BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Tidak dapat dipungkiri, perkembangan ilmu pengetahuan diikuti oleh teknologi. Perkembangan teknologi dimanfaatkan untuk mendorong pertumbuhan bisnis yang begitu pesat. Informasi tersajikan dalam waktu yang begitu cepat. Hanya dengan memanfaatkan teknologi komunikasi, bisnis antar negara dapat dilakukan tanpa perlu bertemu *face to face.*[1] Inilah tanda bahwa era *cyber* dalam bisnis telah dimulai. Selain menguntungkan pelaku bisnis, perkembangan teknologi juga memudahkan untuk mendapatkan informasi, dan berdampak juga terhadap sektor ekonomi, politik, budaya serta hukum suatu negara.

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer. [2]

---

[1] Niniek Suparni, *Cyberspace Problematika & Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009, hlm. 1.

[2] A. Rahmah dan Amiruddin Pabbu, *Kapita Selekta Hukum Pidana*, Mitra Wacana Media, Jakarta, 2015, hlm. 1.

Seiring dengan perkembangan teknologi internet, kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan tercepat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia bisa diketahui selama 24 jam. Melalui dunia internet, apapun dapat dilakukan. Segi positif dunia maya ini tentu saja menambah *trend* perkembangan teknologi dunia sebagai segala bentuk kreatifitas manusia.[3]

Perkembangan paling mutakhir dari teknologi komputer adalah berupa *computer network,* yaitu *time sharing*, konsep yang menghubungkan sejumlah besar pengguna terhadap suatu *single computer* melalui *remote terminal* yang dibangun oleh MIT (*Massachusetts Institute of Technology*) pada tahun 1950-an dan permulaan tahun 1960.[4] Kemudian melahirkan suatu ruang komunikasi dan informasi global yang dikenal dengan internet. Perkembangan yang pesat dalam pemanfaatan jasa internet ternyata tidak saja membawa dampak positif, juga mengundang terjadinya kejahatan. Di dunia internasional, kejahatan tersebut lebih dikenal dengan nama *cybercrime* yang merupakan bentuk dari perkembangan *computer crime*.[5]

David Baindbridge dalam bukunya *Introduction to Computer Law* menjelaskan bahwa perkembangan internet berdampak pada munculnya kejahatan komputer seperti *website spoof* (orang memesan barang atau jasa melalui *website*, namun setelah dilakukan pembayaran, ternyata barangnya tidak ada), mendapatkan

---

[3] Edmon Makarim, *Pengantar Hukum Telematika*, Rajagrafindo Perkasa, Jakarta, 2005, hlm. 31.

[4] Niniek Suparni, *Op.Cit.* hlm. 4.

[5] A. Rahmah dan Amiruddin Pabbu, *Op.cit*. hlm1-2.

akses ke data penting atau data sensitif, men-*download* atau mengirimkan informasi atau gambar yang tidak pantas, men-*download software* yang tidak sah dan virus yang berbahaya. Lebih lanjut, Baindbridge menjelaskan inilah salah satu persoalan yang melatarbelakangi pertemuan Dewan Konvensi Eropa tentang *Cybercrime*.[6]

> *"Potential risks are spoof websites inviting orders for non-existent goods or services, getting access to critical or sensitive data, downloading or sending inappropriate information or images, downloading unauthorised software and the ever-present dangers of viruses. In addressing these and other issues, the Council of Europe Convention on Cybercrime (Budapest, 23 November 2001) has been signed by a large number of member states of the Council of Europe and some non-member states, being Canada, Japan, South Africa and the United States. The Convention, claimed to be the first international response to cybercrime, will enter into force when ratified by five states, including at least three member states of the Council of Europe."*(Hal yang berpotensi yaitu website penipu yang mengundang untuk pelayanan yang tidak ada, mendapatkan akses atau data yang sesitif, mengunduh atau mengirim informasi dan gambar yang tidak pantas, mengunduh software yang tidak sah dan virus yang berbahaya. Dalam menanganinya dan isu lainnya, Dewan Konvensi Eropa tentang *Cybercrime* (Budapest, 23 November 2001) yang ditandatangani oleh sejumlah besar anggota Dewan Eropa dan beberapa negara bukan anggota, seperti Kanada, Jepang, Afrika Selatan dan Amerika Serikat. Konvensi ini merupakan konvensi pertama mengenai *cybercrime*, akan berlaku ketika diratifikasi oleh lima negara, termasuk tiga negara anggota Dewan Eropa".)

Pada Konvensi Eropa tentang *cybercrime* para pihak sepakat untuk melakukan kriminalisasi terhadap perbuatan tertentu dan meminta para pihak untuk mengadopsi dan menjadikan perbuatan tersebut sebagai tindak pidana, sebagaimana yang dijelaskan oleh Baindbridge:

> *As at 30 July 2003, there were three ratifications. The main provisions as to the criminalisation of the certain activities committed intentionally require parties to the Convention to adopt legislative and other measures to establish criminal offences in respect of the following: illegal access (hacking); illegal*

[6] David Bainbridge, *Introduction to Computer Law, Fifth Edition*, Pearson Education Limited, England, 2004, hlm. 362

interception; interference with data and systems; misuse of devices designed or adapted for committing any of the above and in relation to passwords, access codes and similar data, computer-related forgery and fraud; child pornography in relation to computer systems, and; commercial infringement of copyright and related rights by means of a computer system.[7] *(*Pada tanggal 3 Juli 2003, ada tida ratifikasi. Ketentuan utama kriminalisasi untuk kegiatan tertentu yang dilakukan dengan sengaja meminta para pihak dari Konvensi untuk mengadopsi langkah-langkah legislatif dan lainnya untuk membangun tindak pidana sebagaimana berikut; akses ilegal; intersepsi ilegal;; gangguna data; penyalahgunaan perangkat, kode akses dan data yang sama, pemalsuan komputer dan penipuan; kegiatan yang berkaitan dengan pornografi anak, dan; pelanggaran hak cipta.)

Terkait dengan *cybercrime* itu sendiri, Petrus Reinhard Golose, dalam makalahnya yang berjudul Perkembangan *Cybercrime* dan Upaya Penanganannya di Indonesia Oleh Polri, menyebutkan definisi *computer crime* menurut *US Department of Justice* yaitu "*any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution".*[8] Mengenai pengertian *cybercrime* terdapat dalam *Eight United Nations Congress On The Prevention of Crime and The Treatment of Offlenderes* di Havana, Cuba tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada dua istilah *cybercrime.* Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut[9]:

---

[7] *Ibid*, hlm. 363

[8] Petrus Reinhard Golose, Perkembangan *Cybercrime* dan Upaya Penanganannya di Indonesia Oleh Polri, Makalah pada Seminar Nasional tentang "Penanganan Masalah *Cybercrime* di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh Terpadu", diselenggarakan di Menara Sjafruddin Prawiranegara Kompleks Perkantoran Bank Indonesia Jakarta, 10 Agustus 2006, dalam H.M. Arsyad Sanusi, *Cyber Crime*, Milestone, Jakarta, 2011, hlm. 166.

