KULIAH ONLINE HUKUM TELEMATIKA
PERTEMUAN KE-11
TINDAK PIDANA TELEMATIKA
Dosen Koordinator : MEN WIH WIDIATNO

## I. TINDAK PIDANA TELEMATIKA

Cybercrime = computer crime·

Computer crime:

"…any illegal act requiring knowledge of computer technology for its erpetration, investigation, or prosecution"

"any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data"

"Kejahatan di bidang komputer secara umum dapatdiartikan sebagai penggunaan komputer secara illegal". Cybercrime dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

Secara internasional hukum yang terkait kejahatan teknologi informasi digunakan istilah hukum siber atau cyber law. Istilah lain yang juga digunakan adalah hukum teknologi informasi (law of information technology), hukum dunia maya (virtual world law), dan hukum mayantara. Sejalan dengan istilah tersebut Barda Nawawi Arief menyatakan : "tindak pidana mayantara", identik dengan "tindak pidana di ruang siber ("cyber space")" atau yang biasa juga dikenal dengan istilah "cybercrime".

Dewasa ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum cyber atau hukum telematika. Hukum cyber 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.

Cyber Law adalah aspek hukum yang artinya berasal dari Cyberspace Law yang ruang lingkupnya meliputi aspek-aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki dunia cyber atau maya Pemberlakuan cyber law dikarenakan saat ini mulai muncul kejahatan – kejahatan yang ada di dunia maya yang sering di sebut sebagai CyberCrime.

Pengertian Cyberlaw adalah merupakan seperangkat aturan yang dibuat oleh suatu Negara tertentu, dan peraturan yang dibuat itu hanya berlaku kepada masyarakat Negara tertentu. Cyber Law dapat pula diartikan sebagai hukum yang digunakan di dunia cyber (dunia maya), yang umumnya diasosiasikan dengan internet. Pengertian Cybercrime adalah tidak criminal yang dilakkukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Cybercrime merupakan kejahatan yang memanfaatkan perkembangan teknologi computer khusunya internet.

Cybercrime didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi computer yang berbasasis pada kecanggihan perkembangan teknologi internet. Menurut Sutarman (2007) Cyber Crime adalah kejahatan yang dilakukan oleh seseorang maupun kelompok dengan menggunakan sarana computer dan alat komunikasi laiinya.

Cara-cara yang biasa dilakukan dengan merusak data, mencuri data, dan menggunakannya secara illegal.

Hukum yang ada di dunia maya pun berbeda sebutannya, di antaranya adalah CYBERLAW, COMPUTER CRIME LAW & COUNCILE OF EUROPE CONVENTION ON CYBERCRIME. Perbedaannya terdapat pada wilayah hukum itu berjalan. Seperti contoh sebagai berikut :

1. CyberLaw
   Cyberlaw merupakan seperangkat aturan yang dibuat oleh suatu negara tertentu, dan peraturan yang dibuat itu hanya berlaku kepada masyarakat negara tersebut. Jadi,setiap negara mempunyai cyberlaw tersendiri.
2. Computer Crime Act (CCA)
   Merupakan Undang-undang penyalahan penggunaan Information Technology di Malaysia.
3. Council of Europe Convention on Cybercrime
   Merupakan Organisasi yang bertujuan untuk melindungi masyarakat dari kejahatan di dunia Internasional. Organisasi ini dapat memantau semua pelanggaran yang ada di seluruh dunia.

Berdasarkan Sasaran Kejahatan

1. Cybercrime yang menyerang individu
   Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut
   Contoh:
   Pornografi:
   Kegiatan yang dilakukan dengan membuat, memasang,mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas
   Cyberstalking:
   Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya
   Cyber-Tresspass:
   Kegiatan yang dilakukan melanggar area privasi orang lain seperti misalnya Web Hacking. Breaking ke PC, Probing, Port Scanning dan lain sebagainya.
2. Cybercrime menyerang hak milik
   Cybercrime yang dilakukan untuk menggangu atau menyerang hak milik orang lain
   Contoh:
   Pengaksesan komputer secara tidak sah melalui dunia cyber
   Pemilikan informasi elektronik secara tidak sah/pencurian informasi, carding, cybersquating, hijacking, data forgery
   Kegiatan yang bersifat merugikan hak milik orang lain
3. Cybercrime menyerang pemerintah
   Cybercrime Againts Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah.

Contoh: cyber terorism sebagai tindakan yang mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer

## II. CYBERLAW

Perbandingan Cyberlaw di dunia antara lain :

1. Cyber Law Negara Indonesia:

   Munculnya Cyber Law di Indonesia dimulai sebelum tahun 1999. Focus utama pada saat itu adalah pada "payung hukum" yang generic dan sedikit mengenai transaksi elektronik. Cyber Law digunakan untuk mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya, baik transaksi maupun pemanfaatan informasinya. Pada Cyber Law ini juga diatur berbagai macam hukuman bagi kejahatan melalui internet.

