BAB II

KAJIAN PUSTAKA

A. Kejahatan Transnasional

Secara konseptual, *transnational crime* (kejahatan transnasional adalah tindak pidana atau kejahatan yang melintasi negara. Konsep ini diperkenalkan pertama kali secara internasional di tahun 1990-an dalam *The Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders.*[24] Sebelumnya istilah yang lebih dulu berkembang adalah *organized crime* (kejahatan terorganisir). Perserikatan Bangsa-bangsa (PBB) sendiri menyebut:

> *organized crime* (kejahatan terorganisir) sebagai *the large-scale and complex criminal activity carried on by groups of persons, however loosely or tightly organized, for the enrichment of those participating and the espense of the community and its member*[25]

Pada perkembangannya PBB menambahkan bahwa istilah ini seringkali diartikan sebagai:

> *The large-scale and complex criminal activities carried out by tightly or loosely organized associations and aimed at the establishment, supply and esploitation of illegal markets at the expense of society.*[26]

Menurut Mueller dalam *Transnational Crime: Definitions and Concepts*, pada pertengahan tahun 1990-an banyak peneliti mendefinisikan "kejahatan transnasional" untuk menyebut "*...offences whose inception, prevention, and/or*

---

[24]Wagley, John R., ***Transnational Organized Crime:Principal Threats and U.S. Response,*** *Congressional Research Service, The Library of Congress,* 2006, hal 90.

[25]United Nations, ***Changes ib Forms and Dimensions of Criminality – Transnational and National,*** *Working paper prepared by the secretariat for the fifth United Nations Congress on the Prevention of crime and the Treatment of Offenders,* Toronto, Canada, 1-12 September 1975.

[26]United Nations, ***Eight United Nations Congress on the Preventions of Crime and the Treatment of Offenders***, Havana, Cuba, 27 Agustus – 7 September 1990, A/Conf. 144/7, 26 Juli 1990.

direct or indirect effects involve more than one country...".[27] Mueller sendiri menggunakan istilah kejahatan transnasional untuk mengidentifikasi "*...certain criminal phenomena transcending international borders, trans-gressing the laws of several states or having an impact on another country.*[28]

Menurut *United Nations Convention Against Transnational Organized Crime* (Konvensi Kejahatan Transnasional Terorganisir) pada tahun 2000, kejahatan dapat dikatakan bersifat transnasional jika terdiri dari:

1. Dilakukan di lebih dari satu negara,
2. Dilakukan di suatu negara tetapi hal penting dari persiapan, perencanaan, pengarahan, dan perngawasan dilakukan di negara lain,
3. Dilakukan di suatu negara tetapi melibatkan suatu kelompok kejahatan terorganisir (*organized criminal*) dimana kejahatan dilakukan di lebih satu negara
4. Dilakukan di suatu negara tetapi memiliki akibat di negara lain.[29]

Kejahatan transnasional merupakan fenomena sosial yang melibatkan orang, tempat dan kelompok, yang dipengaruhi oleh berbagai sosial, budaya, faktor ekonomi.[30] Akibatnya berbagai negara cenderung memiliki definisi kejahatan transnasional yang sangat berbeda tergantung pada filosofi tertentu. Menurut Martin dan Romano:

> *Transnationl crime may be defined as tha behavior of ongoing organizations that involves two or more nations, with such*

---

[27]Mueller, Gerhard O. W., ***Transnational Crime: Definitions and Concepts***, *Transnational Organized Crime 4*, 1998, hal 76.

[28]Ibid.

[29] United Nations, ***United Nations Convention Against Transnational Organization Crime***, Palermo, 2000.

[30]Mark Findlay, ***The Globalization of Crime: Understanding Transnational Relationship in Context,*** Cambridge University Press, 2003, hal 142.

behavior being defined as criminal by at least one of these nations.[31]

B. Cyberspace

Cyberspace merupakan dunia virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi, yaitu dari perkembangan teknologi informasi dan komunikasi. Teknologi informasi dan komunikasi merupakan gabungan dari teknologi komputer, telekomunikasi serta jaringan komputer dan telekomunikasi.[32]

Cyberspace terbentuk dari berbagai macam jaringan komputer dan telekomunikasi yang saling terhubung dan berinteraksi yang disebut *electronic nervous system.* Jaringan ini bahkan membentuk *global village*,[33] suatu tempat yang dimiliki oleh semua orang, dan dalam tempat tersebut tersimpan berbagai macam informasi yang mungkin tidak dapat dihitung lagi.

