DIPLOMASI PERTAHANAN INDONESIA TERHADAP AUSTRALIA PASCA SKANDAL PENYADAPAN

INDONESIA-AUSTRALIA DEFENSE DIPLOMACY TOWARDS POST TAPPING SCANDAL

Prasetyo[1]

Dosen Universitas Pertahanan Indonesia
(pr483tyo@gmail.com)

Abstrak – Penyadapan informasi secara tidak sah merupakan suatu tindakan melanggar hukum yang dapat mengganggu privasi seseorang. Namun dalam konteks antar negara, penyadapan sebenarnya biasa dilakukan untuk mengetahui niat yang sebenarnya dari suatu negara, terutama yang berkaitan dengan kepentingan nasional negara yang melakukan penyadapan. Disamping itu, informasi yang lebih rinci mengenai kebijakan dan implementasinya perlu diketahui agar dapat melakukan tindakan antisipasi dan mencegah pendadakan. Tindakan penyadapan secara tidak sah merupakan tindakan tercela dan melanggar etika diplomasi, terutama jika diterapkan terhadap negara sahabat sebagaimana yang diakukan oleh Australia terhadap Indonesia. Oleh sebab itu perlu diambil langkah yang tegas namun tepat dan terukur.

Kata Kunci: penyadapan, intelijen, spionase, diplomasi

Abstract *- Unauthorized wiretapping is an unlawful act which may interfere with a person's privacy. However, in the context of inter-state, tapping is actually a common practice, performed to determine the actual intentions of a country, especially with regard to the national interests. Besides, detailed information about the policy and its implementation needs to be known in order to anticipate and prevent acts of surprise. Unauthorized wiretapping is a disgraceful act and a violation of ethics diplomacy, especially if applied to friendly countries as carried out by Australia toward Indonesia. Therefore it is necessary to take bold steps yet precise and measurable actions.*

Keywords: *tapping, intelligence, espionage, diplomacy*

Pendahuluan

Kunjungan Perdana Menteri Australia ke Indonesia pada awal Juni lalu antara lain untuk membahas upaya perbaikan hubungan yang sempat memburuk karena kasus penyadapan di lingkungan Istana Kepresidenan oleh Intelijen Australia. Pertemuan ini merupakan yang pertama kalinya dilakukan oleh kedua kepala negara ini. Kunjungan Abbott ke Indonesia merupakan pertama kalinya pasca kasus penyadapan yang dilakukan

[1]Prasetyo, S.IP., M.Sc., adalah anggota Tim Dosen Mata Kuliah Dinamika Terorisme di Universitas Pertahanan Indonesia Program Studi *Asymmetric Warfare*.

pihak Australia kepada SBY beserta keluarganya. Indonesia dan Australia akhirnya sepakat akan menandatangani kode etik untuk menjamin tidak ada lagi penyadapan yang mengganggu hubungan diplomatik kedua negara.

Seperti diketahui bahwa di penghujung tahun 2013, media massa di Indonesia disibukkan dengan berita-berita tentang kasus penyadapan oleh Australia, yang dibocorkan oleh seorang mantan staf lembaga intelijen Amerika Serikat, Edward Snowden. Untuk ulahnya itu, Snowden telah dikejar oleh pemerintah AS, paspornya dicabut dan didakwa atas kasus spionase sehingga terpaksa meminta suaka di beberapa negara di dunia. Seberapa penting sebenarnya informasi yang dibocorkan tersebut? Padahal kita tahu bahwa kegiatan penyadapan itu kiranya sudah menjadi rahasia umum.

Setiap negara pasti ingin mengetahui niat negara lain terutama yag berkaitan langsung dengan kepentingan nasionalnya. Untuk itulah mereka mengirimkan misi diplomatik ke negara negara lain dengan maksud untuk menjalin hubungan kerja sama dan persahabatan namun sekaligus juga berusaha memahami sejarah, kondisi dan perkembangan sosial budaya, ekonomi, ilmu pengetahuan dan teknologi, politik dan militer. Disamping itu, data yang sering diminati adalah kondisi geografi, demografi dan biografi serta sikap para pemimpinnya. Tanpa penyadapan pun, di era informasi dan keterbukaan seperti sekarang ini, sebenarnya tidak sulit untuk mendapatkan keterangan-keterangan yang sangat diperlukan dalam rangka penyusunan strategi diplomasi, termasuk didalamnya diplomasi pertahanan. Katakanlah jika kita ingin mengetahui rencana anggaran dan pendapatan negara atau rencana pembangunan misalnya, sekarang ini semua telah dibeberkan dengan transparan dan pembahasannya di DPR pun juga dilakukan secara terbuka.

Kebijakan dan strategi pertahanan setiap negara biasanya juga sudah dibeberkan dalam Buku Putih (*White Paper*). Jika ingin mengetahui jumlah dan disposisi instalasi militer, tinggal membuka internet atau *google earth,* maka semua ada disana. Dari informasi sampah hingga informasi yang betul-betul berguna, termasuk lokasi-lokasi markas militer. Bahkan, beberapa pemimpin negara menggunakan media sosial seperti *facebook* dan *twitter* untuk berkomunikasi dengan rakyatnya, jadi sebenarnya nyaris tidak ada lagi rahasia. Komunikasi antar negara sahabat melalui jalur resmi juga tersedia apabila ada hal spesifik yang ingin diketahui oleh pejabat diplomatik, sehingga sedikit sekali

alasan untuk melakukan aksi penyadapan di masa keterbukaan ini, bahkan jika dilakukan dan ketahuan hanya akan melukai perasaan dan mengganggu persahabatan antar negara.

Masalahnya adalah secara alamiah manusia memang selalu diliputi rasa ingin tahu, dan ingin tahu lebih banyak. Apalagi kalau terdapat kemungkinan dapat mempengaruhi atau menghalangi hajat hidup dan kepentingannya. Konsep kepentingan nasional, keamanan nasional dan pertahanan nasional yang umum digunakan untuk mendukung kegiatan rahasia. Bagi negara yang memiliki kemampuan dan kebutuhan untuk melakukan kegiatan dan operasi rahasia menganggap hal tersebut sah-sah saja[2]. Sehingga aksi penyadapan menjadi kegiatan yang seolah-olah 'biasa', tentu saja dengan catatan asal jangan sampai ketahuan.

