TINDAKAN SPIONASE MELALUI PENYADAPAN ANTAR NEGARA SEBAGAI *CYBERCRIME*

Rofi'a Zulkarnain, Herman Suryokumoro S.H.,MS, Dr. Patricia Audrey Ruslijanto S.H.,MKn.

Fakultas Hukum Universitas Brawijaya

105010107111092@ub.ac.id

Abstrak

Kejahatan yang berhubungan dengan teknologi atau *cybercrime* yang merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer. Dalam kondisi seperti ini, hubungan antar negara jauh lebih mudah dari sebelumnya, suatu negara dapat mengalami permasalahan dengan negara lain. Salah satu masalah yang sedang terjadi saat ini adalah masalah spionase melalui penyadapan oleh Australia kepada Indonesia. Mudah diputuskan apabila subjek dan objek spionase merupakan individu atau kelompok dalam satu negara dengan catatan bahwa spionase melaui penyadapan merupakan suatu *cybercrime* dari negara bersangkutan. Maka dari itu penelitian ini dilakukan untuk menganalisis Apakah tindakan spionase melalui penyadapan antar negara termasuk sebagai *cybercrime* dan upaya Indonesia dalam mengatasi tindakan spionase melalui penyadapan antar negara seperti yang telah dilakukan Australia. Penelitian ini dilakukan dengan studi kepustakaan dengan menggunakan pendekatan perundang-undangan serta pendekatan kasus. Berdasarkan hasil penelitian, Tindakan Spionase Melalui Penyadapan Antar Negara dilihat dari beberapa karakteristik *cybercrime* terhadap spionase dan penyadapan, maka spionase melalui penyadapan dapat dikategorikan sebagai cybercrime. Berdasarkan hukum nasional, Australia melanggar hukum nasional Indonesia. Namun, dalam permasalahan ini tidak dapat begitu saja menerapkan hukum nasional meskipun tindakan yang dilakukan Australia adalah melanggar hukum nasional. Selain dengan penyelesaian melalui penyelesaian diplomatik. Persoalan antar negara ini juga dapat diselesaikan melalui Mahkamah Internasional.

Kata kunci: *cybercrime,* spionase, penyadapan

THE ACT OF ESPIONAGE BY INTERCEPTION BETWEEN STATES AS CYBERCRIME

Rofi'a Zulkarnain, Herman Suryokumoro S.H.,MS, Dr. Patricia Audrey Ruslijanto S.H.,MKn.

Fakultas Hukum Universitas Brawijaya

105010107111092@ub.ac.id

Abstrac

Crimes-related Technology or cybercrime refers to a crime related to cyberspace and crime that uses computers. Under these conditions, in which relations between states are more easily than before, a nation may experience problems with other statess. One of the problems is happening now is the problem of act of espionage by interception by Australia. Is easily decided when the subject and object of espionage is an individual or group in the state with a note that act of espionage by interception as cybercrime in related states. Therefore, the authors attempt to analyze; Is the act of espionage by interception between nations categorized as cybercrime and Indonesia's efforts to resolve the acts of espionage by interception between nations such as Australia has been done. The method used in this paper is a library research with statute approach and case approach. Legal materials were analyzed by descriptive qualitative. Based on the results of the study, the authors obtained answers to the exist problems that The Act of Espionage by Interception Between States seen from some of the characteristics of cybercrime to espionage and interception, the espionage by interception can be categorized as cybercrime. Under the Indonesian national laws, Australia violated national laws of Indonesia. however, in this case cannot simply implement national laws despite the action taken by Australia is unlawfull. In addition to the resolution of a diplomatic settlement. The case between states can also be solved by the International Court of Justice.

Keyword: cybercrime, espionage, interception.