   Cyber Law atau Undang-undang Informasi dan Transaksi Elektronik (UU ITE) sendiri baru ada di Indonesia dan telah disahkan oleh DPR pada tanggal 25 Maret 2008. UU ITE terdiri dari 13 bab dan 54 pasal yang mengupas secara mendetail bagaimana aturan hidup di dunia maya dan transaksi yang terjadi di dalamnya. Perbuatan yang dilarang (cybercrime) dijelaskan pada Bab VII (pasal 27-37), yaitu:

   Pasal 27: Asusila, Perjudian, Penghinaan, Pemerasan.
   Pasal 28: Berita bohong dan Menyesatkan, Berita kebencian dan permusuhan
   Pasal 29: Ancaman Kekekrasan dan Menakut-nakuti.
   Pasal 30: Akses Komputer Pihak Lain Tanpa Izin, Cracking.
   Pasal 31: Penyadapan, Perubahan, Penghilangan Informasi.

   Ada satu hal yang menarik mengenai rancangan cyber law ini yang terkait dengan terotori. Misalkan, seorang cracker dari sebuah Negara Eropa melakukan pengrusakan terhadap sebuah situs di Indonesia. Salah satu pendekatan yang diambil adalah jika akibat dari aktivitas crackingnya terasa di Indonesia, maka Indonesia berhak mengadili yang bersangkutan. Yang dapat dilakukan adalah menangkap cracker ini jika dia mengunjungi Indonesia. Dengan kata lain, dia kehilangan kesempatan/ hak untuk mengunjungi sebuah tempat di dunia.

2. Cyber Law Negara Malaysia:

   Digital Signature Act 1997 merupakan Cyber Law pertama yang disahkan oleh parlemen Malaysia. Tujuan cyberlaw ini adalah untuk memungkinkan perusahaan dan konsumen untuk menggunakan tanda tangan elektronik (bukan tanda tangan tulisan tangan) dalam hukum dan transaksi bisnis. Pada cyberlaw berikutnya yang akan berlaku adalah Telemedicine Act 1997. Cyberlaw ini praktis medis untuk memberdayakan memberikan pelayanan medis/konsultasi dari lokasi jauh melalui penggunaan fasilitas komunikasi elektronik seperti konferensi video.

3. Cyber Law Negara Singapore:

   The Electronic Transactions Act telah ada sejak 10 Juli 1998 untuk menciptakan kerangka yang sah tentang undang-undang untuk transaksi perdagangan elektronik si Singapore. ETA dibuat dengan tujuan:Memudahkan komunikasi elektronik atas pertolongan arsip elektronik yang dipercaya.

a) Memudahkan perdagangan elektronik, yaitu menghapuskan penghalang perdagangan elektronik yang tidak sah atas penulisan dan persyaratan tandatangan, dan untuk mempromosikan pengembangan dari undang-undang dan infrastruktur bisnis diperlukan untuk menerapkan menjamin/mengamankan perdagangan elektronik.
b) Memudahkan penyimpanan secara elektronik tentang dokumen pemerintah dan perusahaan.
c) Meminimalkan timbulnya arsip elektronik yang sama, perubahan yang tidak sengaja dan disengaja tentang arsip, dan penipuan dalam perdagangan elektronik, dll.
d) Membantu menuju keseragaman aturan, peraturan dan mengenai pengesahan dan integritas dari arsip elektronik.
e) Mempromosikan kepercayaan, inregritas dan keandalan dari arsip elektronik dan perdagangan elektronik dan untuk membantu perkembangan dan pengembangan dari perdagangan elektronik melalui penggunaan tanda tangan yang elektronik untuk menjamin keaslian dan integritas surat menyurat yang menggunakan media elektronik

4. Cyber Law Negara Vietnam:

   Cybercrime, penggunaan nama domain dan kontrak elektronik di Vietnam sudah ditetapkan oleh Pemerintah Vietnam, sedangkan untuk masalah perlindungan konsumen privasi, spam, muatan online, digital copyright dan online dispute resolution belum mendapat perhatian dari pemerintah sehingga belum ada rancangannya.

5. Cyber Law Negara Thailand:

   Cybercrime dan kontrak elektronik di Negara Thailand sudah sitetapkan oleh pemerintahnya, walaupun yang sudah ditetapkannya hanya 2 tetapi yang lainnya seperti spam, privasi, digital copyright dan ODR sudah dalam tahap rancangan.

6. Cyber Law Negara Amerika Serikat:

   Di Amerika, cyberlaw yang mengatur transaksi elektronik dikenal dengan Uniform Electronic Transaction Act (UETA). UETA adalah salah satu dari beberapa Peraturan Perundang-undangan Amerika Serikat yang diusulkan oleh National Conference of Commissioners on Uniform State Laws (NCCUSL).
   Sejak itu 47 negara bagian, Kolombia, Puerto Rico, dan Pulau Virgin US telah mengadopsinya ke dalam hukum mereka sendiri. Tujuan menyeluruhnya adalah untuk membawa ke jalur hukum Negara bagian yang berbeda atas bidang-bidang seperti retensi dokumen kertas, dan keabsahan tanda tangan elektronik sehingga mendukung keabsahan kontrak elektronik sebagai media perjanjian yang layak.

## III. COUNCIL OF EUROPE CONVENTION ON CYBERCRIME ( COECCC )

COECCC telah diselenggarakan pada tanggal 23 November 2001 di kota Budapest, Hongaria. Konvensi ini telah menyepakati bahwa Convention on Cybercrime dimasukkan dalam European Treaty Series dengan nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal lima Negara, termasuk paling tidak ratifikasi yang

dilakukan oleh tiga Negara anggota Council of Europe. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan criminal yang bertujuan untuk melindungi masyarakat dari cybercrime, baik melalui undang-undang maupun kerja sama internasional.