C. CyberCrime

Sama seperti di dunia konvensional yang penuh dengan permasalahan hukum, *cybersurfers* juga semakin melihat adanya masalah-masalah hukum dalam dunia siber. Kebebasan untuk menggunakan identitas anonim atau alias membutuhkan kepercayaan yang kuat antara para pihak yang melakukan transaksi. Resiko akan semakin besar dalam hal jumlah dan nilai transaksi

---

[31]Martin, J. M. And Romano A. T., ***Multinational Crime-Terorism, Espionage, Drug & Arm Trafficking,*** SAGE Publication, 1992.

[32]Bert-Jaaps Koops, *Should ICT Regulation be Technology-Neutral*, Miriam Lips, CorlensPrins, Maurice Scellekens (eds), **Starting Points for ICT Regulation. Desconstructing Policy One-Liners, IT & Law Series**, Vol 9, The Hague: T.M.C. Asser Press 2006, hal 98.

[33]Marshall Mcluhan, 2010, (online), http//www.livinginternet.com/, (21 September 2013).

semakin banyak dan besar. Tidak adanya saksi yang melihat secara langsung terjadinya transaksi tersebut dapat memperbesar resiko.

Hal yang buruk dalam masalah ialah timbulnya kejahatan seperti yang terjadi dalam dunia fisik. Para penjahat melihat karakteristik internet sebagai kesempatan atau sarana bagi mereka untuk melaksanakan niat jahat melalui berbagai perbuatan yang lebih dikenal dengan *cybercrimes*. Kebebasan menggunakan identitas dimanfaatkan untuk menipu, kebebasan berekspresi dimanfaatkan untuk menyebarkan informasi yang berisi fitnah, kebebasan untuk mengembangkan teknologi dan kreatifitas digunakan untuk merusak website atau menyebarkan virus.

Cybercrimes adalah bagian dari *Computer Crimes*, pengklasifikasian *computer crimes* dapat didasarkan pada teknologi, motivasi, hasil, dan komunikasi, serta informasi.[34]

Cyber Crime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengidentifikasi *cyber crime* dengan *computer crimes* (kejahatan dengan menggunakan komputer). The U.S. Department of Justice memberikan pengertian *computer crime* sebagai: "*...any illegal act requiring knowkedge of computer technology for its perpetration, investigation, or prosecution".*[35]

Dalam tulisannya Andi Hamzah (1989) berkata bahwa, "Aspek-aspek Pidana di Bidang Komputer", mengartikan kejahatan komputer sebagai:

---

[34]Ian Walden, Computer Crimes and Digital Investigations, JosuaSitompul (ed), ***Cyberspace, Cybercrime, Cyberlaw:* Tinjauan Aspek Hukum Pidana,** 2012, hal 36.

[35]Depertment of Justice, ***Department of Justice Disrupts International Cybercrime Rings Distributing Scareware,*** 2011, http://www.justice.gov/opa/pr/2011/June/11-crm-820.html, (13 Juli 2013).

"Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Definisi tersebut identik dengan yang diberikan Organization of European Community Development, yang mendefinisikan kejahatan komputer sebagai "*...any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".*

Menurut Supriyadi *cyber crime* adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.[36]

Berdasarkan jenis aktifitas yang dilakukannya, cybercrime dapat digolongkan menjadi beberapa jenis sebagai berikut:

a. Unauthorized Access

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

b. Illegal Contents

Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.[37]

---

[36]Supriyadi, 2013, **Definisi *Cyber Crime*** (online)**,** http://cybercrime3.wordpress.com/category/cybercrime/,(13 Juli 2013).