I. PENDAHULUAN

Sejauh ini globalisasi serta kemajuan teknologi memberikan dampak positif maupun negatif. Salah satu dampak positif yang didapat 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 baru.[1] 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.[2]

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. Salah satu masalah yang sedang terjadi antar negara saat ini adalah masalah penyadapan, yaitu penyadapan intelejen Australia terhadap presiden RI dan beberapa Menteri serta terhadap beberapa negara di Asia lainnya.

Dalam prakteknya tidak 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

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

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

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

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 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 NEGARA SEBAGAI *CYBERCRIME*** sebagai penelitian penulisan skripsi.

II. PERMASALAHAN

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?

III. PEMBAHASAN

Penelitian ini dilakukan dengan study kepustakaan dengan menggunakan pendekatan perundang-undangan serta pendekatan kasus. Berdasarkan hasil penelitian, Hukum nasional belum mampu menanggulangi secara penuh kejahatan ini dikarenakan karakteristik kejahatan teknologi dan informasi ini adalah maya. Dalam lingkup Internasional kejahatan ini juga masih belum mendapat penanggulangan yang maksimal. *Cybercrime* yang identik dengan kejahatan dalam bidang harta benda, dalam dunia internasional hanya diatur mengenai kejahatan yang dilakukan orang perorangan terhadap individu lain atau terhadap

badan hukum tertentu. Sedangkan mengenai *cybercrime* yang memungkinkan dilakukan oleh negara terhadap negara lain belum ada pengaturan khusus. Bertolak belakang dengan banyak permasalahan yang terjadi dewasa ini.

Bertolak belakang dengan banyak permasalahan yang terjadi dewasa ini. Sebagian negara mengaku telah menjadi objek spionase oleh negara lain. Hal ini diketahui bukan dilakukan dengan cara konvensional, melainkan melalui dunia maya dengan memanfaatkan kemajuan teknologi informasi dan media telekomunikasi. Spionase atau dalam bahasa Inggris *Espionage* diartikan dalam Kamus Besar Bahasa Indonesia adalah penyelidikan secara rahasia terhadap data kemiliteran dan data ekonomi negara lain; segala sesuatu yang berhubungan dengan seluk-beluk spion; pemata-mataan: penangkapan dua orang wakil atase militer itu atas tuduhan.[3] Salah satu konvensi yang mengatur mengenai kegiatan spioase ini adalah *Hague Convention IV 1907* artikel 29 hingga 31. *Hague Convention* mengatur mengenai kegiatan *spying* dan *spies* dalam keadaan perang, dimana kegiatan *spying* yang dimaksud dilakukan secara langsung dengan cara konvensional bukan melalui media yang canggih seperti kasus-kasus yang terjadi dewasa ini.

Geoffrey Demarest mengatakan bahwa, "*The development of international legal principles regarding peacetime espionage has lagged behind changes in international intelligence gathering norms and practices*."[4] Dari pernyataan Demarest tersebut dengan melihat fenomena yang terjadi, memang spionase dalam masa damai telah tertinggal di belakang perubahan dalam norma-norma dan praktek pengumpulan informasi intelijen internasional. Norma-norma dan praktek pengumpulan informasi intelijen internasional jauh lebih berkembang dibanding norma yang mengatur mengenai spionase itu sendiri. Jika peraturan mengenai spionase yang dilakukan pada masa perang dalam *Hague Convention* IV 1907 diterapkan dalam permasalah spionase yang terjadi dewasa ini tentu tidak

[3] Kamus Besar Bahasa Indonesia dalam http://www.artikata.com/arti-351900-spionase.html

[4] Lt. Col. Geoffrey B. Demarest, 1996, ***Espionage in International Law,*** 24 Denv. J. Int'l L. & Pol'y 321, https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=24+Denv.+J.+Int%27l+L.+%26+Pol%27y+321&key=264b0db644528bcd78ae55fa62fec5f2, (diakses 24 Mei 2014)

sesuai. Selain kegiatan spionase dilakukan dalam masa perang, spionase juga dilakukan dengan cara yang konvensional. Bukan melalui media teknologi komunikasi dan informasi yang canggih.

