BAB I

PENDAHULUAN

A. LATAR BELAKANG

Saat ini duniadalam kondisi yang lazim disebut globalisasi, dimana hubungan antar subyek seolah-olah tanpa batas (*borderless*).[1] Globalisasi ini didukung oleh kemajuan teknologi dan informasi yang sangat pesat dengan sumber daya manusia (SDM) yang semakin kreatif demi untuk memenuhi kebutuhan yang semakin kompleks. Untuk menghubungi kolega yang jaraknya beribu-ribu kilo meter cukup dengan tekan angka-angka yang ada pada *handphone*, untuk berdagang dengan mitra bisnis yang berbeda Benua juga tidak perlu repot dengan datang ke lokasi yang dimaksud, cukup menggunakan fasilitas perdagangan elektronik (*e-commerce*). Untuk melakukan aktivitas perbankan juga tidak perlu datang ke bank, cukup memanfaatkan kecanggihan teknologi *e-banking* dan banyak hal lain yang terasa sangat mudah untuk dilakukan dibanding sebelumnya.[2]

Jaringan*borderless*merupakan jaringan yang disediakan untuk memudahkan pengguna internet agar dapat mengakses informasi seluas-luasnya.[3] Perpaduan antara teknologi komputer dan teknologi telekomunikasi membentuk sebuah piranti baru dengan nama internet.

---

[1]Tim Dosen Fakultas Hukum Universitas Brawijaya, 2011, **Ketika Hukum Berhadapan Dengan Globalisasi**, UB Press, Malang, hlm. V.

[2]Ibid, hlm. V.

[3]Intan Innayatun Soeparna, **KejahatanTelematikaSebagaiKejahatanTransnasional**, http://www.academia.edu/208360/Kejahatan_Telematika_sebagai_Kejahatan_Transnasional, tertanggal 22 September 2013

Pada intinya, internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optic, satelit atau gelombang frekuensi.[4]

Di dalam jaringan *borderless* bukan hanya ada individu atau perorangan yang menjadi subjek, negara juga termasuk. Sama halnya dengan individu, cara negara berhubungan dengan negara lain kini makin maju dengan internet dan jaringan telekomunikasi lain. Meskipun dalam hal ini kegiatan diwakili oleh orang, namun dilakukan atas nama negara. Menghubungi kepala negara lain, perdana menteri, atau menteri luar negeri hanya perlu menggunakan telepon. Mengirim surat menggunakan surat elektronik atau *e-mail,* lebih mudah dari sebelumnya yang harus mengirim surat menggunakan jasa pengiriman sehingga memakan waktu lama jika letak negara yang dituju jauh. Selain itu, juga bermafaat sebagai media publikasi mengenai konvensi-konvensi baru yang dibuat dan diratifikasi oleh negara-negara dalam hal perjanjian internasional serta peraturan-peraturan baru yang dibuat oleh pemerintah dalam satu negara.

Sejauh ini globalisasi serta kemajuan teknologi memberikan dampak positif maupun negatif. Salah satu dampak positif yangdidapat yaitu menghemat waktu karna berhubungan dengan orang lain dari tempat yang jauh hanya dengan waktu yang sangat singkat. Dampak negatifnya adalah bahwa dalam globalisasi dan kemajuan teknologi komunikasi ini terdapat penyalahgunaan teknologi, terutama dalam teknologi komunikasi. Era globalisasi dan teknologi informasi membawa pengaruh terhadap munculnya berbagai bentuk kejahatan yang sifatnya

[4]Agus Raharjo. 2002. ***Cybercrime*, Pemahaman dan Upaya Pencegahan kejahatanBerteknologi.** Bandung: Citra Aditya Bakti. Hal. 59.

baru.[5] Jaringan *borderless* digunakan sebagai alat untuk melakukan perbuatan yang bertentangan hukum. Umumnya kejahatan yang berhubungan dengan teknologi atau *cybercrime* merupakan kejahatan yang menyangkut harta benda dan/atau kekayaan intelektual. Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer.[6]

Dalam kondisi globalisasi dengan jaringan komunikasi yang bersifat *borderless,* dimana hubungan antar negara sudah jauh lebih mudah dari sebelumnya, suatu negara dapat mengalami permasalahan dengan negara lain yang menjadi mitra atau negara sahabatnya. Masalah yang terjadi antara negara bermacam-macam, mulai dari masalah yang biasa hingga masalah yang bisa menimbulkan permusuhan.Salah satu masalah yang sedang terjadi antar negara saat iniadalah masalah penyadapan, yaitupenyadapan intelejen Australia terhadap presiden RI dan beberapa Menteri serta terhadap beberapa negara di Asia lainnya.

