1. Adanya paksaan dari luar (sanksi) dari penguasa yang bertugas mempertahankan dan membina tata tertib masyarakat dengan perantara alat -alatnya;
2. Sifat undang-undang yang berlaku bagi siapa saja.

B. Asas Legalitas

Tindak pidana berasal dari suatu istilah dalam hukum belanda yaitu *strafbaarfeit*. Ada pula yang mengistilahkan menjadi delict yang berasal dari bahasa latin *delictum*. Hukum pidana negara anglosaxon memakai istilah *offense* atau *criminal act*. Oleh karena itu KUHP Indonesia bersumber pada *Wetboek van Strafrecht* Belanda, maka memakai istilah aslinya pun sama yaitu *Strafbaarfeit*.[9]

Pemakaian istilah tindak pidana dan kejahatan seringkali mengalami kerancuan dan tumpang tindih dalam pemakaiannya. Istilah yang dipakai dalam rumusan pasal-pasal yang ada dalam KUHP adalah istilah tindak pidana, walaupun Buku kedua bertitel kejahatan. Dalam hukum pidana sendiri istilah tindak pidana dikenal dengan strafbaarfeit dan memiliki penjelasan yang berbedabeda akan tetapi intinya sama yaitu peristiwa pidana atau sebagai tindak pidana. Menurut van Hamel, *strafbaarfeit* adalah kelakuan orang yang dirumuskan dalam *wet* atau undang-undang yang bersifat melawan hukum yang patut dipidana (*strafwaardig*) dan dilakukan dengan kesalahan.[10]

Menurut P. Simons yang menggunakan istilah peristiwa pidana adalah perbuatan atau tindakan yang diancam dengan pidana oleh undang-

[9] Andi Hamzah, Asas-Asas Hukum Pidana, Rineka Cipta, Jakarta,2008, hlm. 84.
[10] Moeljatno, Asas-Asas Hukum Pidana, Rineka Cipta, Jakarta, 2008, hlm. 56.

undang, bertentangan dengan hukum dan oleh orang yang mampu bertanggung jawab.[11] Simon memandang semua syarat untuk menjatuhkan pidana sebagai unsur tindak pidana dan tidak memisahkan unsur yang melekat pada perbuatannya (*crime act*) tindak pidana dengan unsur yang melekat pada aliran tindak pidana (*criminal responsibility* atau *criminal liability* atau pertanggung jawaban pidana). Kemudian dia menyebut unsur-unsur tindak pidana, yaitu manusia, diancam dengan pidana, melawan hukum, dilakukan dengan kesalahan, oleh orang yang mampu bertanggung jawab.

Unsur-unsur tersebut oleh Simon dibedakan antara unsur obyektif dan unsur subyektif. Unsur obyektif adalah perbuatan orang, akibat yang kelihatan dari perbuatan itu, dan kemungkinan adanya keadaan tertentu yang menyertainya. Unsur subyektif berupa keadaan orang yang mampu bertanggung jawab dan adanya kesalahan.[12]

Moeljatno memberikan pengertian tentang perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, barang siapa melanggar larangan tersebut. Larangan tersebut ditujukan kepada perbuatan, sedangkan ancaman pidananya ditujukan pada orang yang menimbulkan kejadian itu. Moeljatno memisahkan antara *criminal act* dan *criminal responsibility* yang menjadi unsur tindak pidana.[13]

---

[11] Ibid., hlm. 58.
[12] Masruchin Ruba'i – Made S. Astuti Djazuli, Hukum Pidana 1, Jurusan Hukum Pidana Fakultas Hukum Universitas Brawijaya, Malang, 1989, hlm 35.
[13] Moeljatno. Op. Cit. hlm. 59.