[37]Mansur, Dikdik M. Arief, op.cit, hal 9

c. Penyebaran virus secara sengaja

Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

d. Data Forgery

Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

e. Cyber Espionage, Sabotage, and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasukisistem

Jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

f. Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

g. Carding

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.[38]

h. Hacking dan Cracker

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya.Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakansitus web, *probing*, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan.

i. Cybersquatting and Typosquatting

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

[38]Maskun, op cit, hal 51.

j. Hijacking

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).

k. Cyber Terorism

Suatu tindakan *cybercrime* termasuk *cyber terorism* jika mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer.[39]

D. Pencegahan Kejahatan

Konsep pencegahan kejahatan *(crime prevention)* menurut *The National Crime "Crime prevention as the anticipation, recognition and appraisal of a crime risk and the initiation of some action to remove or reduce it"*. Defnisi pencegahan kejahatan adalah proses antisipasi, identifikasi dan estimasi resiko akan terjadinya kejahatan dan melakukan inisiasi atau sejumlah tindakan untuk menghilangkan atau mengurangi kejahatan. Menurut Robert L. O'Block menyatakan bahwa kejahatan adalah masalah sosial, maka usaha pencegahan kejahatan yang merupakan usaha yang melibatkan berbagai pihak.[40]

Menurut Fischer, pencegahan kejahatan adalah *"to determind the amount of force a security officer may use to prevent crime, the court have consider circumstance, the seriousness of the crime prevented and the possibility of preventing the crime by other means".* Artinya untuk menentukan jumlah

[39]Maskun, op cit, hal 51.

[40] O'Block L, Robert, ***Security and Crime Prevention***, Mosby Company, St. Louis, 1981, hal 3.

kekuatan petugas pengamanan yang dapat digunakan untuk mencegah kejahatan, pengelola mempertimbangkan keadaan, keseriusan mencegah kejahatan dan kemungkinan mencegah kejahatan dengan cara lain.[41]

Selain konsep diatas, suatu pengertian kejahatan secara umum pada dasarnya ada beberapa penataan sistem yang harus dilakukan bertujuan agar dapat bekerja dengan baik, yaitu:

1. Pendekatan terpadu atau metoda
2. Hubungan antara pemerintah dengan masyarakat yang keduanya merupakan subyek dari segala aktivitas pengamanan
3. Situasi aman sebagai objek pengamanan masyarakat.

Sedangkan pencegahan kejahatan secara khusus pada dasarnya tidak jauh berbeda dengan pengertian pencegahan kejahatan pada umumnya, hanya yang membedakannya mungkin pada cara atau strategi yang digunakan yang salah satunya adalah pencegahan kejahatan dengan pendekatan situasional *(Situasional crime prevention)* yang berasal dari berbagai teori pencegahan yang menggunakan strategi dalam menjelaskan suatu bentuk strategi pencegahan yang diterapkan dalam suatu lingkungan atau kegiatan tertentu. Bentuk dari pendekatan situasional adalah pencegahan kejahatan yang cenderung memusatkan perhatiannya pada pengembangan langkah-langkah berjangka pendek dalam suatu pencegahan kejahatan yang bertujuan untuk pengamanan suatu kegiatan.

Menurut Kaiser, pencegahan kejahatan adalah suatu usaha yang meliputi segala tindakan yang mempunyai tujuan yang khusus untuk memperkecil luas

[41] Fischer, Robert J dan Gion Green, ***Introduction to Security***, Elsevier Science USA, Butterworth Heinemann, Sixth Ed, 1998, hal 144.

lingkup dan kekerasan suatu kejahatan, baik melalui pengurangan kesempatan-kesempatan untuk melakukan kejahatan ataupun melalui usaha-usaha pemberian pengaruh kepada orang-orang yang secara potensial dapat menjadi pelanggar serta kepada masyarakat umum. Selanjutnya terdapat pembagian strategi pencegahan kejahatan yang utama kedalam tiga kelompok, yaitu:

1. Pencegahan primer, yaitu pencegahan dalam bidang sosial, ekonomi, dan bidang lain dalam kebijakan umum. Tujuannya untuk menciptakan kondisi yang sangat memberikan harapan bagi keberhasilan sosialisasi untuk setiap anggota masyarakat.
2. Pencegahan sekunder merupakan pencegahan yang dapat ditemui dalam kebijakan peradilan pidana.
3. Pencegahan tersier merupakan suatu pencegahan yang memberikan perhatian kepada residivis melalui peran polisi dan lembaga-lembaga lain dalam sistem peradilan pidana.[42]

E. Yurisdiksi Negara

Yurisdiksi merupakan suatu kekuatan (*power*) yang dimiliki oleh negara dibawah lingkup Hukum Internasional dalam mengatur segala hal yang meliputi orang, properti serta peristiwa hukum yang merefleksikan prinsip-prinsip dasar tentang kedaulatan negara, prinsip persamaan serta prinsip non-intervensi dalam mengurusi urusan domestik suatu negara[43].

---

[42] Agustina Elfrida, Helen, **Pencegahan Terhadap Tindak Pidana Pencurian dengan Kekerasan Saat Melakukan Pengelolaan dan Pengiriman Uang Tunai Oleh Badan Usaha Jasa Pengamanan**, Skripsi tidak diterbitkan, Jakarta, Fakultas Hukum UPN Jakarta, hal 23.

[43] Shaw, Malcolm N., ***International Law, Sixth Edition***, Cambridge University Press, UK, 2008. Hal. 48.

Yurisdiksi secara khusus merupakan bagian dari kedaulatan negara itu sendiri, hal ini berhubungan erat dengan kewajiban serta kewenangan suatu negara dalam mengatur segala hal yang ada dalam wilayahnya. Yurisdiksi dapat berjalan dengan adanya tindakan melalui lembaga legislatif, eksekutif serta yudikatif, ketiga pilar tersebut secara bersamaan akan menguatkan peran negara sebagai entitas yang mandiri. Terdapat pembatasan dalam menjalankan Yurisdiksi dimana yurisdiksi suatu negara akan berakhir jika telah melewati batas-batas wilayah negaranya, hal ini dimaksudkan untuk menghindari intervensi atau gangguan dari negara lain.

Ruang lingkup serta pelaksanaan yurisdiksi jika didasarkan pada objek dibagi menjadi tiga prinsip, yaitu yurisdiksi domestik (*domestic jurisdiction*), yurisdiksi territorial (*territorial jurisdiction*) serta yurisdiksi universal (*universal jurisdiction*). [44]

Prinsip yurisdiksi domestik secara filosofis merupakan perwujudan asli dari bentuk kedaulatan itu sendiri dimana dalam hal ini negara secara internal mempunyai wewenang serta kekuasaan tertinggi, negara lain tidak mempunyai wewenang intervensi terhadap permasalahn dalam negeri suatu negara. Yurisdiksi domestik berlaku atas personal atau individu-individu maupun benda-benda yang tunduk pada hukum nasional suatu negara. Yurisdiksi domestik dibagi menjadi dua, yang *pertama* yurisdiksi domestik aktif yang berlaku terhadap setiap orang dimana pun ia berada. *Kedua* yurisdiksi domestik pasif yang berlaku untuk setiap warga negara dimanapun ia berada.

[44]Malcolm N.Shaw. *Ibid.* hal. 64.

Yurisdiksi teritorial adalah adalah yurisdiksi yang berlaku terhadap orang atau benda yang berada dalam wilayah kedaulatan suatu negara. Yurisdiksi ini berlaku baik kepada warga negaranya sendiri maupun warga negara asing selama ia berada dalam wilayah kedaulatan suatu negara. Warga negara asing tidak dapat membebaskan diri dari yurisdiksi ini kecuali memiliki hak imunitas yang dalam hukum internasional dimiliki oleh kepala negara atau pemerintahan, perwakilan diplomatik, utusan khusus, kapal pemerintah asing, kapal perang dan organisasi internasional.