Apa yang Ingin Diketahui?

Informasi apa saja yang mendorong suatu negara untuk mengetahui secara diam-diam sehingga melakukan penyadapan? Biasanya di luar informasi umum tentang situasi dan kondisi suatu negara yang mudah didapatkan melalui sumber terbuka ada saja hal-hal yang ingin diketahui lebih jauh dan tidak dibuka secara umum. Informasi mengenai niat terselubung dari para pemimpin misalnya, tentu tidak akan dapat diperoleh melalui sumber terbuka. Demikian pula rencana rahasia dalam bidang politik dan ekonomi yang dibutuhkan guna mengatur strategi politik atau bisnis, sudah tentu hal semacam ini harus didapatkan secara diam-diam. Keterangan mengenai sistem dan pelaksanaan pemilihan umum, elektabilitas tokoh, suksesi, putra mahkota, bisnis keluarga dan semacamnya, merupakan informasi yang menarik sebagai pelengkap komponen biografi pemimpin, yang berguna bagi penopang analisis arah perkembangan politik dari suatu negara. Intinya, semakin lengkap informasi yang dimiliki akan semakin mudah untuk 'menaklukkan' suatu negara, yaitu dengan menggunakan *soft power*. Sebagian pengetahuan mengenai hal diatas dapat diperoleh secara terbuka, tetapi selalu diinginkan substansi yang lebih esensial yaitu informasi dari dalam yang sering merupakan informasi yang bersifat tertutup atau *untold story*. Semakin banyak dan lengkap informasi dari

[2] "Etika dan Moral Intelijen", *Jurnal Intelijen dan Kontra Intelijen*, Volume VI, No. 36, tahun 2012, hlm.62.

dalam dianggap akan semakin akurat analisis dan prediksi yang disusun oleh ahli atau badan yang bertugas untuk itu.

Dalam bukunya "*The Art of War*", yang hingga kini masih menjadi rujukan banyak orang, terutama yang berkecimpung dalam dunia strategi, Sun Tzu mengatakan bahwa: [3]

Prior information
Enables wise rulers
And worthy generals
To move
And conquer,
Brings them success
Beyond that of multitude.

This information
Cannot be obtained
From spirits;
It cannot be deduced
By analogy;
It cannot be calculated
By measurement.

It can be obtained only
From men,
From those who know
The enemy's dispositions.

Dalam buku dengan judul sama "*The Art of War*" oleh Sun Tzu, terbitan Sambhala Publications Inc, terdapat kutipan yang artinya dalam bahasa Indonesia kurang lebih: "Kenali dirimu, kenali musuhmu, seribu kali perang, seribu kali menang", atau dalam bahasa Inggris: "*Also in the military - knowing the other and knowing oneself, in one hundred battles no danger. Not knowing the other and knowing oneself, one victory for one loss. Not knowing the other and not knowing oneself, in every battle certain defeat*".[4] Untuk mengenali 'negara musuh' atau 'siapa tahu suatu saat bisa berubah menjadi musuh' inilah badan pengumpul intelijen suatu negara, agar tidak terdadak, giat mencari, mengumpulkan dan mengolah kepingan-kepingan informasi yang sepintas tidak memiliki nilai apa-apa, tetapi dengan pengalaman dan kemampuan analisis yang tajam dapat saja berubah menjadi informasi yang bermanfaat.

Jono Hatmojo dalam bukunya "Intelijen Sebagai Ilmu" menyatakan bahwa badan pengumpul intelijen umumnya dihadapkan kepada tiga persoalan atau pertanyaan fundamental, yaitu: 1. Apa sebenarnya niat musuh (bisa juga negara tetangga atau negara sahabat), 2. Kebijakan apa yang direncanakan untuk mencapai niat tersebut, dan 3. Bagaimana pelaksanaan kebijakan tersebut.[5] Mengapa 'niat yang sebenarnya' menjadi kepedulian utama dalam pengumpulan intelijen? Hal ini disebabkan karena dalam prakteknya, apa yang diucapkan atau diumumkan secara terbuka tidak sama atau bahkan

[3]Sun Tzu, *The Art of War*, (New York: Penguins Books, 2003), hlm. 90-91.

[4] Sun Tzu, *The Art of War*, (Boston: Sambhala Publications Inc., 2002), hlm.12.

[5] Jono Hatmojo, *Intelijen Sebagai Ilmu*, (Jakarta: Balai Pustaka, 2003), hlm.49-50.

tidak jarang bertentangan dengan niat yang sebenarnya. Dengan mengetahui niat yang sebenarnya inilah akan menjadi lebih mudah ditebak setiap langkah atau manuver yang dilakukan oleh suatu negara dan dapat diambil tindakan antisipasi dan kebijakan yang tepat dalam menyikapinya.

Dalam kasus skandal penyadapan Australia terhadap tokoh-tokoh politik dan negarawan Indonesia bahkan termasuk menyadap telepon seluler Ibu Negara Ani Yudhoyono sebagaimana diberitakan oleh Liputan6.com [6] dipicu oleh sebuah kabel diplomatik yang dikirim oleh Kedutaan Besar AS di Jakarta kepada Diplomat AS di Canberra dan juga untuk CIA, pada 17 Oktober 2007. Kabel diplomatik tersebut juga menuliskan tentang 'dinamika baru' dalam keseimbangan kekuatan politik Indonesia dengan munculnya seorang 'pemain' yang menjadi satu-satunya penasihat paling berpengaruh bagi Presiden SBY. Keputusan menjadikan telepon selular Ani sebagai target merupakan bagian dari strategi Pemerintah Australia yang disengaja dan diperhitungkan yaitu untuk mempelajari lebih lanjut tentang pergeseran keseimbangan kekuasaan di dalam elit penguasa di Indonesia. Apalagi sang Ibu Negara dianggap sudah menyiapkan putera sulungnya sebagai presiden selanjutnya.