Menurut Moeljatno hanyalah unsur-unsur yang melekat pada *criminal act* (perbuatan yang dapat dipidana). Sedangkan yang termasuk unsur-unsur tindak pidana adalah perbuatan (manusia), memenuhi rumusan Undang-undang, bersifat melawan hukum.[14] Menurut C. S. T. Kansil, hukum pidana adalah peraturan atau hukum yang mengatur tentang pelanggaran-pelanggaran dan kejahatan-kejahatan terhadap kepentingan umum, dan bagi pelanggarnya diancam dengan hukuman yang merupakan seuatu penderitaan dan siksaan dengan tujuan menimbulkan efek jera pada penerima sanksi tersebut.[15]

Hukum pidana merupakan bagian keseluruhan hukum yang berlaku di suatu negara, yang menjelaskan dasar-dasar dan aturan untuk:[16]

a) Menentukan perbuatan-perbuatan mana yang tidak boleh dilakukan, yang dilarang dengan disertai ancaman atau sanksi yang berupa pidana tertentu bagi yang melanggarnya.
b) Menentukan kapan dan dalam hal-hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dijatuhi pidana.
c) Menetukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut.

Dalam hukum pidana ini terdapat asas legalitas yang menurut prof. Moeljatno memiliki tiga pengertian, yaitu :

[14] Ibid., hlm. 59.
[15] C.S.T. Kansil, *Loc. Cit.*
[16] Moeljatno, *Op. Cit*, hlm. 1.

1) Tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam sebuah undang-undang.
2) Untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi.
3) Aturan-aturan hukum pidana tidak berlaku surut.[17]

Karena penerapan hukum pidana atau suatu perundang-undangan pidana berkaitan dengan waktu dan tempat perbuatan dilakukan,[18] maka hukum pidana kemudia dikenal dengan asas-asas tentang batas berlakunya hukum pidana menurut waktu dan tempat. Berkaitan dengan berlakunya hukum pidana menurut waktu, penulis akan membahas mengenai asas yang berlaku didalamnya yaitu asas yang terkenal dengan sebutan asas legalitas (*principle of legality)*.

Asas legalitas dalam hukum pidana merupakan asas yang sangat fundamental. Asas legalitas dalam hukum pidana begitu penting untuk menentukan apakah suatu peraturan hukum pidana dapat diberlakukan terhadap tindak pidana yang terjadi. Jadi, apabila terjadi suatu tindak pidana maka akan dilihat apakah telah ada ketentuan hukum yang mengaturnya dan apakah aturan yang telah ada tersebut dapat diberlakukan terhadap tindak pidana yang terjadi.[19] Jadi singkatnya asas legalitas tersebut berkaitan dengan waktu berlakunya hukum pidana.

[17] Ibid., hlm. 28.
[18] Andi Hamzah, *Op. Cit*, hlm. 27
[19] A. Fuad Usfa dan Tongat, Pengantar Hukum Pidana, UMM Press, Malang, 2004, hlm. 9.

C. Asas Hukum Pidana

Penerapan hukum pidana atau suatu perundang-undangan pidana berkaitan dengan waktu dan tempat perbuatan dilakukan. Serta berlakunya hukum pidana menurut waktu menyangkut penerapan hukum pidana dari segi lain. Dalam hal seseorang melakukan perbuatan *(feit)* pidana sedangkan perbuatan tersebut belum diatur atau belum diberlakukan ketentuan yang bersangkutan, maka hal itu tidak dapat dituntut dan sama sekali tidak dapat dipidana. [20]

Berlakunya hukum pidana menurut ruang tempat dan berkaitan dengan orang atau subyek. Dalam hal ini asas-asas hukum pidana menurut tempat dibagi menjadi: [21]

1. Asas Teritorial

Asas ini diatur juga dalam Kitab Undang-Undang Hukum Pidana (KUHP) yaitu dalam pasal 2 KUHP yang menyatakan: "*Ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan suatu tindak pidana di Indonesia". Perluasan dari Asas* Teritorialitas diatur dalam pasal 3 KUHP yang menyatakan: "Ketentuan pidana perundang-undangan Indonesia berlaku bagi setiap orang yang di luar wilayah Indonesia melakukan tindak pidana didalan kendaraan air atau pesawat udara Indonesia".

Tujuan dari pasal ini adalah supaya perbuatan pidana yang terjadi di dalam kapal atau pesawat terbang yang berada di perairan

[20] Buku modul asas-asas hukum pidana

[21] https://masalahukum.wordpress.com/2013/09/01/asas-asas-dalam-hukum-pidana/

bebas atau berada di wilayah udara bebas, tidak termasuk wilayah territorial suatu Negara, sehingga ada yang mengadili apabila terjadi suatu perbuatan pidana.