Yurisdiksi universal diterapkan pada kasus-kasus yang luar biasa seperti pada kasus kejahatan perang dan terorisme. Dimana kedua bentuk kejahatan tersebut termasuk dalam kejahatan internasional yang seluruh negara berkewajiban untuk memberantasnya, sehingga dalam hal ini yurisdiksi yang berlaku adalah yurisdiksi internasional dimana batasan mengennai wilayah atau kedaulatan negara secara *legal* diterobos oleh yurisdiksi ini.

Secara umum terdapat beberapa asas mengenai yurisdiksi yang berkaitan dengan permasalahan kejahatan internasional (*international crime*), hal ini memungkinkan ketentuan hukum suatu negara dapat berlaku dalam mengatur kegiatan serta hubungan antar individu, status hingga kepentingan individu terhadap suatu hal. Beberapa asas dalam yurisdiksi tersebut diantaranya adalah[45].:

a. *Subjective territoriality,* prinsip ini merupakan prinsip mengenai yurisdiksi yang paling penting dan sederhana, suatu peristiwa hukum jika terjadi di wilayah territorial suatu negara maka secara otomatis yurisdiksi negara tersebutlah yang berlaku dimana peristiwa hukum itu terjadi.

[45]Hillier, Tim, ***Sourcebook On Public International Law***,Cavendish Publishing Limited, UK, 1998, hal 78.

b. *Objective territoriality,* prinsip ini menjelaskan dimana suatu peristiwa hukum terjadi diluar wilayah territorial negara, namun objek serta dampak dari peristiwa hukum tersebut mempunyai efek terhadap negara tersebut. sehingga dalam hal ini yang digunakan adalah yurisdiksi negara terkena dampak dari peristiwa hukum tersebut.

c. *Extrateritory,* Yaitu kewenangan suatu Negara yang diberikan oleh hukum internasional untuk melaksanakan kedaulatannya di wilayah yang tidak termasuk yurisdiksi teritorial dan yurisdiksi kuasi teritorialnya.

d. *Nationality,* prinsip ini berlaku berdasarkan status kewarganegaraan individu, sehingga dalam hal ini yurisdiksi mengikuti status nasionalitas individu.

e. *Protective principle,* asas ini menjelaskan tentang keinginan dari suatu kedaulatan negara untuk mengadili para pihak yang telah menyebabkan gangguan terhadap kekuasaan pemerintah atau negara itu sendiri. dalam asas ini negara menjadi pihak yang dilindungi oleh yurisdiksi tersebut.

f. *Passive nationality,* merupakan suatu teori berdasarkan asas kewarganegaraan dimana pelaku dan korban atas suatu peristiwa hukum memiliki kewarganegaraan yang sama sehingga yang berlaku adalah yurisdiksi negara yang bersangkutan meski peristiwa hukum tersebut terjadi di luar wilayah negara mereka.

g. *Universality,* menurut prinsip ini tiap negara mempunyai yurisdiksi yang sama dalam menangani suatu peristiwa hukum yang berkaitan dengan kepentingan dan kemaslahatan semua negara. Prinsip ini lebih ditekankan pada masalah kejahatan internasional seperti terorisme, kejahatan perang, genosida dan kejahatan terhadap kemanusiaan.

F. Hukum Internasional

Hukum internasional adalah keseluruhan hukum yang untuk sebagian besar terdiri dari prinsip-prinsip dan kaidah-kaidah perilaku yang terhadapnya negara-negara merasa dirinya terikat untuk menaati dan karenanya benar-benar ditaati secara umum dalam hubungan-hubungan mereka satu sama lain, dan yang meliputi juga:

1. Kaidah-kaidah hukum yang berkaitan dengan berfungsinya lembaga-lembaga atau organisasi-organisasi internasional, hubungan-hubungan mereka satu sama lain, dan hubungan mereka dengan negara-negara dan individu-individu
2. Kaidah-kaidah hukum tertentu yang berkaitan dengan individu-individu dan badan-badan non-negara sejauh hak-hak dan kewajiban individu dan badan non-negara tersebut penting bagi masyarakat internasional

Sumber hukum materril hukum internasional menurut pasal 38 (1) *Statute of the International Court of Justice*, yaitu:

1. Traktat-traktat internasional

Traktat atau perjanjian yang diadakan anggota masyarakat bangsa-bangsa dan bertujuan untuk mengakibatkan akibat tertentu. Perjanjian ini harus diadakan oleh subjek hukum internasional yang menjadi anggota masyarakat internasional.