[9] *Ibid,* hlm. 168.

1. *Cyber crime in a narrow sense* (*computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them.* (*Cybercrime* dalam arti sempit adalah setiap tindakan ilegal yang dilakukan menggunakan peralatan elektronik yang ditujukan pada keamanan sistem komputer dan pemrosesan data yang menggunakan komputer.)
2. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.* (*Cybercrime* dalam arti luas disebut juga kejahatan yang berhubungan dengan komputer, yaitu setiap perilaku ilegal yang memanfaatkan komputer atau sistem jaringan, termasuk kejahatan tertentu dalam menyimpan, menawarkan, atau mendistribusikan informasi secara ilegal menggunakan sistem atau jaringan komputer.)

Berdasarkan definisi *cybercrime* dan *computer crime* di atas, dapat dilihat perbedaannya, *cybercrime* merupakan suatu kejahatan yang dilakukan oleh pelaku yang tidak bersentuhan langsung dengan komputer target, namun menggunakan jaringan *cyber* sebagai media untuk melakukan kejahatannya. Pelaku hanya membutuhkan komputer serta jaringan komputer untuk melakukan aksinya dan kejahatan tersebut dapat terjadi menembus lintas batas negara. Sedangkan *computer crime* merupakan kejahatan yang menggunakan komputer sebagai alat untuk melakukan kejahatannya.

Selain itu dari *cybercrime* dan *computer crime* menunjukkan bahwa teknologi disebut sebagai "wajah ganda" satu sisi menjadi alat pertanda bagi kemajuan masyarakat secara positif namun disisi lain dapat menjadi alat canggih dalam mempermudah dan memperluas berbagai bentuk perbuatan melanggar hukum.[10]

Banyaknya jenis tindak pidana baru yang muncul akibat kemajuan teknologi menimbulkan kerugian yang amat besar, baik secara materil maupun immateril. Kejahatan ini dapat dilakukan oleh seseorang dari suatu tempat yang sangat pribadi tapi menimbulkan kerugian pada seseorang atau institusi di tempat lain, yang terpisahkan oleh jarak ribuan kilometer, bahkan seringkali bersifat lintas batas teritorial. Dengan demikian kejahatan ini kemudian bisa bersifat transnasional, yaitu kejahatan yang bersifat lintas batas teritorial.[11]

C*ybercrime* merupakan kejahatan yang tergolong baru dengan modus operandi yang berbeda dengan kejahatan konvensional. Di dalam *cybercrime*, kejahatan dilakukan di dalam ruang yang disebut dengan *cyberspace* yaitu dalam ruang yang tidak mengenal batas dan waktu serta tidak mengenal batasan wilayah. Kejahatan yang tidak terlalu memerlukan aktifitas fisik, tidak perlu tatap muka, hanya dengan menggunakan komputer sebagai instrumen, dan internet sebagai medianya. Kejahatan dunia maya ini berkembang seiring majunya teknologi informasi, sehingga

[10] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, 2005, hlm. 22.

[11] Rony Saputra, *Kebijakan Hukum Pidana Terhadap Tindak Pidana Penghinaan/ Pencemaran Nama Baik Melalui Internet di Indonesia Sebagai Cybercrime,* Tesis, Universitas Andalas, Padang, 2016, hlm. 2.

kejahatan ini tergolong kejahatan yang modern yang mana pelakunya bukan orang biasa melainkan orang yang ahli dalam teknologi informasi.[12]

Mengingat karakteristik *cybercrime* yang bersifat *borderless* dan menggunakan teknologi tinggi sebagai media, maka kebijakan kriminalisasi di bidang teknologi informasi harus memperhatikan perkembangan upaya penanggulangan *cybercrime* baik regional maupun internasional dalam rangka harmonisasi dan uniformitas pengaturan *cybercrime,*[13] dengan mengedepankan prinsip-prinsip *Lex informatica.*[14]

Ketiadaan batasan wilayah dalam *cybercrime* ini membuat pelaku kejahatan dapat melakukannya di mana saja. Pelaku dapat melakukan kejahatan di negaranya dengan target yang berada di negara lain. Hal ini menimbulkan masalah dalam pengusutan kasusnya sehingga dibutuhkanlah yurisdiksi hukum untuk menyelesaikannya.

Yurisdiksi merupakan kewenangan suatu negara yang berdaulat untuk menerapkan ketentuan hukum atas orang maupun benda yang (dapat) tunduk oleh hukum nasional yang bersangkutan, sehingga lebih bersifat yuridis.[15] Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan

---

[12] Nilma Suryani dan Arguna Lista, "Tnjauan Yuridis Terhadap Virus Komputer sebagai Alat Bukti Cyber Crime dalam Peradilan Indonesia", *Jurnal Hukum Pidana dan Kriminologi Delicti Universitas Andalas*, Volume XI No. 3 / Januiari s/d Juni 2013, hlm. 58.

[13] Muhammad Amirulloh, Ida Padmanegara, dan Tyas Dian Angraeni, *Kajian EU Convention on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi,* BPHN, Jakarta, 2009, hlm. 1

[14] *Lex Informatica* adalah karakteristik khusus yang terdapat dalam ruang *cyber* dimana pengaturan dan penegakan hukumnya tidak dapat menggunakan cara-cara tradisional, sehingga kegiatan-kegiatan dalam *cyberspace* diatur oleh hukum tersendiri. Lihat **Aron Mefford**, *Lex Informatica*: *Foundations of Law on The Internet*, dalam http://www.repository.law.indiana.edu diakses pada 20 Desember 2016.

[15] Anis Widyawati, *Hukum Pidana Internasional*, Sinar Grafika, Jakarta, 2014, hlm. 168.

prinsip tidak ikut campur tangan. Yurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum. Berdasarkan asas umum dalam hukum internasional, setiap negara memiliki kekuasaan tertinggi atau kedaulatan atas orang dan benda ada dalam wilayahnya sendiri. Oleh karena itu, suatu negara tidak boleh melakukan tindakan yang bersifat melampaui kedaulatannya (*act of sovereignty*) di dalam wilayah negara lain, kecuali dengan persetujuan negara itu sendiri.[16]

Salah satu masalah yang ditimbulkan dalam kasus *cybercrime* adalah bagaimana penerapan yurisdiksi suatu negara terhadap *cybercrime* yang pelakunya berasal dari negara lain. Masalah yurisdiksi tentu berkaitan dengan kedaulatan negara. Menurut hukum internasional yang selama ini berlaku, suatu negara memiliki batasan dalam hal penerapan yurisdiksi terhadap kasus yang melibatkan kepentingan negara lain. Salah satu batasan tersebut adalah kewajiban setiap negara untuk berhati-hati dan sedapat mungkin untuk menghindari munculnya gangguan terhadap negara lain dalam upaya penerapan yurisdiksinya. Meskipun begitu, pada prakteknya hukum internasional tidak dapat memaksakan suatu negara untuk menerapkan suatu konsep yurisdiksi tertentu, bahkan dalam konteks ini setiap negara cenderung diberikan kebebasan dalam menentukan konsep mana yang akan digunakan. Kebebasan tentu saja akan diberikan sepanjang tidak mengancam ketertiban internasional.[17]

---

[16] Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer,* Sinar Grafika, Jakarta, 1992, hlm. 30.