Pertimbangan dibentuknya COECCC
Konvensi ini dibentuk dengan pertimbangan-pertimbangan antara lain sebagai berikut:

- Bahwa masyarakat internasional menyadari perlunya kerjasama antar Negara dan Industri dalam memerangi kejahatan cyber dan adanya kebutuhan untuk melindungi kepentingan yang sah dalam penggunaan dan pengembangan teknologi informasi.

Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Hal lain yang diperlukan adalah adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.

Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik Dan sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi/pendapat.

Konvensi ini telah disepakati oleh masyarakat Uni Eropa sebagai konvensi yang terbuka untuk diakses oleh Negara manapun di dunia. Hal ini dimaksudkan untuk diajdikan norma dan instrument Hukum Internasional dalam mengatasi kejahatan cyber, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi. Council of Europe Convention on Cyber crime merupakan suatu organisasi international dengan fungsi untuk melindungi manusia dari kejahatan dunia maya dengan aturan dan sekaligus meningkatkan kerjasama internasional. 38 Negara, termasuk Amerika Serikat tergabung dalam organisasi international ini. Tujuan dari organisasi ini adalah memerangi cybercrime, meningkatkan investigasi kemampuan.

Tujuan utama dari Council of Europe Convention on Cyber Crime adalah untuk membuat kebijakan “penjahat biasa” untuk lebih memerangi kejahatan yang berkaitan dengan komputer seluruh dunia melalui harmonisasi legislasi nasional, meningkatkan kemampuan penegakan hukum dan peradilan, dan meningkatkan kerjasama internasional.
Untuk tujuan ini, Konvensi ini mengharuskan penandatanganan untuk

- Menetapkan pelanggaran dan sanksi pidana berdasarkan undang-undang domestik mereka untuk empat kategori kejahatan yang berkaitan dengan komputer: penipuan dan pemalsuan, pornografi anak, pelanggaran hak cipta, dan pelanggaran keamanan (seperti hacking, intersepsi ilegal data, serta gangguan sistem yang mengkompromi integritas dan ketersediaan jaringan. Penanda tangan juga harus membuat undang-undang menetapkan yurisdiksi atas tindak pidana tersebut dilakukan di atas wilayah mereka, kapal atau pesawat udara terdaftar, atau oleh warga negara mereka di luar negeri.
- Menetapkan prosedur domestik untuk mendeteksi, investigasi, dan menuntut kejahatan komputer, serta mengumpulkan bukti tindak pidana elektronik apapun. Prosedur tersebut termasuk menjaga kelancaran data yang disimpan dalam komputer dan

komunikasi elektronik (“traffic” data), sistem pencarian dan penyitaan, dan intersepsi real-time dari data. Pihak Konvensi harus menjamin kondisi dan pengamanan diperlukan untuk melindungi hak asasi manusia dan prinsip proporsionalitas.

- Membangun sistem yang cepat dan efektif untuk kerjasama internasional. Konvensi ini menganggap pelanggaran cyber crime dapat diekstradisikan, dan mengizinkan pihak penegak hukum di satu negara untuk mengumpulkan bukti yang berbasis komputer bagi mereka yang lain. Konvensi juga menyerukan untuk membangun 24 jam, jaringan kontak tujuh-hari-seminggu untuk memberikan bantuan langsung dengan penyelidikan lintas-perbatasan.

Jenis Pidana yang diancamkan terhadap pelaku cybercrime berdasarkan convention of cybercrime

Kualifikasi kejahatan dunia maya (cybercrime), sebagaimana dikutip Barda Nawawi Arief, adalah kualifikasi Cybercrime menurut Convention on Cybercrime 2001 di Budapest Hongaria, yaitu

- Illegal access: yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.
- Illegal interception: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke,dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.
- Data interference: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.
- System interference: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.
- Misuse of Devices: penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (access code)
- Computer related Forgery: Pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik)
- Computer related Fraud: Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).
- Content–Related Offences Delik-delik yang berhubungan dengan pornografi anak (child pornography)
- Offences related to infringements of copyright and related rights Delik-delik yang terkait dengan pelanggaran hak cipta

Isi atau Muatan Konvensi Cybercrime

Konvensi ini berisi tentang beberapa hal, salah satunya adalah tindakan yang harus diambil pada tingkat nasional yaitu memasukkan ke dalam hukum nasional masing masing negara byang meliputi tentang:

Pengaturan tentang Pelanggaran terhadap integritas, kerahasiaan

dan ketersediaan data komputer dan sistem, hal ini meliputi:

a) Akses ilegal (Illegal Access)
b) Intersepsi ilegal (Illegal interception)
c) Data gangguan (Data interference)
d) Gangguan Sistem (System interference). .
e) Penyalahgunaan perangkat (Misuse of devices)

Pengaturan tentang Komputer yang berhubungan dengan pelanggaran

- Komputer yang berhubungan dengan pemalsuan.
- Komputer yang berhubungan dengan penipuan
- masukan apapun, perubahan, penghapusan atau penekanan dari data komputer,
- setiap gangguan dengan fungsi dari sebuah sistem komputer