Dimuat dalam vivanews.co.id pada tanggal 21 November 2013,[5] bahwa "*Akhir Oktober 2013, harian Fairfax mengungkap bahwa gedung Kedutaan Australia di beberapa negara Asia, termasuk Indonesia, digunakan sebagai pos penyadapan.*" Dalam konteks yang lebih luas tentang praktik penyadapan yang dilakukan oleh lembaga intelijen/aparat penegak hukum suatu negara, penyadapan tidak hanya dilakukan melalui jaringan telekomunikasi maupun secara elektronik. Informasi hasil penyadapan diperoleh melalui berbagai cara dan sumber, baik dengan menggunakan sarana teknologi, maupun dengan cara-cara konvensional. Sarana teknologi misalnya penggunaan *software* atau *hardware*/perangkat khusus intersepsi, baik dengan atau tanpa melalui jaringan telekomunikasi. Sedangkan cara konvensional bisa dilakukan dengan mendengarkan langsung tanpa alat dengan sembunyi-sembunyi, menguping pembicaraan, atau menggunakan peralatan non-elektronis untuk mendengarkan percakapan pihak yang disadap.[6]

Dilihat dari ciri khusus atau karakteristik dan jenis dan bentuk cybercrime, kegiatan spionase melalui penyadapan teknologi informasi atau alat telekomunikasi bisa tergolong dalam kategori *cybercrime*. Secara sederhana dapat langsung dimasukkan ke dalam jenis *cyber-espionage*, namun jika dipahami secara mendalam dapat masuk ke dalam bentuk dan/atau jenis *cybercrime* yang lain. Bukan hanya karena lain dari kejahatan konvensional tetapi pelaku juga mewakili suatu negara berdasarkan perintah dan merupakan pekerjaan yang semestinya. Berikut adalah karakteristik atau ciri khusus dari *cybercrime* yang sesuai dengan spionase; (1) *Unauthorized acces* atau akses tidak sah, (2) *Non-violance* (tanpa kekerasan), (3) Sedikit melibatkan kontak fisik (*minimaze of physical contact*), (4) Menggunakan peralatan (*equipment*), teknologi, dan

[5] Ita Lismawati F. Malau, Nila Chrisna Yulika, **Sadap Indonesia, Australia Langgar Konvensi Wina: Australia melancarkan aksi spionase kepada Indonesia**, http://politik.news.viva.co.id/news/read/460248-sadap-indonesia--australia-langgar-konvensi-wina, (diakses 31 Desember 2013)

[6] Teguh Arifiyadi, **Langkah Hukum Jika Disadap Negara Tetangga**, http://www.hukumonline.com/klinik/detail/lt5276f8bec3f65/langkah-hukum-jika-disadap-negara-tetangga, (diakses 4 Mei 2014)

memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global, (5) Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.

Kembali menganai penyadapan, Pada dasarnya penyadapan adalah satu cara dari kegiatan spionase. Karena dalam era modern ini spionase yang paling memungkan diakukan dengan sedikit resiko diketahui pihak yang dimata-matai adalah dengan penyadapan. Dengan kecanggihan teknologi informasi dan telekomunikasi, kegiatan dapat dilakuakan dari satu tempat tanpa harus mendengarkan, menguping, atau dengan cara konvensonal lainnya seperti spionase yang dilakukan pada jaman dahulu. Namun, dari segi karakteristik dan jenis mengenai penyadapan dan *cybercrime* jika diartikan masing-masing dapat ditarik satu kesamaan dari keduanya. Berikut adalah kesamaan baik spionase maupun penyadapan yang termasuk dalam *cybercrime* yang dalam hal ini adalah dilakukan antar negara; (1) *Unauthorized acces* atau akses tidak sah, (2) *Non-violance* (tanpa kekerasan), (3) sedikit melibatkan kontak fisik (*minimaze of physical contact*), (4) Menggunakan peralatan (*equipment*), teknologi, dan memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global, (5) Perbuatan yang dilakuakan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber (*cyberspace*), (6) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet, (7) Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional, (8) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.