Menurut Undang-undang No 36 tahun 1999 tentang Telekomunikasi, penjelasan pasal 40;

> *"Yang dimaksud dengan penyadapan dalam pasal ini adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah. Pada dasarnya informasi yang dimiliki oleh seseorang adalah hak pribadi yang harus dilindungi sehingga penyadapan harus dilarang."*

Kemudian, definisi penyadapan yang sah secara hukum menurut *European Telecommunications Standards Institute* (ETSI) yaitu kegiatan penyadapan

[5]Didik M. Arief Mansur dan Elisatris Gultom, 2005**,** ***Cyber Law*: Aspek Hukum Teknologi Informasi**, Refka Aditama, Bandung, hlm. 19.

[6]Didik M. Arief Mansur dan Elisatris Gultom, *Ibid*, hlm.7.

dilakukan terhadap *network operator,* akses *provider, service provider* dengan tujuan agar informasi yang ada selalu siap digunakan sebagai fasilitas kontrol pelaksanaan hukum.[7] Penyadapan pada dasarnya hanya dibolehkan bagi petugas yang berwenang dalam suatu negara guna meningkatkan pengawasan tingkat tinggi dan dilakukan sepenuhnya untuk kepentingan keamanan negara agar mampu mempertahankan dan meningkatkan kemampuan melawan tindakan teror. Kewenangan penuh untuk menerapkan penyadapan yang sah secara hukum tersebut dikenal dengan istilah lawful interception.[8]

Dari beberapa media informasi, didapatkan bahwa kegiatan penyadapan Australia terhadap beberapa negara di Asia termasuk Indonesia dilakukan dengan bekerjasama dengan Amerika Serikat.Menanggapi kejadian tersebut, Presiden SBY menuntut Perdana Menteri Australia untuk segera meminta maaf dan menjelaskan alasan mengapa melakukan penyadapan. Selain itu Presiden SBY juga mengancam akan mengusir perwakilan diplomatik Australia di Indonesia. Dalam prakteknya tidak mungkin akan dilakukan penjelasan mengapa intelejen Australia melakukan penyadapan karena mencari informasi dengan memata-matai adalah sewajarnya pekerjaan dari intelejen. Yang menjadi masalah adalah spionase dilakukan dalam masa damai, bukan dalam keadaan perang. Spionase dilakukan dengan cara menyadap *handphone* milik Presiden RI, kegiatan ini dipusatkan di kantor kedutaan Australia di Indonesia. Hukum positif Indonesia tidak mengatur secara rinci mengenai tindakan spionase dalam Undang-undang tersendiri, namun hal ini diatur di dalam Undang-undang tentang teknologi dan

[7]Firman Nuro, **Aspek Hukum Mengenai Monitoring Aktivitas Komputer dan Tindak Pidana Penyadapan Data Pribadi Pengguna Internet**, jbptunikompp-gdl-firmannuro-24692-4-babii.pdf, hlm. 22. (Diakses 28 Februari 2014)

[8] Firman Nuro,*Ibid*, hlm 22-23.

informasi.Selain itu, Indonesia juga merupakan negara anti spionase.Dalam Undang-undang tentang teknologi dan informasi spionase merupakan kejahatan dunia maya atau *cybercrime*.

Selain spionase yang dilakukan Australia kepada Indonesia dan beberapa negara di Asia Tenggara, kemarahan dunia internasional atas dugaan spionase yang dilakukan Badan Keamanan Nasional (NSA) Amerika Serikat (AS) memuncak.Jerman dan Brazil, sebagian dari negara yang merasa jadi korban spionase NSA merancang resolusi PBB untuk mengakhiri kegiatan spionase yang berlebihan itu. Di Eropa, selain Jerman, Perancis juga berang atas ulah NSA. Sebuah laporan dari media Perancis, Le Monde,mengungkap, 70 juta lebih komunikasi telepon rakyat Perancis disadap NSA. Belum reda kemarahan Perancis, media itu kembali melansir laporan, komunikasi diplomat Perancis di PBB dan Washington juga disadap.Spanyol, yang belum memiliki bukti telah dimata-matai AS, juga berniat memanggil Duta Besar AS yang berada di Spanyol. Di Amerika Latin, selain Brazil, Meksiko juga jadi korban spionase AS. Pemerintah Meksiko marah setelah laporan NSA memata-matai presiden mereka pada tahun 2010 terbongkar. E-mail Felipe Calderon yang pada 2010 menjabat sebagai Presiden Meksiko, disadap oleh NSA. Seperti itulah yang diberitakan dalam sindonews.com pada Sabtu, 26 Oktober 2013.[9]