2. Asas Personal (nasional aktif)

Yakni apabila warganegara Indonesia melakukan ke-jahatan meskipun terjadi di luar Indonesia, pelakunya dapat dikenakan hukum pidana Indonesia, apabila pelaku kejahatan yang hanya dapat dikenakan hukum pidana Indonesia, sedangkan perbuatan pidana yang dilakukan warganegara Indonesia di negara asing yang telah menghapus hukuman mati, maka hukuman mati tidak dapat dikenakan pada pelaku kejahatan itu, hal ini diatur dalam pasal 6 KUHP.

3. Asas Perlindungan (nasional pasif)

Tolak pangkal pemikiran dari asas perlindungan adalah bahwa setiap negara yang berdaulat wajib melindungi kepentingan hukumnya atau kepentingan nasionalnya. Ciri utamanya adalah Subjeknya berupa setiap orang tidak terbatas pada warga negara saja, selain itu tidak tergantung pada tempat, ia merupakan tindakan-tindakan yang dirasakan sangat merugikan kepentingan nasional indonesia yang karenanya harus dilindungi. Kepentingan nasional tersebut ialah:

a) Keselamatan kepala/wakil Negara RI, keutuhan dan keamanan negara serta pemerintah yang sah, keamanan

penyerahan barang, angkatan perang RI pada waktu perang, keamanan Martabat kepala negara RI.

b) Keamanan ideologi negara, pancasila dan haluan negara.
c) Keamanan perekonomian.
d) Keamanan uang negara, nilai-nilai dari surat-surat yang dikeluarkan RI.
e) Keamanan pelayaran dan penerbangan terhadap pembajakan.

Tolak pangkal pemikiran dari asas perlindungan adalah bahwa setiap negara yang berdaulat wajib melindungi kepentingan hukumnya atau kepentingan nasionalnya. Ciri utamanya adalah subjeknya berupa setiap orang tidak terbatas pada warga negara saja, selain itu tidak tergantung pada tempat, ia merupakan tindakan-tindakan yang dirasakan sangat merugikan kepentingan nasional indonesia yang karenanya harus dilindungi. Kepentingan nasional tersebut ialah:

a) Keselamatan kepala/wakil Negara RI, keutuhan dan keamanan negara serta pemerintah yang sah, keamanan penyerahan barang, angkatan perang RI pada waktu perang, keamanan Martabat kepala negara RI;
b) Keamanan ideologi negara, pancasila dan haluan Negara;
c) Keamanan perekonomian;
d) Keamanan uang Negara, nilai-nilai dari surat-surat yang dikeluarkan RI;
e) Keamanan pelayaran dan penerbangan terhadap pembajakan.

4. Asas Universal

Asas universal adalah asas yang menyatakan setiap orang yang melakukan perbuatan pidanan dapat dituntut undang-undang hukum pidana Indonesia di luar wilayah Negara untuk kepentingan hukum bagi seluruh dunia. Asas ini melihat hukum pidanan berlaku umum, melampaui batas ruang wilayah dan orang, yang dilindungi disini ialah kepentingan dunia. Jenis kejahatan yang dicantumkan pidanan menurut asas ini sangat berbahaya tidak hanya dilihat dari kepentingan Indonesia tetapi juga kepentingan dunia. Secara universal kejahatan ini perlu dicegah dan diberantas.

D. Pengertian *Cybercrime*

Cybercrime berasal dari kata *cyber* yang berarti dunia maya atau internet dan *crime* yang berarti kejahatan.[22] Dengan kata lain, *cybercrime* adalah segala bentuk kejahatan yang terjadi di dunia maya atau internet. *Cybercrime* merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama.[23] *Cybercrime* yaitu kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.[24] Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime*. Andi Hamzah dalam buku Aspek-aspek Pidana di Bidang Komputer (1989)

[22] Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: PT Citra Aditya Bakti, 2002).
[23] Ibid.
[24] Budi Raharjo, *Memahami Teknologi Informasi*. (Jakarta: Elexmedia Komputindo, 2002). hlm 23.

mengartikan: “kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal.”