[17] Stephen Wilske and Teresa Schiller, *International Jurisdiction in Cyberspace: Which State May Regulate The Internet*, 50 Fed, Comm, L.J. 117, 171, 1991, dalam Afitrahim M.R, *Yurisdiksi dan Transfer of Proceeding dalam Kasus Cybercrime*, Tesis, Universitas Indonesia, 2012, hlm. 3-4.

Berkaitan dengan konflik yurisdiksi yang ditimbulkan dalam pemberantasan *cybercrime*, Dewan Eropa menghasilkan suatu perjanjian multilateral yaitu *The Council of Europe Convention on Cybercrime* yang ditandatangani di Budapest tahun 2001. Konvensi ini mengatur hukum pidana materil dalam Pasal 2 sampai dengan Pasal 11, yang merumuskan beberapa bentuk *cybercrime.* Daya berlaku hukum pidana substantif tersebut didasarkan pada ketentuan tentang yurisdiksi dalam Pasal 22 yang mengatur prinsip-prisnsip yurisdiksi sebagai dasar berlakunya yurisdiksi kriminal terhadap *cybercrime.*[18] Dalam Pasal 22 negara peserta konvensi dapat menerapkan yurisdiksinya apabila terjadi kejahatan seperti yang terdapat dalam Pasal 2 sampai Pasal 11 dalam konvensi ini. Selain itu negara peserta konvensi dapat menyelesaikan permasalahan yurisdiksi melalui cara ekstradisi dan bantuan timbal balik (*Mutual Legal Assistance*).

Menurut *Convention on Cybercrime*, kejahatan yang terdapat dalam Pasal 2 sampai dengan Pasal 11 tersebut adalah sebagai berikut:[19]

1. Pasal 2 mengatur tentang akses ilegal
   Pihak negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: mengakses secara sadar seluruh atau sebagian dari sistem komputer tanpa hak. Pihak negara berhak mensyaratkan bahwa pelanggaran tersebut melibatkan pelanggaran langkah-langkah pengamanan dengan maksud untuk mengambil data komputer atau untuk niat lain yang tidak jujur, atau berkaitan dengan sebuah sistem komputer yang tersambung kepada sistem komputer lainnya.
2. Pasal 3 mengatur tentang penyadapan ilegal
   Pihak negara harus menerapkan undang-undang dan mengambil tindakan-tndakan lain sebagaimana mungkin perlu untuk ditetapkan sebagai tindak pidana: menyadap tanpa hak, melalui teknik-teknik tertentu, transmisi data komputer yang bukan milik umum, dari atau dalam sebuah sistem komputer

[18] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama, Bandung, 2012, hlm. 251.
[19] *Council of Europe*, *Convention on Cybercrime*, ETS. No. 185,

yang membawa data komputer tersebut. Pihak negara dapat mensyaratkan bahwa tindakan-tindakan tersebut dilakukan dengan tujuan yang tidak jujur, berkaitan dengan sistem komputer yang tersambung kepada sistem komputer lain

3. Pasal 4 mengatur tentang gangguan data
   (1) Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: pengrusakan, penghapusan, pemburukan, perubahan, atau menahan data komputer tanpa hak dan dengan sengaja.
   (2) Pihak Negara berhak mensyaratkan bahwa perilaku yang disebutkan pada paragraf pertama menimbulkan dampak buruk yang serius.
4. Pasal 5 mengatur tentang gangguan sistem
   Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: secara serius merintangi fungsi dari sebuah sistem komputer dengan tanpa hak melalui memasukkan, memindahkan, merusak, menghapus, memperburuk, mengubah atau menahan data komputer.
5. Pasal 6 mengatur tentang penyalahgunaan perangkat
   (1) Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: jika dilakukan secara sadar dan tanpa hak:
      a. produksi, penjualan, pengadaan, impor, distribusi atau mengadakan hal-hal seperti:
         i. sebuah perangkat, termasuk program komputer yang didesain atau diadopsi utamanya untuk tujuan melakukan suatu jenis tindak pidana sebagaimana telah ditetapkan dalam Pasal 2 sampai 5;
         ii. sebuah kata kunci komputer, kode akses, atau data serupa yang bisa membuat keseluruhan atau sebagian sistem komputer dapat diakses, dengan tujuan digunakan untuk melakukan suatu tindak pidana seperti yang disebutkan dalam Pasal 2 sampai 5; dan
      b. pemilikan sebuah benda yang dimaksudkan di dalam Paragraf a.i atau ii di atas, dengan maksud akan digunakan untuk melakukan tindak pidana seperti yang disebutkan dalam Pasal 2 sampai 5. Pihak Negara berhak mensyaratkan atas nama hukum bahwa benda-benda yang disebutkan di atas dimiliki sebelum pertanggungjawaban hukum muncul.
   (2) Pasal ini tidak boleh diterjemahkan sebagai menetapkan konsekuensi hukum bagi kejahatan dimana produksi, penjualan, pengadaan, impor, distribusi, atau mengadakan hal-hal yang disebut dalam paragraf 1 pasal ini yang tidak ditujukan untuk melakukan tindak kejahatan sebagaimana dimaksud dalam Pasal 2 sampai 5 Konvensi ini, seperti untuk pengujian atau perlindungan sebuah sistem komputer yang diperbolehkan.
   (3) Setiap pihak Negara diperbolehkan untuk tidak menerapkan paragraf 1 pasal ini jika kekhususan tersebut tidak berkaitan dengan penjualan,

distribusi atau pengadaan hal-hal yang disebutkan dalam paragraf 1 a.ii pasal ini.

6. Pasal 7 mengatur tentang pemalsuan yang berhubungan dengan komputer
   Setiap pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: melakukan secara sengaja atau tanpa hak memasukkan, mengubah, menghapus, atau menahan data komputer, menyebabkan data menjadi tidak seperti aslinya dengan maksud bahwa hal itu dianggap atau dilakukan untuk sebuah tujuan hukum tertentu seakan-akan asli, tanpa mempertimbangkan apakah data tersebut bisa dibaca dan bisa dimengerti secara langsung. Pihak Negara dapat mensyaratkan maksud untuk menipu atau maksud tidak jujur lainnya, sebelum konsekuensi hukum mengikat.
7. Pasal 8 mengatur tentang penipuan yang berhubungan dengan komputer
   Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperluan untuk ditetapkan sebagai tindak pidana: secara sengaja dan tanpa hak menyebabkan kerugian kepada seseorang dengan cara:
   a. memasukkan, mengubah, menghapus atau menahan data komputer;
   b. mengganggu fungsi sistem komputer, dengan niat tidak jujur dan menipu untuk menhasilkan, tanpa hak, sebuah keuntungan ekonomi untuk diri sendiri atau orang lain.
8. Pasal 9 mengatur tentang pelanggaran yang berkaitan dengan pornografi anak
   (1) Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: secara sadar dan tanpa hak melakukan perilaku-perilaku di bawah ini:
      a. memproduksi pornografi anak dengan maksud untuk disebarkan melalui sistem komputer;
      b. menawarkan atau menyediakan pornografi anak melalui sistem komputer;
      c. mendistribusikan atau menyebarluaskan pornografi anak melalui sistem komputer;
      d. menyediakan pornografi anak melalui sistem komputer untuk diri sendiri atau orang lain;
      e. memiliki pornografi anak di sebuah sistem komputer atau di dalam media penyimpan data komputer.
   (2) Untuk tujuan paeagraf 1 di atas, terminologi “pornografi anak” perlu memasukkan materi pornografi yang secara visual menunjukkan:
      a. seorang anak di bawah umur melakukan hubungan seksual secara jelas;
      b. seseorang yang tampak seperti anak di bawah umur melakukan hubungan seksual secara jelas
      c. gambar yang secara nyata menunjukkan seorang anak kecil melakukan hubungan seksual secara jelas