Hal ini mudah diputuskan apabila subjek dan objek dari spionase ini merupakan individu atau kelompok dalam satu negara. Yang menjadi pertanyaan adalah jika kegiatan spionase yang dilakukan oleh antar negara terhadap negara

[9] Muhaimin, **FOKUS DUNIA: Kemarahan dunia atas spionase AS memuncak,**http://international.sindonews.com/read/2013/10/26/45/798548/kemarahan-dunia-atas-spionase-as-memuncak, tertanggal 9 Desember 2013.

dengan catatan bahwa spionase merupakan suatu *cybercrime* menurut negara yang menjadi objek spionase, tetapi di sisi lain spionase bukan merupakan merupakan suatu *cybercrime* di negara yang melakukan siponase. Dalam dunia internasional pun belum ada konvensi khusus yang mengatur spionase secara terperinci. Namun beberapa negara anti-spionase telah mengusulkan PBB agar mengeluarkan resolusi anti spionase antar negara atau *Anti-Spying Resolution* dengan harapan tidak ada lagi tindakan spionase melalui cara apapun termasuk melalui penyadapan. Dari permasalahan tersebut maka penulis mengambil judul **TINDAKAN SPIONASE MELALUI PENYADAPAN ANTAR NEGARASEBAGAI *CYBERCRIME*** sebagai penelitian penulisan skripsi.

B. RUMUSAN MASALAH

1. Apakah tindakan spionase memalui penyadapan antar negara termasuk sebagai *cybercrime*?
2. Bagaimana upaya Indonesia dalam mengatasi tindakan spionase melalui penyadapan antar negara seperti yang telah dilakukan Australia?

C. TUJUAN PENELITIAN

1. Untuk mengetahui tindakan spionase santar negara temasuk sebagai *cybercrime*.
2. Untuk mengetahui upaya Indonesia dalam mengatasi tindakan spionase melalui penyadapan antar negara seperti yang telah dilakukan Australia

D. MANFAAT PENELITIAN

1. Manfaat Teoris

Memberikan pengetahuan dan pemahaman atas masalah yang timbul dalam ruang lingkup hukum internasional yaitu hubungan antar negara khususnya dalam hal spionase melalui penyadapan antar negara merupakan salah satu bentuk dari *cybercrime*.

2. Manfaat Praktis

   a. Bagi Akademisi

      Memberikan pengetahuan serta referensi bagi sesama akademisi mengenai tindakan spionase melaui penyadapan antar negara sebagai *cybercrime*.

   b. Bagi Pemerintah

      Memberikan masukan kepeada pemerintah RI agar dapat lebih tegas dalam menangani permasalahan Internasional, terutama menyangkut keamanan dan hubungan internasional.

   c. Bagi Penulis

      Menambah pengetahuan penulis akan permasalahan internasional terutama mengenai kejahatan dunia maya yang dilakukan oleh negara. Selain itu juga Penulisan ini merupakan syarat Penulis untuk mendapat gelar kesarjanaan.

E. SISTEMATIKA PENULISAN

BAB I : PENDAHULUAN

Berisi tentang latar belakang yang mendasari dilakukannya penelitian, perumusan masalah yang enjadi persoalan yang jawabannya ingin diketahui oleh peneliti,

tujuan penelitian yang merupakan maksud dari diadakannya penelitian serta manfaat dan sistematika penulisan yang digunakan.

BAB II : KAJIAN PUSTAKA

Berisi penguraian kajian teori-teori ilmiah yang berhubungan dengan pokok permasalahan yang dipermasalahkan dan yang akan dipakai dalam analisis, hasil-hasil kajian ilmiah lain yang berhubungan dengan apa yang dipermasalahkan, dan rangkuman hasil-hasil kajian teori yang berkaitan dengan permasalahan.

BAB III : METODE PENELITIAN

Berisi tentang metode pendekatan yang digunakan, jenis dan sumber bahan hukum, teknik memperoleh bahan hukum, teknik analisis bahan hukum serta definisi konseptual.

BAB IV : HASIL DAN PEMBAHASAN

Menguraikan hasil penelitian atau pembahasan tentang kegiatan spionase melalui penyadapan sebagai cybercrime yang dilakukan negara kepada negara lain menurut hukum internasional.

BAB V : PENUTUP

Berisi kesimpulan dan saran. Kesimpulan merupakan uraian jawaban dari rumusn masalah yang telah dianalisis di dalam pembahasan. Serta saran yang berisi harapan-harapa mengenai hasil kajian ke arah yang lebih baik untuk masa yang akan datang.