Cybercrime adalah perbuatan kriminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Dengan kata lain, *Cybercrime* yaitu kejahatan yang memanfaatkan perkembangan teknologi computer khususnya internet. Dengan demikian *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer berbasasis pada kecanggihan dan perkembangan teknologi internet. *Cybercrime* memiliki karakter yang khas dibandingkan kejahatan konvensional, antara lain: [25]

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya *(cyberspace)*, sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.
c. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional.
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. Perbuatan tersebut seringkali dilakukan secara transnasional/ melintasi batas Negara.

[25] Deris Setiawan, *Sistem Keamanan Komputer, (*Jakarta: PT Elex Media Komputindo, 2005),.hlm. 40.

Pengaturan *CyberCrime* di Indonesia Indonesia belum memiliki Undang-Undang khusus/*cyber law* yang mengatur mengenai *cybercrime.* Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, diantaranya:[26]

a. Kitab Undang-Undang Hukum Pidana. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cybercrime* yaitu:

   1. Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di Internet untuk melakukan transaksi di *ecommerce*. Setelah dilakukan transaksi dan barang dikirimkan kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.
   2. Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut

[26] ibid, hlm. 70-77.

diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

3. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.
4. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan *email* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.
5. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di Internet dengan penyelenggara dari Indonesia.
6. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang terlarang atau illegal.

7. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet, misalnya kasus-kasus video porno para mahasiswa, pekerja atau pejabat publik.
8. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
9. Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

b. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta. Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 30). Harga *program computer / software* yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan harga

yang sangat murah. Misalnya, program *antivirus* seharga $ 50 dapat dibeli dengan harga Rp 20.000,00. Penjualan dengan harga sangat murah dibandingkan dengan *software* asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 per keping. Maraknya pembajakan *software* di Indonesia yang terkesan dimaklumi tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah)."

c. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi atau UndangUndang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik. Menurut Pasal 1 angka (1) Undang - Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu

ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang- Undang ini, terutama bagi para hacker yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

1. Akses ke jaringan telekomunikasi
2. Akses ke jasa telekomunikasi
3. Akses ke jaringan telekomunikasi khusus.

d. Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang. Undang-Undang Nomor 15 Tahun 2002 merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan.

Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan

waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan.[27] Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Dengan semakin pesatnya perkembangan teknologi informasi, maka perlu kiranya diperhatikan upaya penyempurnaan dan perbaikan Kitab Undang-Undang Hukum Pidana Nasional, yaitu:[28]

1. Semakin maraknya kejahatan-kejahatan baru yang timbul sebagai akibat dari kemajuan teknologi informasi *(cybercrime),* maka alat bukti yang diperlukan harus sesuai dengan perkembangan IPTEK, baik dengan penambahan alat bukti lain yang berbasis teknologi, seperti alat bukti berupa surat elektronik *(electronic mail)* dan rekaman elektronik.

[27] *Buletin Hukum Perbankan Dan KeBanksentralan* Volume 4 Nomor 2, Agustus 2006.
[28] Hinca IP Panjaitan dkk, 2005, *Membangun Cyber Law Indonesia yang demokratis*, Jakarta : IMLPC. Hlm 56-58.

2. Salah satu ciri kejahatan di dunia maya *(cybercrime)* adalah memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global. Aspek global menimbulkan kondisi seakan-akan dunia tidak ada batasnya *(borderless)* keadaan ini mengakibatkan pelaku, korban serta tempat dilakukannya tindak pidana *(locus delicti)* terjadi dinegara yang berbedabeda. Oleh karena itu, untuk mengantisipasi hal tersebut maka pemberlakuan Kitab Undang-Undang Hukum Pidana harus diperluas, sehingga tidak hanya mengacu pada asas/ prinsip yang selama ini di anut dalam pasal 2-pasal 9 Kitab Undang-Undang Hukum Pidana yaitu asas personal, asas territorial, dan asas universal.
3. Untuk merumuskan dan menentukan perbuatan-perbuatan yang dapat dikenai sanksi pidana dalam dunia yang *relative* baru dan bergerak cepat, tentu bukan merupakan pekerjaan yang mudah. Oleh karena itu, untuk menjerat pelaku yang melakukan kejahatan-kejahatan di dunia maya *(cybercrime)* dapat digunakan lembaga penafsiran hukum (interpretasi). Hal ini dimaksudkan untuk menghindarkan timbulnya kekosongan hukum. Dikenal adanya beberapa asas yang dapat digunakan, yaitu :
    a. *Subjective territoriality*, yang menekankan bahwa keberlakuan hukum pidana ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.