Cara yang Digunakan Untuk Menggali Informasi

Banyak cara untuk mengumpulkan informasi yang diinginkan, diantaranya melalui sumber terbuka seperti berita media massa, buku-buku biografi, produk hukum yang dipublikasikan secara luas, melalui internet dan sumber terbuka lainnya, serta menggali melaluisumber tertutup seperti penggunaan intelijen manusia (*Human Intelligence*/Humint), dan intelijen teknik (*Technical Intelligence*). Andi Wijayanto dkk, dalam bukunya "Intelijen: *Velox et Exactus*", mengutip Abram N. Shulsky dan Gary J. Scmith,[7] membagi metode kerja, metode pengumpulan data dan analisa intelijen dalam dua kategori, sebagai berikut: [8]

[6] Liputan6.com, "Ini Alasan Australia Sadap Ani Yudhoyono", dalam http://news.liputan6.com/read/774976/ini-alasan-australia-sadap-ani-yudhoyono, diunduh pada 23 Januari 2014.

[7]Abram N. Shulsky dan Gary J. Scmith, *Silent Warfare: Understanding the World of Intelligence*, (Dulles, Virginia: Brasseys's Inc., 2002).

[8] Andi Wijayanto, et.al, *Intelijen: Velox et Exactus*, (Jakarta: Pacivis dan Kemitraan, 2006), hlm. 47.

Metode Kerja	Metode Pengumpulan Data	Analisa Intelijen
Human Intelligence	*Official Cover*	*Basic Research - Data Banks*
	Non-official cover	
	Tradecraft	
	Defectors	
Technical Intelligence	*Photint/Imint*	*Photo Intepretation*
	Sigint	*Cryptanlysis*
	Comint	*Cryptanlysis*
	Telint	*Telemetry Analysis*
	Elint	*Cryptanlysis*
	Masing	*Sensor Analysis*

Sumber: Andi Wijayanto, et.al, *Intelijen: Velox et Exactus*, (Jakarta: Pacivis dan Kemitraan, 2006), hlm. 47.

Human Intelligence (Humint) berkaitan dengan penggunaan agen-agen intelijen untuk mendapatkan keterangan baik dari sumber terbuka maupun tertutup, sedangkan *Technical Intelligence* (*Techint)* berkaitan dengan teknologi informasi. Amerika Serikat dan Inggris telah mengoperasikan lebih dari 120 satelit intelijen yang digunakan untuk pengumpulan data strategis. Sistem satelit yang dikenal sebagai *international leased carrier* ini diluncurkan sejak 1971 dan didukung oleh situs-situs pencegat darat di Morwenstow, Cornwall (Inggris); Yakima, Washington State (AS); Sugar Grove, West Virginia (AS); Sabana Seca (AS); Litrim, Ontario (Kanada); Kojarena, Western Australia (Australia); dan Waihopai, South Island (Selandia Baru).[9]

Aksi-aksi Penyadapan

Aksi penyadapan sudah sejak lama dilakukan orang. Masih ingat kasus skandal penyadapan Watergate yang telah menjungkalkan Nixon dari Gedung Putih? Wartawan *The Washington Post*, Bob Woodward dan rekannya Carl Bernstein yang mendapat informasi rahasia dari seseorang yang menyebut dirinya sebagai "*deepthroat*", telah menyibak rahasia penyadapan di kantor kampanye Partai Demokrat AS di komplek Watergate[10]. Sekedar contoh lain adalah skandal yang melibatkan konspirasi tingkat

[9]*Ibid.*, hlm.48.

[10]Faried Cahyono dan Fahmi Indrayadi, *Misteri Operasi Intelijen*, (Jakarta: Indomedia Publishing, 2007), hlm. 113-118.

tinggi dan spionase yang dilakukan oleh mantan petinggi intelijen kepolisian dan kepala satuan khusus antiteror Filipina, Michael Ray Aquino, dan Leandro Aragoncillo yang telah membobol lebih dari 100 dokumen mengenai Filipina dari database komputer FBI.[11]

Hubungan erat Amerika dengan Israel ternyata juga tidak menghambat organisasi intelijen Israel untuk melakukan penyadapan terhadap para pejabat Amerika Serikat. Claire Hoy dan Victor Ostrovsky dalam bukunya yang berjudul "MOSSAD", membeberkan banyak sekali aksi penyadapan yang dilakukan oleh Badan Intelijen Israel Mossad, termasuk di Amerika Serikat. Sebagian cuplikannya:

> "Ada momentum yang berkembang di Amerika Serikat untuk mencapai penjajaran (pengaturan) damai tertentu. Bahkan Arab mulai melihat keuntungan hal ini, dan Mossad, melalui jaringan alat pendengar rahasia elektronik mereka di rumah-rumah dan kantor-kantor berbagai Kedutaan Besar Arab dan pemimpin di New York serta Washington, mengetahui bahwa PLO cenderung setuju dengan posisi Kissinger tahun 1975 dan mengakui hak Israel untuk eksis".[12]

Aksi penyadapan juga banyak dilakukan oleh aparat yang berwenang untuk membantu membongkar jaringan kejahatan. Sekedar contoh, Ken Conboy dalam bukunya "*The Second Front*" mengisahkan bahwa dalam upaya membongkar jaringan terorisme di Asia Tenggara, penyadapan dilakukan terhadap hubungan telepon Zubair untuk mengungkap keberadaan kelompok Nurdin M Top dan Hambali.[13]

Penyadapan Tetangga Selatan[14]

- Tahun 1950-an, Duta Besar Australia di Indonesia, Sir Walter Crocker (1955-1956), mengakui lembaga sandi Australia, *Defense Signal Directorate* (*Australian Signal Directorate*), secara rutin memecahkan sandi diplomatik Indonesia sejak pertengahan 1950. Kedutaan Besar Australia di Jakarta menjadi stasiun pertama Badan intelijen Australia, *Australian Secret Intelligence Service* (ASIS), di luar negeri.

[11] *Ibid.,* hlm.124.

[12] Claire Hoy dan Victor Ostrovsky, *Mossad, Tipu Daya yang Dibeberkan oleh Mantan Agen Dinas Rahasia Israel* (Judul asli *By Way of Deception*), (Ciputat, Tangerang: Binarupa Aksara, 2007), hlm.482.

[13] Ken Conboy, *The Second Front*, (Jakarta, Singapore: Equinox Publishing, 2006), hlm. 202-3.