(3) Untuk tujuan paragraf 2 di atas, terminologi "di bawah umur" berarti semua orang di bawah umur 18 tahun. Pihak Negara boleh menetapkan batas umur yang lebih rendah namun tidak boleh lebih rendah dari 16 tahun.
(4) Pihak Negara berhak untuk tidak menerapkan seluruh atau sebagian dari paragraf 1, sub-paragraf d dan e, dan 2, sub-paragraf b dan c.

9. Pasal 10 mengatur tentan pelanggaran yang berkaitan dengan hak cipta dan hak-hak lainnya
(1) Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: pembajakan hak cipta, sebagaimana dijelaskan dalam undang-undang Pihak Negara tersebut, mengikuti kewajiban-kewajiban yang telah diterima menurut Paris Act 24 Juli 1971 yang merevisi Konvensi Bern untuk Perlindungan Karya Sastra dan Karya Artistik, Kesepakatan Mengenai Aspek-Aspek Hak Intelektual yang berhubungan dengan Perdagangan dan Perjanjian Hak Cipta WIPO, dengan pengecualian segala jenis hak-hak moral yang dimaksudkan oleh konvensi-konvensi tersebut, di mana perilaku-perilaku tersebut dilakukan dengan sengaja, pada skala komersil dan melalui sistem komputer.
(2) Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: pelanggaran dari hak-hak terkait, sebagaimana didefinisikan dalam undang-undang pihak tersebut, mengikuti kewajiban-kewajiban yang telah diterima dalam Konvensi Internasional untuk Perlindungan Pemain dan Produser dari Fonogram dan Organisasi Penyiaran (Konvensi Roma), Kesepakatan mengenai Aspek-aspek Hak Intelektual yang berhubungan dengan Perdagangan dan Perjanjian Hak Cipta WIPO, Perjanjian Penampilan dan Fonogram, dengan pengecualian segala jenis hak-hak moral yang ditetapkan oleh konvensi-konvensi tersebut, di mana perilaku-perilaku tersebut dilakukan dengan sepenuh hati, pada skala komersil dan melalui sistem komputer.
(3) Pihak negara berhak untuk tidak menerapkan konsekuensi hukum di dalam paragraf 1 dan 2 dari pasal ini pada keadaan-keadaan tertentu, selama cara-cara efektif lainnya tersedia dan kekhususan tersebut tidak menyimpang dari kewajiban internasional pihak tersebut yang dimuat dalam instrumen-instrumen internasional yang dimasukkan dalam paragraf 1 dan 2 pasal ini.

10. Pasal 11 mengatur tentang mencoba dan menolong atau membantu
(1) Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: secara sadar menolong atau membantu pelanggaran yang ditetapkan sejalan dengan Pasal 2 sampai 10 Konvensi ini dengan maksud untuk melakukan pelanggaran tersebut.

(2) Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana: secara sadar melakukan suatu pelanggaran sebagaimana ditetapkan di dalam Pasal 3 sampai 5, 7, 8, dan 9.1.a dan c Konvensi ini.
(3) Pihak Negara berhak untuk tidak menerapkan keseluruhan atau sebagian dari paragraf 2 pasal ini.

Terkait dengan yurisdiksi kriminal, KUHP mengenal beberapa asas, yaitu; pertama, asas *teritorialiteit* yang diatur dalam Pasal 2 KUHP yang menyatakan "Aturan pidana dalam perundang-undangan pidana Indonesia berlaku bagi setiap orang yang melakukan perbuatan pidana di dalam wilayah Indonesia". Asas teritorial ini diperluas lingkupnya dengan ketentuan yang terdapat dalam pasal 3 KUHP: "Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi setiap orang yang diluar wilayah Indonesia melakukan tindak pidana di dalam kendaraan air atau pesawat udara Indonesia". Asas ini berlandaskan kedaulatan negara di wilayahnya sendiri. Hukum pidana berlaku bagi siapa pun juga yang melakukan delik di wilayah negara tersebut. Kewajiban suatu negara untuk menegakkan hukum dan menjaga ketertiban hukum di wilayahnya sendiri terhadap siapa pun.[20] Kedua, asas *personaliteit* yang diatur dalam Pasal 5 ayat (1) KUHP yaitu tergantung atau mengikuti subyek hukum atau orangnya, yakni warga negara di manapun keberadaannya.[21] Ketiga, asas perlindungan, yaitu berlakunya hukum pidana menurut atau berdasarkan kepentingan hukum yang dilindungi dari suatu negara yang dilanggar di luar wilayah Indonesia. Kepentingan hukum yang dilindungi ini bukan didasarkan pada kepentingan hukum pribadi, tetapi pada kepentingan hukum negara dan bangsa atau kepentingan nasional dari negara Indonesia. Asas ini terdapat pada

[20] Andi Hamzah, *Op.cit*, hlm 64
[21] Adami Chazawi, *Kejahatan Mayantara*, PT. Refika Aditama, Bandung, 2005, hlm. 209

Pasal 4 KUHP.[22] Keempat, Asas Universal, diberlakukan terhadap kejahatan yang bersifat merugikan kepentingan internasional dan terjadi dalam suatu wilayah yang tidak termasuk kedaulatan suatu negara manapun, seperti di lautan terbuka atau di daerah kutub.[23]

Terkait dengan *cybercrime* yang bersifat lintas batas negara bahkan dianggap sebagai kejahatan yang *borderless*, berakibat pada ketidakmampuan KUHP untuk menjangkau beberapa perbuatan yang dikategorikan sebagai *cybercrime.* Persoalan ini dianggap sebagai suatu masalah yang serius terutama dikaitkan dengan *online activity* di dunia maya, ketidakmampuan capaian hukum pidana tersebut menjadi bahasan yang serius oleh beberapa ahli hukum, yang oleh Barda Nawawi disebut dengan *cyber jurisdiction.*[24]

Di Indonesia, untuk menjawab masalah *cyber jurisdiction* ini, telah diatur dalam Pasal 2 Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elekronika Jo UU No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2011 Tentang ITE (selanjutnya disebut dengan UU ITE) yang menyatakan "Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia."