b. *Objective territoriality*, yang menyatakan bahwa hukum yang berlaku adalah akibat utamanya perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.

c. *Nationality*, yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku tindak pidana.

d. *Passive nationality*, yang menekankan yurisdiksi berdasarkan kewarganegaraan dari korban kejahatan.

e. *Protective principle*, yang menyatakan bahwa berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya. Azas ini pada umumnya diterapkan apabila korbannya adalah negara atau pemerintah.

f. *Universality*, bahwa setiap negara berhak untuk menangkap dan menghukum pelaku kejahatan. Munculnya kejahatan *cybercrime* merupakan suatu fenomena yang membutuhkan penanggulangan secara cepat dan akurat. Perubahan terhadap beberapa ketentuan yang terdapat dalam Kitab Undang-Undang Hukum Pidana merupakan salah satu cara yang dapat dipergunakan untuk mengatasi jenis kejahatan baru tersebut. Diharapkan dengan dilakukannya berbagai perubahan dalam Kitab Undang Hukum Pidana Nasional sebagai akibat dari timbulnya berbagai perubahan.

E. Kasus *Cybercrime* di Indonesia

a. Pencurian dan penggunaan account Internet milik orang lain. Di antara kesulitan dari sebuah ISP *(Internet Service Provider)* adalah adanya *account* pelanggan mereka yang "dicuri" dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, "pencurian" *account* cukup menangkap "*userid*" dan "*password*" saja. Hanya informasi yang dicuri. Sementara orang yang kecurian tidak merasakan hilangnya "benda" yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunaan dibebani biaya penggunaan *account* tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan *account* curian oleh dua warnet di Bandung.

b. Membajak situs web. Salah satu kegiatan yang sering dilakukan oleh *cracker* adalah mengubah halaman web, yang dikenal dengan istilah *deface*. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya.

c. *Probing* dan *port scanning*. Salah satu langkah yang dilakukan *cracker* sebelum masuk ke *server* target yaitu melakukan pengintaian, dengan cara melakukan *"port scanning"* atau *"probing"* untuk melihat servis-servis apa saja yang tersedia di *server* target. Misalnya, hasil *scanning* dapat menunjukkan bahwa *server* target menjalankan program *web server Apache, mail server*

send mail, dan seterusnya. Analogi hal ini dengan dunia nyata yaitu dengan melihat-lihat apakah pintu rumah target terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan *firewall* atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan.

d. Virus. Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia. Penyebaran umumnya dilakukan dengan menggunakan *email*. Seringkali sistem email seseorang yang terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui *email*nya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, *I love you*, dan *SirCam*. Untuk orang yang terkena virus, kemungkinan tidak banyak yang dapat dilakukan.

e. *Denial of Service (DoS)* dan *Distributed DoS (DDos) attack.*. *DoS attack* merupakan serangan yang bertujuan untuk melumpuhkan target *(hang, crash)* sehingga dia tidak dapat memberikan layanan. Aktifitas serangannya tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari *DoS attack* ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank termasuk nasabah dapat mengalami kerugian finansial. *DoS attack*

dapat ditujukan kepada *server* (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan *bandwidth*). *Tools* untuk melakukan hal ini banyak tersebar di Internet. *DDoS attack* meningkatkan serangan ini dengan melakukannya dari beberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari *DoS attack* saja.