[14] "Dokumen Yang Memanaskan Jakarta", *Majalah Tempo*, 25 November – 1 Desember 2013, hlm. 121.

- Tahun 1960-an, Badan intelijen sinyal Inggris, *Government Communications Headquarter* (GCHQ), membantu *Defence Signal Directorate* memecahkan kunci alat sandi produksi Swedia, Hagelin, yang digunakan Kedutaan Besar Indonesia di Darwin Avenue, Canberra.
- Tahun 1970-an, Pos pemantauan lainnya adalah stasiun Penerima Shoal Bay di dekat Darwin. Fasilitas ini menargetkan komunikasi militer Indonesia, dioperasikan dari markas besar DSD di Russel Hill, Canberra.
- Tahun 1980-an, *Defence Signal Directorate* mengoperasikan intersepsi sinyal dan pemantauan di Kepulauan Cocos, 1.100 km barat daya Pulau Jawa. Fasilitasnya meliputi radio pengawasan, pelacak arah, dan stasiun satelit bumi.
- Tahun 1990-an, Laporan detail proyek pengintaian global bersandi 'Echelon' oleh *United Kingdom-United States of America Agreement* (UKUSA) terbuka untuk publik. Program bersama ini memberi Australia, sebagai partner UKUSA, akses luas ke komunikasi satelit dan telepon.
- Tahun 2007, intelijen Australia dan Amerika Serikat mengumpulkan informasi nomor kontak pejabat Indonesia saat Konferensi Perubahan Iklim pada 2007 di Bali. Operasi ini dilakukan dari stasiun di Pine Gap, yang dijalankan dinas intelijen Amerika, CIA, dan Departemen Pertahanan Australia.
- Tahun 2013, ASD mengoperasikan program bersandi Stateroom, memanfaatkan fasilitas diplomatik Australia di berbagai negara, termasuk Indonesia. Menurut dokumen Edward Snowden, ASD sudah melakukannya sejak 1980-an.

Dari data diatas terbukti bahwa aksi penyadapan terhadap Indonesia bukanlah merupakan 'barang baru', bahkan sudah dimulai saat negara Republik Indonesia baru berumur lima tahun, dan kita tidak mampu berbuat apa-apa.

Pelibatan Negara-Negara Lain

Dua negara sahabat Indonesia, Singapura dan Korea Selatan, disebut-sebut memainkan peran kunci membantu Amerika Serikat dan Australia dalam menyadap jaringan

telekomunikasi di seluruh Asia. Demikian menurut dokumen rahasia yang dibocorkan mantan kontraktor intelijen AS, Edward Snowden.

Seperti dikabarkan surat kabar Australia, *The Age*, Senin 25 November 2013, dengan judul artikel *"Singapore, South Korea revealed as Five Eyes spying partners"*, [15] yang dikutip oleh E.Y. Kristanti dalam sebuah artikel liputan6.com dengan judul artikel "Snowden: Singapura Diduga Bantu AS-Australia Sadap Indonesia",[16] bahwa peta rahasia Badan Keamanan AS (NSA) mengungkap AS dan partner berbagi intelijennya atau yang dikenal dengan *'Five Eyes'*, menyadap kabel serat optik berkecepatan tinggi di 20 lokasi di seluruh dunia. Operasi penyadapan tersebut melibatkan kerja sama dengan pemerintahan lokal dan perusahaan telekomunikasi atau melalui operasi 'diam-diam dan rahasia'. Operasi intersepsi kabel bawah laut adalah bagian dari jaringan global, yang dalam dokumen perencanaan NSA yang dibocorkan, memungkinkan kemitraan *Five Eyes* – AS, Inggris, Australia, Kanada, dan Selandia Baru – melacak 'siapapun, di mana pun, kapan saja', dalam apa yang digambarkan sebagai "zaman keemasan" sinyal intelijen. Peta NSA, yang dipublikasikan koran Belanda, *NRC Handelsblad* menunjukkan bahwa AS mempertahankan cengkeramannya pada saluran komunikasi trans-Pasifik dengan fasilitas intersepsi di pantai Barat Amerika Serikat, juga di Hawaii dan Guam -- menyadap lalu lintas kabel komunikasi di Samudera Pasifik serta saluran komunikasi antara Australia dan Jepang. Peta itu juga mengonfirmasi bahwa Singapura, salah satu pusat komunikasi dunia, menjadi 'pihak ketiga' yang bekerja sama dengan 'Five Eyes'.[17]

Pada Agustus 2013, *Fairfax Media* melaporkan, badan mata-mata elektronik Australia, *Defence Signals Directorate* (DSD) bekerjasama dengan intelijen Singapura untuk menyadap kabel SEA-ME-WE-3 yang membentang dari Jepang, melintasi Singapura, Djibouti, Suez, Selat Gibraltar, ke Jerman Utara. Sumber-sumber intelijen Australia kepada Fairfax mengatakan bahwa divisi intelijen dan keamanan yang amat rahasia pada Kementerian Pertahanan Singapura bekerjasama dengan DSD dalam rangka mengakses

---

[15]"Singapore, South Korea revealed as Five Eyes spying partners", *The Age*, 25 November 2013, dalam http://www.theage.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html , diunduh pada 22 Juli 2014.

[16]E. Y.Kristanti, "Snowden: Singapura Diduga Bantu AS-Australia Sadap Indonesia", dalam http://news.liputan6.com/read/755644/snowden-singapura-diduga-bantu-as-australia-sadap-indonesia, 25 November 2013, diunduh pada 23 Januari 2014.