Kemudian jika penyadapan termasuk dalam *cybercrime,* maka beberapa bentuk *cybercrime* yang ada, penyadapan sesuai dengan beberapa bentuk dibawah ini; (1) *Unauthorized Acces to Computer System and Service*, (2) *Cyber Espionage*, (3)*Infringements of Privacy*, dan (4) *Cyber-stalking*. Dari beberapa

karakteristik khusus dan bentuk *cybercrime*, tindakan penyadapan bisa dikategorikan ke dalam *cybercrime*. Dapat masuk ke salah satu atau beberapa dari bentuk yang telah dijelaskan diatas. Meskipun dalam pengertian yang sempit *cybercrime* hanya merujuk pada tindakan kejahatan dunia maya yang dilakukan dengan media komputer. Perkembangan serta pengertian penyadapan sendiri berdasar undang-undang saat ini, *cybercrime* sudah mengarah pada tindakan yang dilakukan bukan hanya dengan komputer. Tindakan baik penyadapan atau kejahatan lain dilakukan dengan media elektronik yang berhubungan dengan internet serta teknologi lain yang mendukung.

Peraturan Mengenai Spionase, Penyadapan dan Cybercrime

Peraturan internasional mengenai *cybercrime* terdapat dalam *Conventiom on Cybercrime* 2000. *Convention on Cybercrime* juga biasa disebut dengan *Budapest Covention*. Konvensi ini mencantumkan tindakan apa saja yang tergolong dalam *cybercrime*. Yang termasuk *cybercrime* dalam konvensi ini adalah *Illegal access*, *Illegal interception, Data interface, System interface, Misuse of devices, Computer-related forgery, dan Computer-related fraud***.** Kemudian dalam UNCLOS 1982 (*United Nations Convention Law Of The Sea*) juga terdapat satu pasal mengenai kegiatan pengumpulan informasi yang merugikan bagi pertahanan atau keamanan negara. Terdapat pada pasal 19 ayat (2) c mengenai Lintas Damai, pasal 19 ayat (2) c menyatakan "*setiap perbuatan yang bertujuan untuk mengumpulkan informasi yang merugikan bagi pertahanan atau keamanan negara pantai*". Jika diartikan sepintas pasal ini hanya diperuntukkan kegiatan kapal asing di perairan negara pantai, namun jika diartikan secara luas, yang dimaksud perbuatan atau kegiatan mengumpulkan informasi yaitu mengumpulkan informasi dalam bentuk apapun teramasuk spionase mealalui penyadapan merupakan kegiatan yang merugikan bagi pertahanan atau keamanan negara.

Di beberapa negara juga diatur mengenai spionase, penyadapan dan *cybercrime*. German Peraturan mengenai spionase serta spies atau intelejen serta *cybercrime* diatur dalam *German Criminal Code* atau *German Penal Code* atau dalam bahasa Jerman peraturan ini disebut dengan *Strafgesetzbuches*, dan

disingkat menjadi StGB.[7] Di Australia peraturan mengenai spionase terdapat dalam *Crimes Act* 1995 dan *Crimianl Code Amendement (Espionage and Relaed Matters) Bill* 2002. *Criminal Code Act* 1995 menyebutkan tindakan apa saja yang termasuk dalam spionase dan hukuman yang dapat dijatuhkan pada pelaku. Sedangkan *Criminal Code Amendement Bill 2000* adalah penambahan peraturan dari peraturan *Criminal Code Act* 1995 dan *Crimes Act* 1914.