---

[22] *Ibid,* hlm. 219

[23] C.S.T. Kansil, Cristine S.T. Kansil, *Pokok-Pokok Hukum Pidana*, PT. Pradnya Paramita, Jakarta, 2004, hlm 25

[24] Barda Nawawi Arief, *Tindak Pidana Mayantara*, PT. Rajagrafindo Persada, Jakarta, 2006, hlm. 29

Yurisdiksi dalam UU ITE diperlakukan dengan perluasan, yaitu; pertama, bagi yang berada di wilayah Indonesia dan perbuatannya memiliki akibat hukum di wilayah indonesia saja; kedua, berada di wilayah Indonesia dan perbuatannya memiliki akibat hukum di luar wilayah hukum Indonesia; ketiga, berada di wilayah hukum Indonesia dan perbuatannya memiliki akibat hukum di wilayah dan di luar wilayah hukum Indonesia; keempat, berada di luar wilayah hukum Indonesia dan perbuatannya memiliki akibat hukum di wilayah hukum Indonesia saja; kelima, berada di luar wilayah hukum Indonesia dan perbuatannya memiliki akibat hukum di luar wilayah hukum Indonesia saja; dan keenam, berada di luar wilayah hukum Indonesia dan perbuatannya memiliki akibat hukum di wilayah dan di luar wilayah hukum Indonesia.

Beberapa kasus yang meliputi persoalan yurisdiksi tersebut diantaranya, *carding* yang dilakukan oleh orang Indonesia yang menggunakan nomor kartu kredit warga negara asing untuk membeli sesuatu di internet. Ketentuan ini merupakan suatu ketentuan yang sebelumnya tidak pernah ada dalam hukum pidana di Indonesia. Hal ini dikarenakan sifat akibat kejahatan mayantara yang mampu melampaui batas wilayah suatu negara. Pembuatan *website* pornografi yang bernuansa Indonesia yang dilakukan oleh orang Indonesia yang dapat diakses oleh orang dimana saja berada. Ketentuan ini juga merupakan suatu ketentuan yang sebelumnya tidak pernah ada dalam hukum pidana di Indonesia. Pengrusakan terhadap jaringan keamanan suatu bank yang berada di Indonesia yang dilakukan oleh warga negara asing yang berada di luar wilayah hukum Indonesia. Kasus pengrusakan terhadap jaringan keamanan suatu bank yang berada di negara lain yang dilakukan oleh warga negara asing yang

berada di luar wilayah hukum Indonesia, namun pengrusakan terhadap jaringan keamanan tersebut mengakibatkan kerugian terhadap ekonomi Indonesia. dan Pemuatan website yang berisikan tentang penghinaan terhadap suatu agama yang dianut oleh banyak negara.

Salah satu contoh konkrit kasus yurisdiksi terhadap *cybercrime* ini yaitu Kasus pembobolan BNI Cabang New York, ialah kasus seorang pegawai yang bernama Rudy Demsy yang pernah bekerja di BNI Cabang New York sejak tahun 1980 sampai dengan September 1985. Pada waktu masih bekerja, yang bersangkutan bertugas sebagai operator komputer untuk mengakses *Citybank New York* atau *Mantrust New York*, oleh karenanya yang bersangkutan memegang *password* dengan kode tertentu. Pada tanggal 31 Desember 1986, yang bersangkutan bekerja sama dengan orang lain berhasil mengoperasikan komputer di sebuah hotel untuk melakukan transfer ke rekening bank tertentu,yaitu dengan menggunakan *USER ID* dan *password enter* dengan melawan hukum. Proses tersebut dimulai dengan memerintahkan *Citybank New York* untuk mentransfer dana atas beban rekening BNI kepada rekening BNI di *Mantrust*. Dari sini kemudian yang bersangkutan mentransfer dana ke beberapa bank lainnya untuk keuntungan sendiri.[25]

Dengan adanya kasus tersebut menunjukkan bahwa perbuatan kriminal terhadap aktifitas *cyber* dalam UU ITE yang mengatur penyalahgunaan teknologi informasi dan komunikasi dalam aktivitas di dunia *cyber* belum memadai. Diperlukan adanya kerjasama internasional dalam rangka penegakan hukum terhadap c*ybercrime,* mengingat sifat transnasional dari tindak pidana tersebut. Kerjasama internasional

[25] Niniek Suparni, *Op.cit.* hlm. 11.

sangat penting berkaitan dengan ekstradisi, bantuan timbal balik, *capacity building* dan hal-hal lain yang diperlukan dalam penegakan hukum. Kriminalisasi *cybercrime* dalam hukum nasional merupakan hal penting, tetapi bukan satu-satunya yang diperlukan dalam penegakan hukum terhadap *cybercrime*.[26]

Untuk mengatasi berbagai macam kasus dari *cybercrime,* sesungguhnya hukum internasional dan hukum nasional saling membutuhkan dan mempengaruhi satu sama lain, mengingat semakin canggihnya teknologi tentu semakin beragam pula tindak pidana yang dapat terjadi dikemudian hari. Dalam praktek hukum internasional, penyelesaian masalah penerapan yurisdiksi dalam *cybercrime* tidak terlihat mudah karena walaupun sudah diatur dalam *Convention on Cybercrime* dan peraturan perundang-undangan di setiap negara tetapi tidak semua negara setuju untuk melakukan kerja sama karena hal ini bersinggungan dengan kedaulatan hukum suatu negara.

Timbulnya masalah hukum dalam penerapan yurisdiksi terhadap pelaku *cybercrime* yang melakukan tindak pidana lintas batas negara tersebut menjadi daya tarik penulis untuk mengangkat judul **"Yurisdiksi Kriminal Berlakunya Hukum Pidana Nasional Terhadap *Cybercrime* Diluar Yurisdiksi Indonesia"**

[26] Sigid Suseno, *Op.cit*, hlm. 131.

B. Rumusan Masalah

Berdasarkan latar belakang yang sudah dipaparkan sebelumnya, maka permasalahan yang akan dibahas antara lain sebagai berikut:

1. Bagaimana penerapan yurisdiksi kriminal berlakunya hukum pidana nasional terhadap orang yang melakukan *cybercrime* di luar yurisdiksi Indonesia?
2. Bagaimana upaya yang efektif untuk pemberlakukan yurisdiksi yang diperluas untuk menangani *cybercrime* yang terjadi di lintas batas negara?

C. Tujuan Penelitian

Tujuan pembahasan dalam penelitian ini adalah sebagai berikut:

1. Untuk mengetahui penerapan yurisdiksi kriminal berlakunya hukum pidana nasional terhadap orang yang melakukan *cybercrime* di luar yurisdiksi Indonesia.
2. Untuk mengetahui upaya yang efektif untuk pemberlakukan yurisdiksi yang diperluas untuk menangani *cybercrime* yang terjadi di lintas batas negara.