[17] *Ibid.*

dan berbagi komunikasi yang dibawa oleh kabel SEA-ME-WE-3 dan SEA-ME-WE-4 yang membentang dari Singapura ke kawasan selatan Prancis. Ahli intelijen Australia dari *Australian National University*, Profesor Des Ball mendeskripsikan, sinyal intelijen Singapura 'mungkin yang paling maju' di Asia Tenggara, setelah pertama kali dikembangkan dalam kerjasama dengan Australia di pertengahan 1970-an dan kemudian memanfaatkan posisi Singapura sebagai pusat telekomunikasi regional. Indonesia dan Malaysia disebut-sebut sebagai target kunci kerja sama intelijen Australia dan Singapura sejak 1970-an. Banyak rute lalu lintas telekomunikasi dan internet dua negara melewati Singapura.[18]

Peta rahasia NSA yang dibocorkan juga menunjukkan, Korea Selatan adalah titik kunci intersepsi di mana kabel di Busan menyediakan akses ke komunikasi internal Cina, Hong Kong, dan Taiwan. Badan Intelijen Korsel selama ini diduga menjadi kolaborator bagi Badan Pusat Intelijen AS (*US Central Intelligence Agency*), NSA, juga Badan Intelijen Australia. Peta NSA dan dokumen lain yang dibocorkan oleh Snowden dan diterbitkan oleh surat kabar Brasil, *O Globo,* juga mengungkapkan detail baru pada integrasi fasilitas penyadapan sinyal intelijen *Five Eyes* di Australia dan Selandia Baru. Dan untuk pertama kalinya, diungkap fasilitas penyadapan satelit DSD di Kojarena, dekat Geraldton di Australia Barat dengan kode 'STELLAR'. Fasilitas serupa di Waihopai, Selandia Baru diberi kode "IRONSAND". Sementara, fasilitas DSD di Shoal Bay dekat Darwin tidak diidentifikasi. Namun ketiganya terdaftar oleh NSA sebagai fasilitas primer pengumpulan satelit komunikasi asing (FORNSAT). Pemantauan komunikasi satelit di seluruh Asia dan Timur Tengah juga didukung fasilitas NSA di pangkalan Angkatan Udara AS di Misawa, Jepang, fasilitas diplomatik AS di Thailand dan India. Juga fasilitas *Government Communications Headquarters* (GCHQ) Inggris di Oman, Nairobi Kenya, dan pangkalan militer Inggris di Cyprus. Bocoran peta NSA juga menunjukkan kabel bawah laut yang diakses NSA dan GCHQ melalui fasilitas militer di Djibouti dan Oman, memastikan pemantauan maksimum terhadap komunikasi di Timur Tengah dan Asia Selatan.[19]

[18] *Ibid.*

[19] *Ibid.*

Pengertian dan Ketentuan Penyadapan dalam Perspektif Hukum

Situs web BPHN (Badan Pembinaan Hukum Nasional t.thn.) memuat beberapa Undang-Undang yang terkait dengan tindak penyadapan, antara lain:[20]

- Undang-Undang Nomor 5 Tahun 1997 Tentang Psikotropika, Pasal 55 mengatur bahwa: Selain yang ditentukan dalam Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Tahun 1981 Nomor 76, Tambahan Lembaran Negara Nomor 3209), penyidik polisi negara Republik Indonesia dapat menyadap pembicaraan melalui telepon dan/atau alat telekomunikasi elektronika lainnya yang dilakukan oleh orang yang dicurigai atau diduga keras membicarakan masalah yang berhubungan dengan tindak pidana psikotropika. Jangka waktu penyadapan berlangsung untuk paling lama 30 (tiga puluh) hari.
- Penjelasan Pasal 55 : Pelaksanaan teknik penyidikan penyerahan yang diawasi dan teknik pembelian terselubung serta penyadapan pembicaraan melalui telepon dan/atau alat-alat telekomunikasi elektronika lainnya hanya dapat dilakukan atas perintah tertulis Kepala Kepolisian Negara Republik Indonesia atau pejabat yang ditunjuknya.
- Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang, Pasal 31 :

  Berdasarkan bukti permulaan yang cukup sebagaimana dimaksud dalam pasal 26 ayat (4),penyidik berhak: menyadap pembicaraan melalui telepon atau alat komunikasi lain yang diduga digunakan untuk mempersiapkan, merencanakan, dan melakukan tindak pidana terorisme.

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, mengatur tata cara melakukan penyadapan, khususnya pasal 42 :

(1) Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima, oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya.

[20]"Penyadapan", Hukum Acara Pidana dan Peraturan Terkait", dalam http://acarapidana.bphn.go.id/proses/penyadapan/?s=penyadapan&type=all, diunduh pada 4 Februari 2014.

(2) Untuk keperluan proses peradilan pidana, penyelenggara jasa telekomunikasi dapat merekam informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi serta dapat memberikan informasi yang diperlukan atas :

a. permintaan tertulis Jaksa Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu;

b. permintaan penyidik untuk tindak pidana tertentu sesuai dengan Undang-undang yang berlaku.

(3) Ketentuan mengenai tata cara permintaan dan pemberian rekaman informasi sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 42 :

Ayat (2) Yang dimaksud dengan proses peradilan pidana dalam ketentuan ini mencakup penyidikan, penuntutan, dan penyidangan.

Huruf a: Yang dimaksud dengan tindak pidana tertentu adalah tindak pidana yang diancam dengan pidana penjara selama 5 (lima) tahun ke atas, seumur hidup atau mati.

Huruf b: Contoh tindak pidana tertentu sesuai dengan Undang-undang yang berlaku ialah tindak pidana yang sesuai dengan Undang-undang tentang Narkotika dan tindak pidana yang sesuai dengan Undang-undang tentang Psikotropika.

Undang-Undang Nomor 11 Tahun 2008 Tentang ITE, Pasal 31 :

(3) Kecuali intersepsi sebagaimana dimaksud padaayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Kolom Opini dalam situs web ICW (*Indonesian Corruption Watch)* mengutip sumber Kompas tanggal 15 Juli 2009, menyatakan antara lain bahwa:[21] Berdasarkan UU Telekomunikasi, penyadapan merupakan perbuatan pidana. Secara eksplisit ketentuan Pasal 40 undang-undang tersebut menyatakan bahwa setiap orang dilarang melakukan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apa pun. Pasal 56 menegaskan, barang siapa melanggar ketentuan sebagaimana dimaksud Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun. Sebagai perbuatan pidana, penyadapan dapat dipahami mengingat ketentuan dalam konstitusi yang menyatakan tiap orang berhak untuk berkomunikasi dan mendapat informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang ada (Pasal 28F UUD 1945).