f. Kejahatan yang berhubungan dengan nama domain *(domain name)* digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah *cybersquatting.* Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat "domain plesetan", yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah *typosquatting.*

g. IDCERT *(Indonesia Computer Emergency Response Team).* Salah satu cara untuk mempermudah penanganan masalah keamanan dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya *"sendmail worm"* (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk

sebuah *Computer Emergency Response Team (CERT).* Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact* bagi orang untuk melaporkan masalah keamanan. IDCERT merupakan CERT Indonesia.

h. Sertifikasi perangkat *security.* Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia.[29] *Cybercrime* membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Adapun langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cybercrime* adalah:[30]

a) Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.

b) Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

c) Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan

[29] http://www.gatra.com/2004-10-13/. *Cybercrime di Era Digital.* Diakses 13 Juli 2020 pukul 21.18

[30] http://budi.insan.co.id. *Keamanan Sistem Informasi Berbasis Internet*. Diakses 14 Juli Pukul 12.43.

penuntutan perkara-perkara yang berhubungan dengan *cybercrime*.

d) Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya upaya pencegahan kejahatan agar tidak mudah terjadi.

e) Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan mutual *assistance treaties*. Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika dan ketiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi atau diakses secara ilegal dan tanpa hak.[31]

F. Pengaturan Tindak Pidana Siber di Indonesia

1. Pengaturan Tindak Pidana Siber Materil di Indonesia

Pengaturan tindak pidana siber di Indonesia dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana sepanjang dengan menggunakan bantuan atau sarana sistem

[31] Ahmad, Ramli. *Prinsip-prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, (Bandung: Fakultas Hukum Universitas Padjajaran, 2004), hlm. 2.

elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana maupun tindak pidana perbankan serta tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sama halnya seperti *Convention on Cybercrimes*. UU ITE juga tidak memberikan definisi mengenai *cybercrimes*, tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada *Convention on Cybercrimes*.

(1) Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:

a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari:

1) Kesusilaan (Pasal 27 ayat (1) UU ITE);

2) Perjudian (Pasal 27 ayat (2) UU ITE);

3) penghinaan dan/atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE);
4) pemerasan dan/atau pengancaman (Pasal 27 ayat (4) UU ITE);
5) berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE);
6) menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE);
7) mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);

b. Dengan cara apapun melakukan akses illegal (Pasal 30 UU ITE);

c. Intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 Undang-Undang Nomor 19 Tahun 2016)

(2) Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:

a. Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* - Pasal 32 UU ITE);

b. Gangguan terhadap Sistem Elektronik (*system interference* –Pasal 33 UU ITE);

1) Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);

2) Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);

3) Tindak pidana tambahan (*accessoir* Pasal 36 UU ITE); dan

4) Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE).

2. Pengaturan Tindak Pidana Siber Formil di Indonesia

Selain mengatur tindak pidana siber materil, UU ITE mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana dan ketentuan dalam UU ITE. Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain:

1. Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil (PPNS) Kementerian Komunikasi dan Informatika.
2. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data.

3. Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana.
4. Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Ketentuan penyidikan dalam UU ITE dan perubahannya berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE dan perubahannya. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan.

Adapun prosedur untuk menuntut secara pidana terhadap perbuatan tindak pidana siber, secara sederhana dapat dijelaskan sebagai berikut:

1. Korban yang merasa haknya dilanggar atau melalui kuasa hukum, datang langsung membuat laporan kejadian kepada penyidik POLRI pada unit/bagian *Cybercrime* atau kepada penyidik PPNS pada Sub Direktorat Penyidikan dan Penindakan, Kementerian Komunikasi dan Informatika. Selanjutnya, penyidik akan melakukan penyelidikan yang dapat

dilanjutkan dengan proses penyidikan atas kasus bersangkutan Hukum Acara Pidana dan ketentuan dalam UU ITE.

2. Setelah proses penyidikan selesai, maka berkas perkara oleh penyidik akan dilimpahkan kepada penuntut umum untuk dilakukan penuntutan di muka pengadilan. Apabila yang melakukan penyidikan adalah PPNS, maka hasil penyidikannya disampaikan kepada penuntut umum melalui penyidik POLRI.