D. Manfaat Penelitian

Hasil penelitian ini diharapkan mempunyai manfaat teoritis maupun praktis yang diperoleh antara lain:

1. Diharapkan memberikan sumbangan pemikiran dalam pengembangan ilmu pengetahuan hukum, khususnya dalam lingkup pidana.
2. Melatih kemampuan penulis dalam melakukan penelitian penulisan ilmiah.
3. Membantu penegak hukum dalam hal penyelesaian permasalahan hukum mengenai permasalahan ini.

E. Kerangka Teoritis dan Konseptual

1. Kerangka Teoritis

a. Teori Penegakan Hukum

Menurut Soerjono Sukanto, efektifitas diartikan sebagai taraf sampai sejauh mana suatu kelompok mencapai tujuannya.[27] Hukum dikatakan efektif apabila terjadi dampak hukum yang positif, dengan demikian hukum mencapai sasarannya dalam membimbing ataupun merubah perilaku manusia sehingga menjadi perilaku hukum.[28]

Penegakan hukum adalah kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan dalam kaedah-kaedah/pandangan-pandangan menilai yang mantap dan mengejawantahkan dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup.[29] Efektifitas penegakan hukum adalah hasil positif dari seluruh kegiatan yang berhubungan dengan upaya melaksanakan, memelihara dan mempertahankan hukum agar hukum tidak kehilangan makna dan fungsinya sebagai hukum, yaitu sebagai pelindung terhadap kepentingan manusia, baik perorangan (pribadi) maupun seluruh masyarakat.[30]

---

[27] Soerjono Sukanto, *Beberapa Aspek Sosio Yuridis Masyarakat*, Alumni, Bandung, 1983, hlm. 41.

[28] *Ibid.* hlm. 32.

[29] *Ibid.* hlm. 129.

[30] Devitra Romisza, *Analisis Yuridis Penerapan Ketentuan Rahasia Bank Dalam Penegakan Tindak Pidana Pencucian Uang di Indonesia*, Tesis, Fakultas Hukum Universitas Andalas, 2015, hlm. 11.

Penegakan hukum dapat diartikan sebagai tindakan menerapkan perangkat atau sarana hukum yang dimaksudkan untuk melaksanakan sanksi hukum guna menjamin ditaatinya ketentuan yang ditetapkan. Tujuan akhir dari penegakan hukum adalah ketaatan terhadap ketentuan hukum yang berlaku. Ketaatan adalah suatu kondisi tercapainya dan terpeliharanya ketentuan hukum baik berlaku secara umum maupun yang berlaku secara individual dan mencakup masyarakat awam ataupun pejabat administrasi negara yang dalam kehidupan sehari-hari harus menjunjung tinggi penegakan hukum.[31]

b. Teori Kedaulatan Negara

Kedaulatan merupakan salah satu unsur penting suatu negara. I Wayan Parthiana menyatakan bahwa kedaulatan dapat diartikan sebagai kekuasaan tertinggi yang mutlak, utuh, bulat dan tidak dapat dibagi-bagi dan oleh karena itu tidak dapat ditempatkan di bawah kekuasaan lain.[32]

Apa yang dimaksud dengan kedaulatan (*souvereignty*) adalah kekuasaan tertinggi, absolut, dan tidak ada instansi lain yang dapat menyamakannya atau mengontrolnya, yang dapat mengatur warga negara dan mengatur juga apa yang menjadi tujuan dari suatu negara, dan mengatur juga apa yang menjadi tujuan dari suatu negara, dan mengatur berbagai aspek pemerintahan, dan melakukan berbagai tindakan dalam suatu negara,

[31] Soerjono Soekanto dan Otje Salman, *Disiplin Hukum dan Disiplin Sosial*, Rajawali, Jakarta, 1987, hlm. 111.

[32] Surya Sakti Hadiwijoyo, *Aspek Hukum Wilayah Negara Indonesia*, Graha Ilmu, Yogyakarta, 2012, hlm. 103.

termasuk tetapi tidak terbatas pada kekuasaan membuat undang-undang, menerapkan dan menegakkan hukum, menghukum orang, memungut pajak, menciptakan perdamaian dan menyatakan perang, menandatangani dan memberlakukan traktat, dan sebagainya.[33]

Penganjur Teori Kedaulatan Negara, yaitu Hans Kelsen dalam buku *"Reine Rechtslehre"* mengatakan bahwa Hukum itu ialah tidak lain daripada "kemauan negara" (*Wille des Staates*). Namun demikian, Hans Kelsen mengatakan bahwa orang taat kepada hukum bukan karena Negara menghendakinya, tetapi orang taat pada hukum karena ia merasa wajib mentaatinya sebagai perintah Negara.[34]

Jean Bodin menyatakan bahwa kedaulatan merupakan atribut dan ciri khusus dari suatu negara. Tanpa adanya kedaulatan, maka tidak akan ada yang dinamakan negara.[35] Menurut asal katanya, kedaulatan memang berarti kekuasaan tertinggi. Negara berdaulat memang berarti bahwa negara itu tidak mengakui suatu kekuasaan yang lebih tinggi dari pada kekuasaannya sendiri. Dengan perkataan lain, negara memiliki monopoli kekuasaan, suatu sifat khas organisasi masyarakat dan kenegaraan dewasa ini yang tidak lagi membenarkan orang perseorangan mengambil tindakan sendiri apabila ia

[33] Munir Fuady, *Teori-Teori (Grand Theory) Dalam Hukum*, Kencana, Jakarta, 2013, hlm. 91.
[34] C.S.T. Kansil, *Op.cit.* hlm. 63.
[35] Fred Isjwara, *Pengantar Ilmu Politik*, Binacipta, Bandung, 1996, hlm. 108 dalam Surya Sakti Hadiwijoyo, *Batas Wilayah Negara Indonesia "Dimensi, Permasalahan dan Strategi Penanganan (Sebuah Tinjauan Empiris dan Yuridis)*, Gava Media, Yogyakarta, 2009, hlm. 23-24.

dirugikan. Walaupun demikian, kekuasaan teringgi ini mempunyai batas-batasnya.[36]

Kedaulatan negara tersebut dilakukan melalui kekuasaan negara yang menurut John Locke terdiri dari: kekuasaan legislatif, yaitu kekuasaan membuat undang-undang;dan kekuasaan eksekutif, yaitu kekuasaan melaksanakan undang-undang; dan kekuasaan federatif, yaitu kekuasaan negara mengenai perang dan damai, membuat perserikatan dan aliansi serta segala tindakan dengan semua orang atau badan-badan di luar negeri. Namun kekuasaan (*trias politica*), yang terpisah satu sama lain, yaitu legislatif, eksekutif, dan yudikatif. Kekuasaan federatif dari John Locke, menurut Montesquieu termasuk dalam kekuasaan eksekutif. Dalam negara Indonesia yang berdasarkan Pancasila dan Undang-Undang Dasar (UUD) 1945 tidak dikenal pemisahan kekuasaan (*separation of power*) sebagaimana dianut negara-negara lain yang menganut ajaran *trias politica* tetapi menganut pembagian kekuasaan (*division of power*) yang dilaksanakan oleh lembaga-lembaga negara sebagaimana diatur dalam UUD 1945.[37]

[36] Mochtar Kusumaatmadja dan Etty R. Agoes, *Pengantar Hukum Internasional*, P.T. Alumni, Bandung: 2003, hlm. 17-18.