Berbeda dengan German dan Australia, peraturan mengenai kejahatan dikodifikasi dalam satu *Ciminal Code*. Di USA peraturan mengenai spionase diatur khusus dalam *The Espionage Act of* 1917. Menurut *The Espionage Act of* 1917. Untuk cybercrime, USA mempunyai banyak peraturan dimana tiap tindakan dikelompokkan, beberapa diantaranya yaitu *Computer Software Privacy and Control Act, Department of Justice - Computer Crime and Intellectual Property Section, Electronic Communications Privacy Act, Electronic Communications Privacy Act, Economic Espionage Act (EEA), Communications Assistance for Law Enforcement Act (CALEA)* dan masih banyak lagi. Sedangkan peraturan mengenai intersepsi atau penyadapan terdapat dalam *Communications Assistance for Law Enforcement Act of* 1994 (CALEA).

Terlepas dari pasal mengenai *spies* dalam *Hague Convention IV* 1907, sama halnya dengan dunia Internasional, di Indonesia pengaturan khusus mengenai spionase juga tidak ada. Namun dicantumkan dalam beberapa Undang-undang, pengaturan sekilas mengenai penyadapan yang bisa dikatakan sebagai bentuk baru dari spionase dalam perkembangan teknologi dan informasi sekarang. Undang-undang yang mencantumkan sekilas mengenai penyadapan in adalah Undang-undang No.36 Tahun 1999 tentang Telekomunikasi dan Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Poin dari kedua Undang-undang tersebut adalah bahwa Penyadapan merupakan kegiatan yang dilarang. Lain dengan Undang-undang tentang Telekomunikasi dan Undang-undang tentang Informasi dan Transaksi Elektronik, Peraturan Menteri NO: 11/PER/M.KOMINFO/02/2006 tentang Teknis Penyadapan Terhadap Informasi, merupakan salah satu peraturan yang memperbolehkan penyadapan. Penyadapan

[7] http://en.wikipedia.org/wiki/Strafgesetzbuch, (diakses 3 Juni 2014).

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]

Pemberitaan media yang merespon paparan informasi dari harian berita Australia, *Australian Broadcasting Corporation* (ABC) dan *Sydney Morning Herald* mengenai dokumen penyadapan pejabat tinggi Indonesia menjadi puncak dari berbagai pemberitaan mengenai negara tetangga di sebelah tenggara tersebut.[9] Di Indonesia, Anggota Komisi I DPR Meutya Hafid meminta agar Pemerintah mengusir Duta Besar Australia Greg Moriarty dari Indonesia. Bukan tanpa alasan, pengusiran itu bisa dilakukan karena Australia telah melanggar Pasal 9 Konvensi Wina tahun 1961 mengenai hubungan diplomatik. Dalam pasal itu disebutkan pengusiran kepada duta besar bisa dilakukan jika wakil diplomatik itu melanggar tiga hal. Pertama, duta besar melakukan kegiatan yang subversif dan merugikan kepentingan nasional. Kedua, kegiatan yang dilakukan oleh wakil diplomatik melanggar hukum atau perundang-undangan negara penerima. Ketiga kegiatan yang digolongkan sebagai kegiatan mata-mata atau spionase yang dapat mengganggu stabilitas keamanan negara penerima.[10]

Menanggapi hal ini, jika terbukti Australia telah melakukan penyadapan kepada Indonesia dengan tujuan spionase, maka pemeritah perlu menanggapi dan menangani hal ini dengan cermat. Pertama, kegiatan penyadapan ini dilakukan di Indonesia. Maka hukum indonesia dapat diberlakukan sesuai aturannya. Dimana kegiatan penyadapan yang tidak sah atau *unlawfull interception* merupakan

---

[8] 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).