Demikian pula Pasal 28G Ayat (1) UUD 1945 menyatakan, tiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang ada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.[22]

Dari ketentuan perundangan di atas jelaslah bahwa dengan tujuan mengungkap suatu tindak kejahatan, misalnya seperti mencegah penyebaran psikotropika dan tindakan terorisme, bagi instansi tertentu diberikan wewenang untuk melakukan penyadapan dengan menggunakan tatacara tertentu.

Meskipun demikian, demi *due process of law*, menyatakan antara lain bahwa kewenangan penyadapan seyogyanya memang harus diatur dengan jelas, termasuk di dalamnya mekanisme pengawasan yang ketat. Aturan jelas tidak semata-mata demi perlindungan privasi seseorang, lebih dari itu adalah untuk menegakkan*due process of law*. Marc Webber Tobias dan Roy Davis Petersen dalam "*Pre-Trial Criminal Procedure: A Survey of Constitutional Rights*" mendefinisikan *due process of law* sebagai jaminan

[21]"Penyadapan dalam Hukum Pidana", *Indonesia Corruption Watch*, dalam http://www.hukumonline.com/berita/baca/lt4b34d3deb69c6/penyadapan, diunduh pada 23 Januari 2014.
[22]*Ibid.*

konstitusi bahwa setiap warga negara berhak atas perlindungan terhadap tindakan pemerintah yang sewenang-wenang.[23]

Penyadapan yang Dilakukan Orang Asing

"Bagaimana sanksi jika negara lain menyadap komunikasi atau rahasia negara Indonesia tanpa sepengetahuan pemerintah Indonesia, lalu hukum negara manakah yang digunakan dalam kasus tersebut? " Ini adalah pertanyaan yang menggelitik yang diajukan oleh Fikri S pada situs (Hukum Online.com t.thn.).[24]Pertanyaan tersebut dijawab oleh Teguh Arifiadi, SH., M.H. yang secara umum menjelaskan tentang definisi penyadapan menurut UU Nomor 36 tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Kutipan jawabannya antara lain sebagai berikut : Kedua undang-undang tersebut tidak pernah mengatur bagaimana jika penyadapan dilakukan oleh seseorang atas dasar perintah negara tertentu. Bobot pembebanan pemidanaan hanya ditujukan kepada "orang" yang secara*de facto*melakukan penyadapan. Tidak ada ketentuan turunan lainnya, semisal jika "orang" tersebut melakukan penyadapan atas perintah negara lain atau perintah institusi.[25]

Dalam UU ITE, yang dimaksud "orang" adalah warga negara Indonesia, warga negara asing maupun badan hukum (Pasal 1 angka 21 UU ITE). Jadi, jika pelaku penyadapan ilegal adalah warga negara asing, UU ITE dapat diberlakukan. UU ITE dapat diberlakukan bagi setiap orang yang melakukan perbuatan hukum yang diatur dalam UU ITE (baik yang berada di wilayah hukum Indonesia maupuan di luar wilayah hukum Indonesia) selama perbuatan hukum tersebut memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia (Pasal 2 UU ITE).[26]

---

[23]Hukum Online,"Aturan Penyadapan, Perlindungan atau Ancaman Bagi Pengguna Telekomunikasi?", dalam http://www.hukumonline.com/berita/baca/lt4b34d3deb69c6/penyadapan, diunduh pada 23 Januari 2014.

[24] Hukum Online, "Langkah Hukum Jika Disadap Negara Tetangga", dalam http://www.hukumonline.com/klinik/detail/lt5276f8bec3f65/langkah-hukum-jika-disadap-negara-tetangga, diunduh pada 4 Februari 2014.

[25]*Ibid.*

[26]*Ibid.*

Sedangkan dalam UU Telekomunikasi, tidak dijelaskan siapa yang dimaksud "orang", namun dalam terminologi pidana pada umumnya, "orang" yang dimaksud adalah individu/pribadi yang melakukan perbuatan pidana. Dengan demikian, sanksi tentang penyadapan dalam ketentuan normatif kita hanya berlaku bagi orang perseorangan maupun badan hukum, dan tentu tidak berlaku bagi negara lain secara institusional.[27]

Terkait pertanyaan hukum negara manakah yang digunakan, tentunya harus dipastikan terlebih dahulu apakah penyadapan yang dilakukan tersebut melanggar ketentuan undang-undang negara atau tidak. Dalam kasus ini, belum dapat dipastikan apakah penyadapan tersebut melanggar undang-undang negara penyadap, ataukah melanggar undang-undang negara yang disadap, atau melanggar undang-undang kedua negara. Jika melanggar keduanya, hukum salah satu atau kedua negara dapat diberlakukan bagi pelaku penyadapan. Untuk menentukan hukum mana yang digunakan, bisa juga digunakan pendekatan berbagai teori *Locus Delicti* (tempat terjadinya perbuatan pidana). Untuk menetapkan *Locus Delicti* memang tidak diatur khusus dalam suatu undang-undang, melainkan diserahkan kepada ilmu dan praktik peradilan.

Dalam menetapkan *Locus Delicti* atau tempat terjadinya perbuatan pidana, juga dikenal 'teori alat', 'teori akibat', dan 'teori perbuatan materiil'. Secara ringkas, kami akan menjelaskan ketiga teori tersebut. 'Teori alat' menentukan bahwa tempat terjadinya pidana adalah tempat di mana alat bekerja atau tempat di mana alat yang dipergunakan untuk menyelesaikan suatu tindak pidana. Misalkan alat yang digunakan untuk menyadap berada di negara X, maka hukum yang berlaku adalah hukum negara X. 'Teori Akibat' menentukan bahwa tempat terjadinya pidana adalah tempat di mana perbuatan/kejadian tersebut menimbulkan akibat. Misalkan penyadapan yang dilakukan seseorang memberi akibat bagi orang lain yang tinggal di negara Y, maka hukum negara Y yang dapat digunakan untuk menjerat pelaku penyadapan. 'Teori Perbuatan Materiil' menentukan bahwa tempat terjadinya pidana adalah tempat di mana perbuatan dilakukan, misalnya jika penyadapan terjadi di wilayah hukum Indonesia, maka akan menggunakan hukum Indonesia, begitupun sebaliknya, jika penyadapan terjadi di wilayah hukum negara lain,

[27] *Ibid.*

dan dianggap sebagai perbuatan pidana di negara tersebut, maka hukum negara tersebutlah yang dapat digunakan.