[37] Ismail Suny, Pembagian Kekuasaan Negara, Aksara Baru, Jakarta, 1978, hlm. 5-6.

Sesuai konsep hukum internasional, kedaulatan memiliki tiga aspek utama[38] yaitu: ekstern, intern dan teritorial.

1) Aspek ekstern kedaulatan adalah hak bagi setiap negara untuk secara bebas menentukan hubungannya dengan berbagai negara atau kelompok-kelompok lain tanpa kekangan, tekanan atau pengawasan dari negara lain.
2) Aspek intern kedaulatan ialah hak atau wewenang ekslusif suatu negara untuk menentukan bentuk lembaga-lembaganya, cara kerja lembaga-lembaga tersebut dan hak untuk membuat undang-undang yang diinginkannya serta tindakan-tindakan untuk mematuhi.
3) Aspek teritorial kedaulatan berarti kekuasaan penuh dan eksklusif yang dimiliki oleh negara atas individu-individu dan benda-benda yang terdapat di wilayah tersebut.

Suatu negara tidak dapat melaksanakan yurisdiksi eksklusifnya ke luar dari wilayahnya yang dapat mengganggu kedaulatan negara lain. Suatu negara hanya dapat melaksanakannya secara eksklusif dan penuh hanya di dalam wilayahnya saja. Karena itu pula suatu subyek (hukum internasional) yang tidak memiliki wilayah, tidak mungkin menjadi suatu negara.[39] Jadi dengan adanya kedaulatan maka suatu negara dapat melakukan tindakan-tindakan dalam hal kenegaraan dan segala kepentingannya karena adanya kekuasaan dalam melaksanakannya.

---

[38] Boer Mauna, *Hukum Internasional*, Alumni, Bandung, 2003, hlm. 24.

[39] Huala Adolf, *Aspek-Aspek Negara Dalam Hukum Internasional*, Rajawali Pers, Jakarta, 1991, hlm. 100.

c. Teori Yurisdiksi

Yurisdiksi adalah kompetensi atau kekuasaan hukum negara terhadap orang, benda, dan peristiwa hukum. Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, persamaan derajat negara dan prinsip non intervensi.[40]

Setiap Negara pasti memiliki yurisdiksi atau kewenangan untuk mengatur tindakan di dalam wilayahnya sendiri. Yurisdiksi dapat digolongkan ke dalam prinsip-prinsip yurisdiksi berikut:

1) Yurisdiksi Teritorial

Menurut yurisdiksi teritorial, pelaksanaan yurisdiksi oleh suatu negara terhadap harta benda, orang tindakan atau peristiwa yang terjadi di dalam wilayahnya jelas diakui oleh hukum internasional untuk semua anggota negara masyarakat internasional. Prinsip tersebut telah dikemukakan dengan tepat oleh Lord Macmillan:[41]

> "Adalah suatu ciri pokok dari kedaulatan dalam batas-batas ini, seperti semua negara merdeka yang berdaulat, bahwa Negara harus memiliki yurisdiksi terhadap semua orang dan benda di dalam batas-batas teritorialnya dan dalam semua perkara perdata dan pidana yang timbul di dalam batas-batas territorial ini."

Dilihat dari penyataan tersebut maka setiap orang yang berada dalam wilayah Indonesia harus mematuhi segala peraturan atau undang-undang yang ada di Indonesia baik pidana maupun perdata karena ketentuan pidana

[40] Sefriani, *Op.cit*. hlm. 233.

[41] Compania Naviera Vascongado v Cristina SS AC 485 hlm. 496-497, dalam JG. Starke, Pengantar Hukum Internasional, Sinar Grafika, Jakarta, 2001, hlm. 270-271.

dalam undang-undang Indonesia yang melakukan sesuatu perbuatan yang boleh dihukum.

2) Yurisdiksi Terhadap Individu

Yurisdiksi terhadap individu, berbeda dengan yurisdiksi atas wilayah, bergantung pada kualitas orang yang terlibat dalam peristiwa hokum. Kualitas ini dapat membenarkan suatu Negara atau Negara-negara menjalankan yurisdiksi apabila orang itu berada dalam kekuasaan negara, dan proses peradilan dapat dilaksanakan terhadapnya. Hal ini umum terjadi apabila seorang individu memasuki wilayah negara tersebut, baik secara sukarela maupun akibat tindakan ekstradisi.[42]

Menurut praktek internasional, yurisdiksi terhadap individu dilaksanakan berdasarkan prinsip nasional aktif dan prinsip nasional pasif. Dalam prinsip nasional aktif, yurisdiksi didasarkan atas siapa yang menjadi pelaku kejahatan dan di mana tempat kejahatan dilakukan, serta adanya kepentingan dari negara yang bersangkutan untuk membuat, melaksanakan, dan memaksakan peraturan perundang-undangan pidana nasionalnya.[43]

Warga negara dari negara itu sendiri yang melakukan kejahatan yang dilakukannya di suatu tempat di wilayah negara lain yang ditujukan kepada sesama warga negara dari negara yang bersangkutan, dan atas kejahatannya itu negara yang bersangkutan berkepentingan untuk melindungi warga

[42] *Ibid*. hlm. 302-303.

[43] I Wayan Parthiana, *Hukum Pidana Internasional*, Yrama Widya, Bandung, 2015, hlm. 166-167.

negaranya yang menjadi korbannya, dengan membuat, melaksanakan atau menerapkan, dan memaksakan hokum atau peraturan perundang-undangan pidananya.[44]

Mengenai prinsip nasional pasif menurut Antonio Cassese dalam bukunya *Intenational Criminal Law* yaitu[45]:

> *"By virtue of the principle of passive nationality states may exercise jurisdiction over crimes committed abroad against their own nationals. plainly, the principle is grounded both on: (i) the need to protect nationals living or residing abroad and (ii) a substantial mistrust in the exercise of jurisdiction by the foreign territorial state."(*Berdasarkan prinsip kewarganegaraan pasif negara melaksanakan yurisdiksi atas kejahatan yang dilakukan di luar negeri terhadap warga negara mereka sendiri. Jelas bahwa prinsip ini berdasarkan pada (i) kebutuhan untuk melindungi warga negara yang tinggal atau berada di luar negeri dan (ii) ketidakpercayaan substansial dalam pelaksanaan yurisdiksi oleh teritorial negara asing.")