Konten yang terkait dengan pelanggaran

a. Pelanggaran yang berkaitan dengan pornografi anak
    - Setiap Pihak wajib mengambil tindakan-tindakan legislatif dan lainnya yang dianggap perlu untuk menetapkan sebagai kejahatan pidana menurut hukum nasionalnya, apabila dilakukan dengan sengaja dan tanpa hak melakukan
    - Untuk tujuan ayat 1 di atas, istilah "pornografi anak" mencakup materi pornografi yang secara visual menggambarkan
    - Untuk tujuan ayat 2 di atas, istilah "anak" akan mencakup semua orang di bawah orang yang terlibat dalam perilaku seksual eksplisit
    - Setiap pihak dapat berhak untuk tidak menerapkan secara keseluruhan atau sebagaian, paragraf 1, sub-paragraf d, dan an e, dan 2, sub-paragraf b. dan c.
b. Pelanggaran yang berkaitan dengan pelanggaran hak cipta dan hak terkait lainnya.Pelanggaran yang berkaitan dengan pelanggaran hak cipta dan hak terkait meliputi:
    - Setiap Pihak wajib mengambil tindakan-tindakan legislatif dan lainnya yang dianggap perlu untuk menetapkan sebagai kejahatan pidana berdasarkan hukum nasionalnya pelanggaran hak-hak terkait, sebagaimana didefinisikan dalam hukum Pihak tersebut, sesuai dengan kewajiban yang telah dilakukan di bawah Konvensi Internasional untuk Perlindungan terhadap Pelaku Pertunjukan, Produser Rekaman dan Organisasi Penyiaran (Konvensi Roma),
    - Perjanjian tentang Trade-Related Aspek Hak Kekayaan Intelektual dan Pertunjukan WIPO dan Perjanjian Rekaman, dengan pengecualian dari setiap hak moral yang diberikan oleh konvensi-konvensi tersebut, di mana tindakan seperti itu berkomitmen sengaja, pada skala komersial dan melalui suatu sistem komputer.
    - Pihak dapat berhak untuk tidak membebankan tanggung jawab kriminal di bawah paragraf 1 dan 2 dari artikel ini dalam keadaan terbatas, asalkan pengobatan efektif lainnya tersedia dan pemesanan tersebut tidak menyimpang dari kewajiban internasional Partai diatur dalam instrumen internasional sebagaimana dimaksuddalam ayat 1 dan 2 pasal ini.
c. Tentang Tambahan Kewajiban dan Sanksi
    - Tentang Mencoba dan membantu atau bersekongkol.
    - Setiap Pihak wajib mengambil tindakan-tindakan legislatif dan lainnya yang dianggap perlu untuk menetapkan sebagai kejahatan pidana menurut hukum

nasionalnya, apabila dilakukan dengan sengaja, membantu atau bersekongkol dengan komisi dari setiap kejahatan yang ditetapkan sesuai dengan Pasal 2 sampai 10 dari Konvensi ini dengan maksud bahwa kejahatan semacam itu dilakukan.Setiap Pihak

- wajib mengambil tindakan-tindakan legislatif dan lainnya yang dianggap perlu untuk menetapkan sebagai kejahatan pidana menurut hukum nasionalnya, apabila dilakukan dengan sengaja, upaya untuk melakukan salah satu kejahatan yang ditetapkan sesuai dengan Pasal 3 sampai 5, 7, 8, dan 9.1.a dan c.Konvensi ini.
- Setiap Pihak dapat berhak untuk tidak menerapkan, secara keseluruhan atau sebagian, huruf b pasal ini.

d. Tentang kewajiban perusahan atau badan hukum swasta:
   - Setiap Pihak wajib mengambil tindakan-tindakan legislatif dan lainnya yang mungkin diperlukan untuk memastikan bahwa orang-orang hukum dapat bertanggung jawab untuk tindak pidana yang ditetapkan sesuai dengan Konvensi ini, berkomitmen untuk keuntungan mereka dengan setiap orang alami, bertindak baik secara individual atau sebagai bagian dari organ badan hukum, yang memiliki posisi terdepan di dalamnya, berdasarkan:
     - kekuatan representasi badan hukum;
     - kewenangan untuk mengambil keputusan atas nama badan hukum;
     - wewenang untuk melakukan kontrol dalam badan hukum.
     - Selain kasus-kasus yang sudah diatur dalam ayat 1 pasal ini, setiap Pihak wajib mengambil langkah-langkah yang diperlukan untuk memastikan bahwa badan hukum dapat bertanggung jawab dimana kurangnya pengawasan atau kontrol oleh orang alam sebagaimana dimaksud dalam ayat 1 telah dimungkinkan komisi dari tindak pidana yang ditetapkan sesuai dengan Konvensi ini untuk kepentingan orang hukum oleh orang perorangan yang bertindak di bawah wewenangnya.
   - Berdasarkan prinsip-prinsip hukum Partai, tanggung jawab suatu badan hukum dapat pidana, perdata atau administratif.
   - Tanggung jawab tersebut tanpa mengabaikan tanggung jawab pidana orang-orang alami yang telah melakukan pelanggaran.

e. Tentang Sanksi dan tindakan
   - Setiap Pihak wajib mengambil tindakan-tindakan legislatif dan lainnya yang mungkin diperlukan untuk memastikan bahwa tindak pidana yang ditetapkan sesuai dengan Pasal 2 sampai 11 dapat dihukum dengan sanksi yang efektif, proporsional dan yg menasihati jangan, yang meliputi perampasan kebebasan.
   - Setiap Pihak wajib menjamin bahwa badan hukum bertanggung jawab sesuai dengan Pasal 12 dikenakan efektif, sanksi pidana atau non-pidana proporsional dan yg menasihati jangan atau tindakan, termasuk sanksi moneter.