Catatan penting dalam kasus penyadapan adalah sulitnya melakukan pembuktian. Penggunaan sarana teknologi dalam praktik penyadapan, akan menyulitkan penyidik untuk mendalami dan menguraikan bukti-bukti yang ada, bahkan jika penyidik menggunakan bantuan ahli *digital forensic* sekalipun.[28]

Cara Menyikapi Skandal Penyadapan Australia Secara Diplomatis

Sebagaimana diuraikan diatas bahwa kegiatan penyadapan ini sudah menjadi praktek yang 'biasa', namun sebagai suatu negara yang berdaulat, apabila mengetahui kantor pemerintahan atau pejabatnya disadap sudah barang tentu harus mengambil sikap yang tegas tetapi tepat dan terukur. Dari ketentuan perundangan yang ada, kita tidak memiliki ketentuan yang mengatur secara khusus kejahatan yang dilakukan terhadap negara seperti halnya penyadapan informasi tersebut. Undang-Undang Subversi telah dicabut untuk memberikan jaminan kehidupan rakyat yang bebas dari rasa takut terhadap ketidaksewenangan aparat.

Barangkali sudah saatnya kita memiliki Undang Undang Rahasia Negara yang mengatur secara khusus tentang tatacara melindungi rahasia negara dari perbuatan jahat berupa pencurian dokumen rahasia atau penyadapan informasi negara yang berklasifikasi rahasia. Pemerintah sudah pernah mengajukan draft RUU Rahasia Negara ini kepada DPR, namun hingga kini belum jelas kelanjutannya. Dengan adanya Undang Undang Rahasia Negara yang mengatur tentang cara menjaga rahasia negara diharapkan terdapat landasan hukum yang sesuai untuk penanganan kasus seperti penyadapan sehingga tindakan yang diambil akan lebih dapat dipertanggungjawabkan.

Pada saat ini, apabila ketahuan yang melakukan penyadapan adalah warga negara yang memiliki hubungan diplomatik, kita dapat minta penjelasan resmi dari wakil negara tersebut dan mengirimkan nota diplomatik. Tindakan mengadukan atau mengusulkan

[28]*Ibid.* Tindakan hukum tersebut masih terdapat pengecualian, yaitu apabila pelaku tindakan penyadapan memiliki kekebalan diplomatik, maka yang dapat dikenakan adalah memberlakukan status *persona non grata* dan memulangkan orang tersebut ke negara asalnya. Sedangkan yang tidak memiliki kekebalan hukum dapat dikenakan tuduhan sebagai mata-mata.

suatu resolusi ke Perserikatan Bangsa-Bangsa sebagaimana yang telah dilakukan oleh Indonesia bersama Brasil dan Jerman[29] juga merupakan langkah yang tegas tetapi bermartabat. Pemanggilan Duta Besar untuk 'melakukan konsultasi' biasanya juga sudah dianggap suatu 'hukuman' dalam tata cara dan etika diplomasi. Selain itu dapat dilakukan penetapan status *persona non grata* dan pengusiran bagi pejabat diplomat asing yang melakukan tindak penyadapan. Lebih jauh dapat pula diadakan peninjauan kembali atau bahkan penghentian sebagian atau keseluruhan kerja sama bilateral antara kedua negara sebagaimana dilakukan oleh Indonesia untuk menyikapi skandal penyadapan yang dilakukan oleh Australia tersebut.

Tindakan yang lebih serius dapat pula dilakukan hingga tataran pemutusan hubungan diplomatik dengan negara yang nyata-nyata tidak mau bersikap saling menghormati. Seringkali gerakan masyarakat berupa protes atau demonstrasi seperti yang terjadi di Ambon dan penyiaran berita secara luas di media massa juga dapat menambah tekanan terhadap pemimpin negara yang melakukan penyadapan[30]. Namun, itu semua tak lebih hanya untuk menjaga harga diri bangsa dan negara. Sedangkan esensi yang sebenarnya dalam menghadapi aksi penyadapan seperti itu adalah terletak pada bagaimana mengamankan informasi rahasia kita agar tidak dicuri oleh negara atau pihak lain.

Seperti diketahui bahwa Australia sudah sejak lama melakukan tindakan spionase dan penyadapan terhadap Indonesia seperti ditunjukkan melalui salah satu contoh berita yang diungkap oleh Merdeka.Com dengan judul artikel "Pengakuan Philip Dorling" bahwa Australia sudah lama mengintai tindak tanduk tetangganya Indonesia. Soal ini diungkap Dorling dalam kolomnya di Sydney Morning Herald yang selanjutnya menyatakan adanya sebuah catatan harian salah satu diplomat senior Australia yang tidak terpublikasikan

[29] Okezone, "Indonesia Ajukan Resolusi Penyadapan ke PBB" , dalam http://international.okezone.com/read/2013/11/19/411/899285/indonesia-ajukan-resolusi-penyadapan-ke-pbb, diunduh pada 23 Januari 2014.

[30] Metro TV News.com, "Bendera Australia dibakar di Ambon", http://www.metrotvnews.com/metronews/read/2013/11/27/6/197393/Bendera-Australia-Dibakar-di-Ambon, diunduh pada 23 Januari 2014.

yang menyebutkan bahwa badan intelijen Australia (DSD) rutin menyadap hubungan kawat diplomatik Indonesia sejak pertengahan 1950-an.[31]

Meskipun Indonesia sering menghadapi 'kenakalan' dalam praktek diplomasi Australia, namun dalam menyikapi kasus skandal penyadapan oleh Australia, Indonesia tetap mengambil langkah-langkah yang tepat dan terukur yaitu dengan meminta penjelasan resmi dari pemerintah Australia dan penghentian kerjasama beberapa program kerja sama di bidang pertahanan seperti program-program latihan militer bersama antara kedua negara hingga kasus itu mendapatkan penjelasan yang memuaskan dan permintaan maaf secara resmi dan terbuka.