3) Yurisdiksi Menurut Prinsip Perlindungan

Berdasarkan prinsip yurisdiksi perlindungan, suatu negara dapat melaksanakan yurisdiksinya terhadap warga-warga asing yang melakukan kejahatan dari luar negeri yang diduga dapat mengancam kepentingan keamanan, integritas, dan kemerdekaan negara. Penerapan prinsip ini dibenarkan sebagai dasar untuk penerapan yurisdiksi suatu Negara..[46]

4) Yurisdiksi Menurut Prinsip Universal

Yurisdiksi universal merupakan yurisdiksi negara yang tidak semata-mata didasarkan pada tempat, waktu maupun pelaku tindak pidana melainkan

---

[44] *Ibid*.
[45] Antonio Cassese, *International Criminal Law*, Oxford University Press, 2003, hlm. 282.
[46] Huala Adolf, Op.Cit. hlm. 213.

lebih dititikberatkan pada kepentingan umat manusia yang universal, sebagai contoh adalah pelanggaran HAM (*human trafficking, genocide*, kejahatan kemanusiaan yang lain), terorisme internasional, *transnational crime* (pembajakan pesawat udara, pembajakan kapal) dan lain sebagainya.[47] Jelas bahwa tujuan pemberian yurisdiksi universal adalah untuk menjamin bahwa tidak ada tindak pidana semacam itu yang tidak dihukum di negara manapun.

Dengan demikian, yurisdiksi suatu negara berarti kedaulatan negara dalam menjalankan kewenangannya. Berdasarkan prinsip-prinsip yurisdiksi di atas maka dari situlah dapat menentukan yurisdiksi yang akan digunakan dalam menghadapi *cybercrime* yang terjadi lintas batas teritorial.

2. Kerangka Konseptual

a. Yurisdiksi Kriminal

Yurisdiksi adalah refleksi dari kedaulatan suatu negara, yang dilaksanakan dalam batas-batas wilayahnya, sebagaimana juga yang melekat pada semua negara merdeka yang berdaulat, bahwa kekuasaan tersebut mencakup yurisdiksi atau kewenangan atas semua orang dan benda/peristiwa yang ada atau terjadi dalam batas-batas wilayahnya, baik yang bersifat keperdataan maupun pidana.[48]

I Wayan Parthiana menyebutkan yurisdiksi kriminal merupakan yurisdiksi yang berkaitan dengan masalah kriminal. Tegasnya jika ada suatu peristiwa kejahatan yang terjadi di dalam dan atau di luar wilayah

[47] Surya Sakti Hadiwijoyo, *Aspek Hukum. Op.cit.* hlm. 115.
[48] Sigid Suseno. *Op.cit*. hlm. 54.

suatu negara, sepanjang ada kepentingan dari Negara itu atau warga negara ataupun badan-badan hukum nasionalnya yang harus dilindungi oleh negara yang bersangkutan, maka negara itu dapat memiliki yurisdiksinya.[49]

b. Hukum Pidana Nasional

Hukum pidana adalah suatu keseluruhan asas-asas dan peraturan-peraturan yang diikuti oleh negara atau suatu masyarakat hukum lainnya, di mana mereka itu sebagai pemelihara dari ketertiban hukum umum telah melarang dilakukannya tindakan-tindakan yang bersifat melanggar hukum dan yang telah mengaitkan pelanggaran terhadap peraturan-peraturannya dengan suatu penderitaan yang bersifat khusus berupa hukuman.[50] Pengertian mengenai hukum pidana nasional berdasarkan pengertian dari hukum pidana di atas merupakan keseluruhan dari peraturan yang dibentuk dengan tujuan untuk menciptakan ketertiban yang berlaku dalam suatu negara.

c. *Cybercrime*

Cybercrime adalah segala tindakan yang merugikan orang lain dengan menggunakan komputer sebagai alat untuk melakukan kejahatan serta sistem dan data di dalamnya sebagai target.[51]

---

[49] I Wayan Parthiana, *Op.cit.*hlm. 160-161.
[50] PAF Lamintang. *Dasar-Dasar Hukum Pidana Indonesia*, Sinar Baru, Bandung, 1984, hlm. 1.
[51] Abdul Wahid dan Mohammad Labib, *Op.cit*, hlm. 40.

F. Metode Penelitian

1. Tipe Penelitian

Penelitian merupakan suatu sarana pokok dalam pengembangan ilmu pengetahuan dan teknologi, oleh karena itu penelitian bertujuan untuk mengungkapkan kebenaran secara sistematis, metodologis dan konsisten dengan mengandalkan analisa dan konstruksi.[52] Metodologi penelitian yang digunakan penulis dalam proposal ini adalah yuridis normatif yang dapat diartikan sebagai penelitian hukum kepustakaan yang dilakukan berdasarkan pada kepustakaan atau data sekunder.[53] Dengan kata lain penelitian ini penelitian kepustakaan (*library research*) artinya penelitian ini dilakukan dengan membaca karya-karya yang terkait dengan persoalan yang akan dikaji kemudian memuat kajian tentang penelitian.[54] Dalam penelitian ini menggunakan pendekatan undang-undang (*statute approach*) dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani[55] serta menggunakan pendekatan konseptual (*conceptual approach*).

2. Sifat Penelitian

Penelitian ini bersifat deskriptif analitis yaitu analisis yang menggambarkan regulasi-regulasi internasional serta peraturan perundang-

---

[52] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Raja Grafindo Persada, Jakarta, 2007, hlm. 1.

[53] Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum*, Ghalia Indonesia, Jakarta, 1990, hlm. 11.

[54] Mestika Zed, *Metode Penelitian Kepustakaan*, Yayasan Obor Indonesia, Jakarta, 2007, hlm. 3.

[55] Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana, Jakarta, 2010, hlm. 93.

undangan yang berlaku yang berkaitan dengan teori-teori hukum yang menyangkut objek penelitian yang dibahas dalam penulisan ini.

3. Sumber Bahan Hukum

Dalam penelitian hukum normatif maka sumber hukum yang digunakan adalah data sekunder, yang terdiri bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif artinya mempunyai otoritas[56] yaitu berupa perjanjian-perjanjian internasional serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Bahan hukum sekunder yaitu bahan yang memberikan penjelasan mengenai bahan hukum primer[57] yang berasal dari buku-buku teks, termasuk hasil penelitian berupa skripsi, tesis dan disertasi maupun hasil penelitian lainnya, tulisan jurnal, majalah, dan lain-lain.

Bahan-bahan hukum tersier adalah bahan-bahan yang memberi petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder seperti kamus, ensiklopedia dan sebagainya.[58]

4. Metode Pengumpulan Data

Sebagaimana ciri dari penelitian hukum normatif, maka metode pengumpulan data dapat dilakukan dengan studi kepustakaan (*library research*), yaitu dengan melakukan penelitian terhadap bahan pustaka.[59] Selain itu

[56] *Ibid*, hlm. 141.
[57] Soerjono Soekanto dan Sri Mamudji, *Op.cit*.
[58] *Ibid.*
[59] *Ibid*. hlm. 61

dilakukan dengan studi dokumen terhadap literatur-literatur yang berkaitan dengan penelitian ini.

5. Analisis Data

Penulis menggunakan metode penelitian hukum normatif dalam penelitian ini, sehingga pengolahan data yang dilakukan dengan cara mensistematisasi bahan-bahan hukum tertulis. Analisis data yang digunakan penulis adalah analisis kualitatif karena bahan hukum yang diperoleh tersebut dijabarkan dalam bentuk kalimat.