## IV. JENIS SANKSI PIDANA DALAM UU ITE DAN KONVENSI CYBERCRIME

Jenis-jenis sanksi yang dapat dijatuhkan untuk korporasi menurut UU ITE adalah pidana pokok berupa penjara dan denda yang dirumuskan secara komulatif serta ada pemberatan ancaman pidana sebagaimana diatur dalam Pasal 52 ayat (4)185 yang isinya

“dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga”.

Pemberatan pidana terhadap korporasi dalam UU ITE yakni penjatuhan denda ditambah dua pertiga tidak memiliki aturan yang khusus, terutama mengenai pidana pengganti untuk denda yang tidak dibayar. Ini berarti dikenakan ketentuan umum KUHP (Pasal 30), yaitu denda kurungan pengganti denda (maksimal 6 bulan, yang dapat menjadi 8 bulan apabila ada pemberatan pidana).

Konvensi Palermo kaitannya tentang Hukum Internasional mengenai Cyber Crime.

- Konvensi Palermo memutuskan kesepakatan pada pasal 1 bertujuan ;:
- “Tujuan dari konvensi palermo adalah untuk meningkatkan kerjasama dengan semua negara di dunia untuk memerangi kejahatan transnasional yang terorganisir”.
- Pasal 2 konvensi Palermo ayat C mengisayaratkan bahwa kejahatan ini merupakan kejahatan yang serius sehingga hukuman minimal 4 tahun atau lebih” . Artinya bahwa ketentuannya pelaku kejahatan transnasional akan mendapat hukuman minimal 4 tahun penjara dalam konsensi ini.
- Banyak sekali kejahatan transnasional maka yang disebut dengan hasil kejahatan adalah harta yang diperoleh secara langsung atau tidak langsung melalui bentuk pelanggaran.Jadi yang dimaksud adalah memiliki atau mengambil barang orang lain tanpa ijin atau melalui pelanggaran hukum.
- Predikat palanggaran seperti dalam Pasal 2 ayat h adalah pelanggaran dari setiap hasil yang bisa menjadi subyek dari suatu pelanggaran, yang ditetapkan dalam pasal 6 konvensi ini.
- Dimana Pasal 6 ayat 1 berbunyi bahwa setiap negara harus mengadopsi sesuai dengan prinsip-prinsip hukum domestik, antala legislatif dan langkah-langkah sebagai mungkin perlu menetapkan sebagai pelanggaran pidana. Artinya setiap negara harus membuat hukum yang mengatur tentang penegakan Cyber Crime sebagai bukti keseriusan untu melaksanakan kaidah Konsensi Palermo, berupa UU no. 11 tahun 2008 tentan ITE.
- Konvensi ini digunakan untuk semakin terjaminnya keamananan Internasional dalam menghadapi kejahatan transnasional dalam kerjasama internasional.
  Pasal 27 ayat 1 menerangkan bahwa ;
  “Pihak Negara-negara akan bekerjasama dengan erat satu sama lain sesuai dengan rumah tangga masing-masing sesuai hukum dan administrasi untuk meningkatkan efektifitas penegakan hukum untuk memerangi tindakan pelanggaran yang mencakup dalam konvensi tiap negara wajib mengadobsi langkah-langkah efektif tersebut.” Bentuk kerjasama dapat berupa organisasi artau konsensi dan atau merespon tiap informasi secara bersama-sama.
- Implementasi dari konvensi ini adalah tertuang dalam pasal 34 ;

  Setiap negara harus mengambil langkah-langkah yang diperlukan termasuk legislatif dan tindakan-tindakan administratif sesuai dengan prinsip-prinsip dah hukum domestik, untuk menjamin kewajiban dalam konvensi ini.
  Pelanggaran yang sesuai dengan pasal 5.6, 8 dan 23 dalam pasal konvesi ini harus dibentuk dalam setiap negara untuk menghadapi kriminal yang mencakup wilayah transnaional baik pribadi maupun kelompok.

- Setiap negara harus mengadobsi konvensi ini.