[9] R. Aj. Rizka F. Prabaningtyas, **Indonesia–Australia: Menguji Persahabatan di Tengah Konflik Penyadapan**, Institute of International Studies Universitas Gadjah Mada, https://www.iis.fisipol.ugm.ac.id. (Diakses 12 Jui 2014)

[10] Ita Lismawati F. Malau, Nila Chrisna Yulika, **Sadap Indonesia, Australia Langgar Konvensi Wina: Australia melancarkan aksi spionase kepada Indonesia**, http://politik.news.viva.co.id/news/read/460248-sadap-indonesia--australia-langgar-konvensi-wina, (diakses 31 Desember 2013)

pelanggaran hukum di Indonesia. Terlepas dari masalah dalam sisi hubungan diplomatik, tindakan yang dilakukan Australia memang bertentangan dengan hukum nasional Indonesia. Selain itu pun dalam konvensi internasional juga dikatakan bahwa *illegal interception* merupakan salah satu dari *cybercrime*. Terkait penyadapan dalam hukum nasional Indonesia, kegiata ini secara tegas dilarang kecuali dilakukan oleh pihak yang berwenang. Sesuai dengan bentuk penyadapan dan *cybercrime* di Indonesia tindakan Australia dapat dipastikan melanggar hukum Indonesia. Apabila tindakan penyadapan dilakukan oleh agen tertentu yang ditugaskan untuk melakukan spionase maka hukum nasional dapat diberlakukan kepada agen tersebut. Jika tindakan secara langsung dilakukan oleh wakil diplomatik Australia untuk Indonesia, maka yang dapat dilakukan adalah pengusiran wakil diplomik.

IV. PENUTUP

Dilihat dari beberapa karakteristik *cybercrime* terhadap spionase dan penyadapan, maka spionase melalui penyadapan dapat dikategorikan sebagai cybercrime. Karakteristik yang pertama *Unauthorized acces* atau akses tidak sah, kegiatan spionase merupakan kegiatan yang *Non-violance* (tanpa kekerasan), Sedikit melibatkan kontak fisik *(minimaze of physical contact*), menggunakan peralatan *(equipment*), teknologi, dan memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global, Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional. Selain itu berdasarkan bentuk dari cybercrime maka penyadapan dapat masuk di beberapa bentuk seperti; *Unauthorized Acces to Computer System and Service*, *Cyber Espionage*, *Infringements of Privacy*, dan *Cyber-stalking.*

Berdasarkan hukum nasional Indonesia, Undang-undang No.36 Tahun 1999 tentang Telekomunikasi dan Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tindakan yang dilakukan Australia melanggar hukum nasional Indonesia. Namun, dalam permasalahan ini tidak dapat begitu saja menerapkan hukum nasional meskipun tindakan yang dilakukan Australia

adalah melanggar hukum nasional. Selain dengan penyelesaian melalui penyelesaian diplomatik. Persoalan antar negara ini juga dapat diselesaikan melalui Mahkamah Internasional atau International Court of Justice.

DAFTAR PUSTAKA

Didik M. Arief Mansur, Elisatris Gultom, 2005, ***Cyber Law*: Aspek Hukum Teknologi Informasi**, Refka Aditama, Bandung.

INTERNET

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. (28 Februari 2014).

http://en.wikipedia.org/wiki/Strafgesetzbuch (3 Juni 2014).

Ita Lismawati F. Malau, Nila Chrisna Yulika, **Sadap Indonesia, Australia Langgar Konvensi Wina: Australia melancarkan aksi spionase kepada Indonesia**, http://politik.news.viva.co.id/news (31 Desember 2013)

Kamus Besar Bahasa Indonesia, http://www.artikata.com/arti-351900-spionase.html

Lt. Col. Geoffrey B. Demarest, 1996, ***Espionage in International Law,*** 24 Denv. J. Int'l L. & Pol'y 321, https://litigation-essentials.lexisnexis.com (24 Mei 2014)

R. Aj. Rizka F. Prabaningtyas, **Indonesia–Australia: Menguji Persahabatan di Tengah Konflik Penyadapan**, Institute of International Studies Universitas Gadjah Mada, https://www.iis.fisipol.ugm.ac.id (12 Juni 2014)

Teguh Arifiyadi, **Langkah Hukum Jika Disadap Negara Tetangga**, http://www.hukumonline.com (4 Mei 2014)