harus dilakukan secara sinergi, sinergi dalam artian terdapat paeran masyarakat selain peran pemerintah, pihak swata atau bisnis. Peran tersebut dapat dilakukan dengan, misalnya :
a.) Masyarakat dapat membentuk lembaga yang memantau perkembangan Teknologi Informasi Indonesia dan dapat memberikan masukan kepada Pemerinatah.
b.) Para pelaku usaha dapat dan sepatutnya mengedukasi serta memberikan penjelasan mengenai (i) proses Transaksi Elektronik, (ii)penggunaan Sistem Elektronik yang diselenggarakannya, dan (iii)resiko-resiko mungkin terjadi yang diakibatkan oleh keteledoran pengguna Sistem Elektronik.