Inilah yang mendasari dibuatnya sebuah hukum yang mengatur dalam mengatasi kejathatan transnasional dalam hal ini cyber crime.
Perbuatan Yang Dilarang dalam UU ITE Konvensi Budapest membahas tentang sanksi pidana. :

1. Pelanggaran kesusilaan.
2. Perjudian.
3. penghinaan dan/atau pencemaran nama baik.
4. pemerasan dan/atau pengancaman.
5. menyebarkan berita bohong dan menyesatkan
6. menyebarkan informasi yang menimbulkan kebencian bersifat SARA.
7. ancaman kekerasan atau menakut-nakuti.
8. melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
9. melakukan intersepsi atau penyadapan atas Informasi Elektronik milik Orang lain.
10. melakukan intersepsi yang tidak bersifat publik dari, ke, dan di dalam suatu Sistem Elektronik tertentu milik Orang lain, tidak menyebabkan perubahan apapun maupun menyebabkan perubahan, penghilangan, dan/atau penghentian Informasi Elektronik sedang ditransmisikan.
11. Pelanggaran terhadap kerahasiaan, integritas dan ketersediaan data dan sistem komputer.
12. akses ilegal,
13. cegatan ilegal,
14. Data gangguan,
15. penyalahgunaan perangkat Komputer yang berhubungan dengan pelanggaran dalam Konvensi ini adalah : Computer yang terkait pemalsuan.yang terkait penipuan.
16. Pelanggaran yang terkait dengan pornografi anak
17. Pelanggaran yang berkaitan pelanggaran hak cipta dan hak-hak yang terkait .

**KEJAHATAN KOMPUTER**

Trend perkembangan teknologi informasi, terutama internet. Dampak negatif seperti pornografi Internet. "CyberCrime" → kejahatan melalui jaringan Internet:

- pencurian kartu kredit
- hacking situs
- menyadap transmisi data orang lain
- memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program komputer

Dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil:

- Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin
- Delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain

Kejahatan menggunakan sarana komputer (Bainbridge,1993) :

- Memasukkan instruksi yang tidak sah;
- Perubahan data input;
- Perusakan data;
- Komputer sebagai pembantu kejahatan;
- Akses tidak sah terhadap sistem komputer.

- Ancaman terhadap Penggunaan Internet (Bernstein et.al., 1996):
- Menguping (eavesdropping);
- Menyamar (masquerade);
- Pengulang (reply);
- Manipulasi data (data manipulation);
- Kesalahan Penyampaian (misrouting);
- Pintu jebakan atau kuda Trojan (trapdoor);
- Virus (viruses);
- Pengingkaran (repudoition);
- Penolakan Pelayanan (denial of service).

Beberapa kendala di internet akibat lemahnya sistem keamanan komputer (Bernstein et.al., 1996):

- Kata sandi seseorang dicuri ketika terhubung ke sistem jaringan dan ditiru atau digunakan oleh pencuri.
- Jalur komunikais disadap dan rahasia perusahaan pun dicuri melalui jaringan komputer.
- Sistem informasi dimasuki (penetrated) oleh pengacau (intruder).
- Server jaringan dikirim data dalam ukuran sangat besar (e-mail bomb) sehingga sistem macet.

## V. KENDALA YURIDIS UNDANG-UNDANG ITE

Undang-Undang ITE tidak mengatur secara khusus hal-hal yang menyangkut cybercrime. Di dalam Bab Ketentuan Umum tidak secara jelas digambarkan tentang penjelasan kejahatan-kejahatan dengan menggunakan komputer. Kejahatan-kejahatan komputer yang dikenal dalam dunia maya tidak tergambar secara jelas. Pemerintah dalam membentuk Undang-Undang ITE ini masih menggunakan pendekatan politis-pragmatis, bukan menggunakan pendekatan kebijakan publik yang melibatkan lebih banyak kalangan, sehingga tidak heran kalau UU ITE ini hanya sepotong-sepotong mengatur pemanfaatan teknologi yang sudah begitu luas penggunaannya di berbagai aspek kehidupan manusia.

UU ITE ini lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, tidak lebih. Padahal siapapun tahu bahwa dunia siber (cyberword ) lebih luas dari sekedar transaksi elektronik. Banyak ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam Undang-Undang ITE seperti hal-hal yang diatur dalam buku I KUHP tidak ada dalam Undang-Undang ITE. Seperti kelalaian atau khilaf, di mana lalai atau khilaf adalah kalimat yang sering dilakukan oleh manusia dalam melakukan kegiatannya. Apabila kelalaian itu dilakukan oleh manusia di dunia nyata dan menimbulkan kerugian bagi dirinya sendiri dan orang lain, diatur secara tersendiri dengan menggunakan pasal-pasal tertentu, bahkan kadang pula si pembuat lalai ini juga akan mendapatkan ancaman hukuman seperti banyak ditemukan kasus-kasus pelanggaran lalu lintas. Namun di dalam dunia maya (cyberspace) kelalaian adalah tindakan fatal yang bisa menimbulkan kerugian yang tidak sedikit, bahkan bisa menghancurkan sebuah negara sekalipun.

Dalam Undang-Undang ITE tidak menyebutkan sedikitpun tentang kelalaian yang dibuat oleh pembuat situs sehingga hacker bisa masuk dengan leluasa. Kegiatan yang lain yang sama pentingnya dengan kelalaian adalah percobaan melakukan perbuatan jahat dan

turut serta melakukan. Dalam Undang-Undang ITE ini tidak diatur apakah percobaan melakukan dan juga turut serta kejahatan hacking dapat dipidana atau tidak. Kemudian Undang-Undang ITE ini juga tidak mengatur kapan kadaluwarsa perbuatan pidana kejahatan hacking. Semua kegiatan kejahatan tersebut diatur pada Bab tentang perbuatan perbuatan apa saja yang dilarang, sehingga terkesan seperti pasal keranjang sampah, pokoknya semua kegiatan yang melanggar aturan telematika di Indonesia itulah yang dilarang. Dari sekian banyak sisi gelap yang ada dalam cyberspace, yang paling banyak mendapat perhatian adalah perbuatan yang dilakukan oleh Hacker Hitam (Cracker).