Pengaruh dari suatu traktat atau perjanjian dalam memberi arahan kepada pembentukan kaidah-kaidah hukum internasional bergantung pada sifat hakikat traktat yang bersangkutan. Dalam kaitan ini terdapat dua pembedaan, yaitu :

a. Traktat-traktat "yang membuat hukum" (*law making*), yang menetapkan kaidah-kaidah yang berlaku secara universal dan umum;
b. "traktat-traktat kontrak" (*Treaty contracts*) misalnya, suatu traktat antara dua atau hanya beberapa negara, yang berkenaan dengan suatu pokok permasalahan khusus yang secara eksklusif menyangkut negara-negara ini.

2. Kebiasaan internasional, yang terbukti dari praktek umum telah diterima sebagai hokum

Hukum kebiasaan internasional ialah kebiasaan internasional yang merupakan kebiasaan umum yang diterima sebagai hukum. Untuk dapat dikatakan kebiasaan internasional itu merupakan sumber hukum perlu terdapat unsur-unsur sebagai berikut :

a. Harus terdapat suatu kebiasaan yang bersifat umum (material)
b. Kebiasaan itu harus diterima sebagai hukum (psikologis)

Sebagai sumber hukum, kebiasaan internasional tidak berdiri sendiri. Kebiasaan internasional erat hubungannya dengan perjanjian internasional, dimana hubungan ini adalah hubungan timbal balik. Perjanjian internasional yang berulang kali diadakan mengenai hal yang sama dapat menimbulkan suatu kebiasaan dan menciptakan lembaga hukum.

3. Prinsip-prinsip umum hukum yang diakui oleh bangsa-bangsa beradab

Asas hukum umum ialah asas hukum yang mendasari sistem hukum modern yaitu sistem hukum positif yang didasarkan atas asas dan lembaga hukum negara barat yang untuk sebagian besar didasarkan atas asas dan lembaga hukum romawi. Menurut pasal 38 ayat (1) asas hukum umum merupakan suatu sumber

hukum formal utama yang berdiri sendiri di samping kedua sumber hukum di atas.

4. Keputusan-keputusan pengadilan dan ajaran para sarjana yang terkemuka dari berbagai negara sebagai sumber tambahan untuk menetapkan aturan kaidah hukum

Keputusan pengadilan dan pendapat para sarjana hanya merupakan sumber hukum subsider atau sumber tambahan. Artinya keputusan pengadilan dan pendapat para sarjana dapat dikemukakan untuk membuktikan adanya kaidah hukum internasional mengenai suatu persoalan yang didasarkan atas sumber hukum primer. Keputusan pengadilan dan pendapat para sarjana itu sendiri tidak mengikat, artinya tidak dapat menimbulkan suatu kaidah hukum. Keputusan Mahkamah internasional sendiri tidak mengikat selain bagi perkara yang bersangkutan, maka "*a fortion"* keputusan pengadilan lainnya tidak mungkin mempunyai keputusan yang mengikat.[46]

G. *Convention on Cybercrime*

Convention on Cybercrime merupakan konvensi yang sering menjadi acuan oleh negara-negara yang menjadi pihak dan anggota maupun di luar konvensi ini dalam perancangan undang-undang yang berkaitan dengan teknologi informasi dan kejahatan dunia maya. Banyak negara yang menganut pasal-pasal dalam konvensi tersebut.

[46] Starke J. G., **Pengantar Hukum Internasional**, Sinar Grafika, Jakarta, 2010, hal 65.

Salah satu tantangan utama yang dihadapi dalam penyelidikan kejahatan dunia maya adalah masalah yurisdiksi dan anonimitas.[47] Masalah yurisdiksi berkaitan dengan kegiatan kejahatan ini yang sering melewati batas-batas negara atau akibat hukumnya berada di negara lain.