Pada umumnya reaksi yang diberikan oleh korban Cracker adalah merasa kaget, kesal dan terakhir mencela ulah Cracker ini. Akibat ulah Cracker ini bukan hanya uang yang seharusnya dapat diinvestasikan untuk keperluan lain menjadi terhambat, melainkan keuntungan seperti dijanjikan ketika memasuki cyberspace untuk sementara tidak terwujud. Para korban umumnya menganggap serangan Cracker ini sebagai sebuah kecelakaan dan mereka tidak mau mempublikasikan atau melaporkan apa yang dideritanya kepada polisi meskipun sebenarnya tahu apa yang dilakukan oleh Cracker itu merupakan tindak kejahatan. Internet sebagai hasil revolusi teknologi memungkinkan transfer data secara cepat dan efisien pada skala global, namun tampaknya sumber daya aparatur belum sepenuhnya menyadari betapa hebatnya teknologi informasi dan komunikasi yang menyebabkan perubahan paradigma dalam kehidupan berbangsa dan bernegara. Ketidak-mampuan polisi dalam menangani aktivitas Hacking juga menjadi sorotan dari para korban Cracker.

Ketidakmampuan ini telah mengubah paradigma teori labeling yang mengasumsikan tindakan penangkapan merupakan proses awal dari labeling. Polisi belum dapat menangkap Cracker yang menghack sebuah situs (termasuk ketidakmampuan menangkap Cracker yang men-yerang situs Polri sendiri) sehingga langkah awal dari proses labeling berupa penangkapan tidak ada. Proses awal dari labeling justru terdapat dari laporan-laporan media massa yang secara gencar memberitahukan aktivitas Hacking. Indonesia menjadi tampak tertinggal dan sedikit terkucilkan di dunia internasional, karena negara lain misalnya Malaysia, Singapura dan Amerika Serikat sudah sejak 10 tahun yang lalu mengembangkan dan menyempurnakan Cyberlaw yang mereka miliki. Malaysia punya Computer Crime Act (Akta Kejahatan Komputer) 1997, Communication and Multimedia Act (Akta Komunikasi dan Multimedia) 1998, dan Digital Signature Act (Akta Tandatangan Digital) 1997. Singapura juga sudah punya The Electronic Act (Akta Elektronik) 1998, Electronic Communication Privacy Act (Akta Privasi Komunikasi Elektronik) 1996. Amerika Serikat intens untuk memerangi child pornography dengan:
US Child Online Protection Act (COPA), US Child Pornography Protection Act, US Child Internet Protection Act (CIPA), US New Laws and Rulemaking (Romi Satria Wahono, Analisa Undang-Undang ITE, diunduh dari http://romisatriawahono.net/2008/04/24/analisa-uu-ite/, tanggal 24 Desember 2009).

Lahirnya Undang-Undang ITE ini belum dibarengi oleh peraturan yang mengatur tentang hukum formilnya. Perangkat hukum yang ada di Indonesia belum memadai untuk menjerat kejahatan dunia maya ( cybercrime ) pada umumnya dan kejahatan hacking pada khususnya. Indonesia saat ini pun baru mempunyai sebuah Undang-Undang baru yang mengatur tentang perilaku kegiatan di dunia siber (cyberspace), namun Undang-Undang ITE yang ada saat ini masih menggunakan model umbrella provision sehingga ketentuan cybercrime tidak diatur dalam peraturan perundang-undangan tersendiri, sedangkan

peraturan perundang-undangan yang ada sebelum Undang-Undang ITE ini lahir juga ada mengatur tentang kegiatan di dunia siber (I) meskipun itu hanya beberapa pasal saja. Kitab Undang-Undang Hukum Pidana yang dipunyai Indonesia juga harus dilakukan perubahan revolusioner untuk mengatur kegiatan di dunia siber (cyberspace) dengan memperluas pengertian- pengertian yang terkait dengan kegiatan-kegiatan di cyberspace

## VI. TERMINOLOGI CYBER CRIME

Istilah cybercrime saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (cyberspace) dan tindakan kejahatan yang menggunakan komputer . ada ahli yang menyamakan antara tindak kejahatan cyber (cybercrime) dengan tindak kejahtan komputer, dan ada ahli yang membedakan keduanya. Barda Nawawi Arief menunjuk pada kerangka ( sistematik ) Draft Convention on cybercrime dari Dewan Eropa ( Draft No.25, Desember 2000). Beliau menyamakan peristilah antara keduanya dengan memberikan definisi cybercrime sebagai "crime related to technology, computers and the internet" atau secara sederhana berarti kejahatan yang berhubungan dengan teknologi, komputer dan internet. Kejahatan yang berhubungan erat dengan pengguna teknologi komputerdan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokan beberapa bentuk, antara lain:

- Unauthorized access to computer system and service, yaitu kejahatan yang dilakukan kedalam sistem suatu jaringan secara tidak sah, tanpa izin atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang di masukinya.
- Illegal contens, yaitu kejahatan denagn memasukan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis dan dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh adalah :
- Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
- Pemuatan yang berhubungan dengan pornografi
- Data forgery, yaitu kejahatan dengan memalsukan data pada dokumendokumen penting tersimpan sebagai scriptless document melalaui internet. Kejahatan ini biasanya di tujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah salah ketik sehingga menguntungkan pelaku.
- Cyber espionage,yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasukan sistem jaringan komputer pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau data-data pentingnya tersimpan dalam suatu sisitem komputerisasi.
- Cyber sabatage and extortion, yaitu kejahatan yang dilakukan dengan membuat gangguan,perusak atau penghancur terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet.
- Offence against intelectualproperty,yaitu kejahatan yang ditujukan terhadap hak kekayaan intelektual yang di miliki seseorang di internet.contoh peniruan tampilan web page suati situs orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang.
- Infringements of privacy, yaitu kejahatan yang di tujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi seseorang yang tersimpan

secara komputerisasi yang apabila di ketahui oleh orang lain maka akan menimbulkan kerugian materil maupun inmateril seperti nomor kartu keredit, nomor PIN ATM dan sebagainya.

## VII. PENYIDIKAN TERHADAP TINDAK PIDANA CYBER CRIME

Menurut Undang-Undang No 2 Tahun 2002 tentang Kepolisian Pasal 1 angka 13 penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Undang-Undang untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Dalam memulai penyidikan tindak pidana Polri menggunakan parameter alat bukti yang sah sesuai dengan Pasal 184 KUHAP yang dikaitkan dengan segi tiga pembuktian/evidence triangle untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi.

Dalam penyidikan tindak pidana cybercrime selain berlaku ketentuan dalam Kitab Undang-Undang Hukum Acara Pidana juga berlaku ketentuan-ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang diatur dalam Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pembuktian sebenarnya telah di mulai dalam tahap penyidikan, pembuktian, bukan dimulai pada tahap penuntutan maupun persidangan.

Dalam penyidikan, penyidik akan mencari pemenuhan unsur pidana berdasarkan alat-alat bukti yang diatur dalam perundang-undangan. Pada tahap penuntutan dan persidangan kesesuaian dan hubungan antara alat-alat bukti dan pemenuhan unsur pidana akan diuji. Penyidikan terhadap tindak pidana cybercrime selain dilaksanakan berdasarkan ketentuan yang diatur mengenai penyidikan yang tedapat dalam Kitab Undang-Undang Hukum Acara Pidana juga dilaksanakan berdasarkan ketentuan khusus mengenai penyidikan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, hal ini dilakukan agar penyidikan dan hasilnya dapat diterima secara hukum. Berikut adalah beberapa hal mengenai penyidikan yang diatur dalam Undang – Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik :

- Pasal 43 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa yang diizinkan untuk melakukan penyidikan di dalam undang -undang ini adalah penyidik Kepolisian Negara Republik Indonesia dan pejabat pegawai negeri sipil tertentu yang lingkup tugas dan tanggung jawabnya di bidang teknologi dan transaksi elektronik.
- Pasal 43 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa penyidikan terhadap tindak pidana cybercrime harus memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan perundang-undangan.
- Pasal 43 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan setempat.

- Pasal 43 ayat (6) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib 22 meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

HAMBATAN

Adapun hambatan-hambatan yang ditemukan di dalam proses penyidikan antara lain adalah sebagai berikut:

1. Perangkat Hukum yang Belum Memadai
   Lemahnya peraturan perundang-undangan yang dapat diterapkan terhadap pelaku cybercrime, sedangkan penggunaan pasal-pasal yang terdapat di dalam KUHP seringkali masih cukup meragukan bagi penyidik. Oleh sebabitu perlu dibuat undang-undang yang khusus mengatur cybercrime.
2. Kemampuan Penyidik
   Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus kejahatan dunia maya. Beberapa faktor yang sangat berpengaruh (determinan) adalah:
3. Kurangnya pengetahuan tentang komputer.
   Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus cybercrime masih terbatas.
   Faktor sistem pembuktian yang menyulitkan para penyidik.
   Dalam hal menangani kasus cybercrime diperlukan penyidik yang cukup berpengalaman (bukan penyidik pemula), pendidikannya diarahkan untuk menguasai teknis penyidikan dan menguasai administrasi penyidikan serta dasar-dasar pengetahuan di bidang komputer dan profil hacker.
4. Alat Bukti
   Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap Cybercrime antara lain berkaitan dengan karakteristik kejahatan cybercrime itu sendiri, yaitu:

   Sasaran atau media cybercrime adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya. Oleh karena itu, data atau sistem komputer atau internet yang berhubungan dengan kejahatan tersebut harus direkam sebagai bukti dari kejahatan yang telah dilakukan. Permasalahan timbul berkaitan dengan kedudukan media alat rekaman (recorder) yang belum diakui KUHAP sebagai alat bukti yang sah.
   Kedudukan saksi korban dalam cybercrime sangat penting disebabkan cybercrime seringkali dilakukan hampir-hampir tanpa saksi. Di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.
5. Fasilitas Komputer Forensik
   Untuk membuktikan jejak-jejak para hacker, cracker dan phreackerdalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy, seperti image, program, dan sebagainya. Dalam hal ini Polri

masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas forensic computingyang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu mengumpulkan bukti(evidence collection), analisis forensik (forensic analysis), petunjuk saksi (expert witness).