Dalam menangani kejahatan dunia maya perlu adanya keseragaman hukum antara negara-negara yang terlibat, antara lain dengan mengadopsi peraturan yang tepat guna dan memupuk kerjasama internasional. Menurut Xingan Li *"only an international open approach and cooperation including international standardization process could cobtribute to achive these goals"*[48]

Dalam pendahuluan *Convention on Cybercrime* dijelaskan salah satu tujuan utama konvensi tersebut adalah "*Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting approriate legislation and fostering international co-operation"*.[49] Secara implisit pernyataan tersebut menjelaskan perlunya kerja sama internasional dalam menangani kejahatan dunia maya dengan mengharmonisasi hukum-hukum domestik di Eropa.

Tujuan kerja sama tersebut adalah:

1. Meningkatkan kesadaran akan keamanan pada tingkat internasional
2. Meningkatkan kesadaran akan keamanan pada tingkat nasional
3. Mengaharmonisasikan perundang-undangan
4. Melakukan koordinasi dan kerja sama dalam bidang penegakan hukum.

---

[47] Deb Shinder, 2011, ***What Makes Cybercrime Laws so Difficult to Enforce*** (online), http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/, (23 November 2013).

[48]Stein Schjolberg, solange Ghernaouti-Helie, ***A Global Treaty on Cybersecurity and Cybercrime***, Josua Sitompul, op cit, hal 104.

[49]Convention Committe on Cybercrime, ***Convention on Cybercrime***, Budapest, Council of Europe, 2001, hal 1.

Terdapat beberapa asas yang digunakan dalam konvensi ini, yaitu:

1. Universal

Pihak-pihak dalam konvensi berhak menerapkan hukum pidananya terhadap pelaku tindak pidana dengan permintaan ekstradisi dengan syarat tindakan tersebut merupakan suatu tindak pidana di kedua negara. Apabila negara-negara yang terlibat mensyaratkan ekstradisi hanya bisa dilakukan jika ada perjanjian ekstradisi, konvensi ini dapat dijadikan landasan hukum.

2. *Dual Criminality* (Kriminalitas Ganda)

Dual criminality (kriminalitas ganda) adalah merupakan kejahatan atau peristiwa pidana menurut sistem hukum kedua pihak (negara pemohon dan termohon).[50] Asas ini tertuang dalam pasal 25 ayat 5 "*Where, in accordance with the provisions of this chapter, the requested party is permitted to make mutual assistance conditional upon the existence of dual criminality...*".[51]

Asas ini digunakan dalam konvensi sebagai dasar pelaksanaan ekstradisi dan *mutual legal assistance* dalam proses penyidikan.[52]

3. *Electronic Evidence* (Bukti Elektronik)

Bukti elektronik dianggap bukti yang sah oleh konvensi ini. Konvensi ini menyadari bahwa jaringan komputer dan informasi elektronik dapat digunakan untuk melakukan tindak pidana dan bukti-bukti tindak pidana tersebut dapat disimpan dan dikirim melalui jaringan tersebut.

---

[50] Elisatris Gultom, 2010, ***Mutual Legal Assistance* dalam Kejahatan Transnasional Terorganisasi** (online), http://elisatris.wordpress.com/mutual-legal-assistance-dalam-kejahatan-transnasional-terorganisasi/, (15 Desember 2013).

[51] Convention Committe on Cybercrime, ***Convention on Cybercrime***, Budapest, Council of Europe, 2001.

[52] Albert Rees, ***International Cooperation in Cybercrime Investigation***, makalah disajikan dalam OAS Regional Cyber Crime Workshop, Criminal Divisions, U.S. Department of Justice, April 2007, hal 5.

Konvensi juga mengharuskan negara yang terikat dengan konvensi untuk membentuk kewenangan-kewenangan dan prosedur pelaksanaannya untuk pengumpulan bukti elektronik dari suatu tindak pidana demi keperluan penyidikan.

Dalam bagian 2 tentang hukum acara formil konvensi ini mengatur kewajiban negara anggota untuk menerapkan undang-undang untuk membentuk kewenangan-kewenangan otoritas yang ditunjuk maupun yang berasal dari negara lain untuk tujuan penyidikan.

Bab III pasal 23-35 konvensi ini mengatur tentang kerjasama internasional, meliputi ekstradisi, bantuan saling menguntungkan (*mutual assistance*), informasi spontan, persyaratan tentang permintaan bantuan tanpa perjanjian internasional serta bantuan mengenai kewenangan penyidikan

Convention on Cybercrime dibuka untuk ditandatangi oleh negara-negara anggota sejak 23 November 2001, namun mulai berlaku pada tahun 2004.[53] Menurut Pasal 36 (4) *Convention on Cybercrime:*

> *"In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention."*[54]

Menurut pasal tersebut, konvensi mulai berlaku di negara-negara yang telah terikat dalam konvensi pada hari pertama dalam bulan pertama setelah berakhirnya periode tiga bulan setelah tanggal persetujuan tersebut diberikan.

Konvensi ini juga terbuka bagi negara-negara non-anggota. Sampai saat ini, telah ada empat puluh tiga negara anggota *Council of Europe* yang

[53] Maskun, op cit, hal 107.
[54] Convention Committe on Cybercrime, op cit.

menandatangani konvensi tersebut, dari negara-negara yang menandatangani konvensi, tiga puluh dua negara telah meratifikasinya. Selain itu, negara-negara non-anggota *Council of Europe* yang menandatangani *Convention on Cybercrime* ialah Kanada, Jepang, Afrika Selatan, Amerika Serikat dan Australia.

H. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan undang-undang pertama di Indonesia yang secara khusus mengatur tindak pidana siber. Undang-undang ini memiliki sejarah tersendiri dalam pembentukan dan pengundangannya. Rancangn UU ITE mulai dibahas sejak Maret 2003 oleh Kementerian Negara Komunikasi dan Informatika dengan nama Rancangan UU Informasi Komunikasi dan Transaksi Elektronik. Pada awalnya, RUU ini merupakan penyatuan dua rancangan undang-undang yang disusun oleh dua kementerian, yaitu Departemen Perhubungan dan Departemen perindustrian dan Perdagangan, bekerja sama dengan Lembaga Kajian Hukum dan Teknologi Universitas Indonesia, Tim dari fakultas Hukum Universitas Padjajaran, serta Tim Asistensi dari ITB. Kemudian berdasarkan Surat Presiden RI. No.R./70/Pres/9/2005 naskah UU ITE secara resmi disampaikan kepada DPR RI. Pada tanggal 21 April 2008, undang-undang ini disahkan.

Tujuan dari undang-undang ini terdapat pada pasal 4, yaitu:

a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;

b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
c. meningkatkan efektifitas dan efisiensi pelayanan publik;
d. membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

Terdapat beberapa asas di dalam undang-undang ini, yaitu :

1. Asas Kepastian Hukum

   Asas ini menegaskan bahwa undang-undang ini merupakan landasan hukum bagi pemanfaatan teknologi informasi dan transaksi elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.

2. Asas Manfaat

   Pemanfaatan teknologi informasi dan transaksi elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat.

3. Asas Kehati-hatian

   Landasan bagi pihak yang bersangkutan harus memerhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan teknologi informasi dan transaksi elektronik.

4. Asas Iktikad Baik

Asas yang digunakan para pihak dalam melakukan transaksi elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum yang mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.

5. Asas Kebebasan Memilih Teknologi Netral Teknologi

Asas pemanfaatan teknologi informasi dan transaksi elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

6. Asas Ekstrateritorial

Berdasarkan pasal 2, UU ITE beserta ancaman-ancaman pidananya berlaku bagi :

a) Orang (yaitu orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum dalam wilayah hukum Indonesia.
b) Orang (WNI, WNA, badan hukum) di luar wilayah hukum Indonesia, dan perbuatan tersebut memiliki akibat hukum di wilayah hukum Indonesia atau memiliki akibat hukum di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.