Bagaimanapun esensi yang sebenarnya dalam menghadapi aksi penyadapan seperti itu adalah terletak pada bagaimana mengamankan informasi rahasia kita agar tidak dicuri oleh negara atau pihak lain. Adu keterampilan dan penguasaan teknologi informasi canggih memang tidak dapat dihindari oleh aparat intelijen untuk menggali informasi negara lain dengan tetap menjaga hubungan baik antar negara tanpa menimbulkan skandal diplomatik, sambil mengamankan kerahasiaan informasi negara kita sendiri yang memang perlu dirahasiakan.

Badan-badan seperti Lembaga Sandi Negara, Kementerian Komunikasi dan Informasi maupun seluruh pemangku kepentingan serta masyarakat teknologi informasi di Indonesia perlu memikirkan suatu sistem pengamanan informasi yang canggih dan handal agar jalur komunikasi dan informasi resmi antar instansi dan para pejabat negara dapat dilindungi dari tindakan penyadapan. Penggunaan teknologi informasi yang tepat dan canggih dapat membantu kegiatan mengamankan dan mencari informasi tersebut tanpa melanggar kebiasaan diplomatik dan ketentuan hukum internasional.

Kesimpulan

Setiap negara pasti ingin mengetahui niat negara lain terutama yag berkaitan langsung dengan kepentingan nasionalnya. Untuk itulah mereka mengirimkan misi diplomatik ke negara negara lain dengan maksud untuk menjalin hubungan kerja sama dan

[31] Merdeka.Com, "Pengakuan Philip Dorling", dalam http://www.merdeka.com/peristiwa/4-aksi-spionase-asing-di-indonesia-yang-menggemparkan/pengakuan-philip-dorling.html, diunduh pada 26 Juli 2014.

persahabatan namun sekaligus juga berusaha memahami sejarah, kondisi dan perkembangan sosial budaya, ekonomi, ilmu pengetahuan dan teknologi, politik dan militer. Disamping itu, data yang sering diminati adalah kondisi geografi, demografi dan biografi serta sikap para pemimpinnya.

Namun pengumpulan informasi secara terbuka tersebut seringkali dianggap tidak cukup sehingga dalam melakukan diplomasi antar negara tidak jarang terjadi skandal penyadapan yang dilakukan untuk menggali keterangan tersembunyi dalam rangka pengambilan kebijakan di bidang pertahanan dan bidang-bidang lainnya seperti ekonomi dan perdagangan.

Dalam kasus skandal penyadapan oleh Australia, Indonesia telah mengambil langkah-langkah yang tepat dan terukur yaitu dengan meminta penjelasan resmi dari pemerintah Australia dan penghentian kerja sama beberapa program kerja sama di bidang pertahanan hingga kasus itu mendapatkan penjelasan yang memuaskan dan permintaan maaf secara resmi dan terbuka. Sebagai hasil kunjungan Perdana Menteri Australia ke Indonesia, akhirnya Indonesia dan Australia sepakat akan menandatangani kode etik untuk menjamin tidak ada lagi penyadapan yang mengganggu hubungan diplomatik kedua negara. Dengan berlakunya kesepakatan tersebut hubungan diplomasi khususnya diplomasi pertahanan antara Indonesia dan Australia dapat dipulihkan. Namun merupakan pekerjaan rumah bagi Lembaga Sandi Negara, Kementerian Komunikasi dan Informasi dan seluruh pemangku kepentingan maupun masyarakat teknologi informasi di Indonesia bahwa kedepan harus dipikirkan dan disiapkan suatu sistem pengamanan informasi yang lebih handal agar jalur komunikasi dan informasi resmi antar instansi dan para pejabat negara dapat dilindungi dari tindakan penyadapan yang dapat merugikan kepentingan negara dan hubungan diplomatik khususnya dengan negara tetangga tersebut tetap dapat dipertahankan dengan baik.

Daftar Pustaka

Buku

Cahyono, Faried dan Fahmi Indrayadi. 2007. *Misteri Operasi Intelijen*. Jakarta: Indomedia Publishing.

Conboy, Ken. 2006. *The Second Front*. Jakarta, Singapore: Equinox Publishing.

Hatmojo, Jono. 2003. *Intelijen Sebagai Ilmu*. Jakarta: Balai Pustaka.

Hoy, Claire dan Victor Ostrovsky. 2007. *Mossad, Tipu Daya yang Dibeberkan oleh Mantan Agen Dinas Rahasia Israel* (Judul asli *By Way of Deception*). Ciputat Tangerang: Binarupa Aksara.

Shulsky, Abram N. dan Gary J. Scmith. 2002. *Silent Warfare: Understanding the World of Intelligence*. Dulles, Virginia: Brasseys's Inc.

Tzu, Sun. 2003. *The Art of War*. New York: Penguins Books.

Tzu, Sun. 2002.*The Art of War*. Boston: Sambhala Publications Inc.

Wijayanto, Andi et.al. 2006. *Intelijen: Velox et Exactus*. Jakarta: Pacivis dan Kemitraan.

Jurnal

"Etika dan Moral Intelijen". 2012. *Jurnal Intelijen dan Kontra Intelijen*. Volume VI. No. 36.

Majalah

"Dokumen Yang Memanaskan Jakarta". *Majalah Tempo*. 25 November – 1 Desember 2013.

Website

Hukum Online, "Aturan Penyadapan, Perlindungan atau Ancaman Bagi Pengguna Telekomunikasi?", dalam http://www.hukumonline.com/berita/baca/lt4b34d3deb69c6/penyadapan, diunduh pada 23 Januari 2014.

Hukum Online, "Langkah Hukum Jika Disadap Negara Tetangga", dalam http://www.hukumonline.com/klinik/detail/lt5276f8bec3f65/langkah-hukum-jika-disadap-negara-tetangga, diunduh pada 4 Februari 2014.

Indonesia Corruption Watch, dalam "Penyadapan dalam Hukum Pidana", dalam http://www.hukumonline.com/berita/baca/lt4b34d3deb69c6/penyadapan, diunduh pada 23 Januari 2014.

Kristanti, E. Y., "Snowden: Singapura Diduga Bantu AS-Australia Sadap Indonesia", dalam http://news.liputan6.com/read/755644/snowden-singapura-diduga-bantu-as-australia-sadap-indonesia, 25 November 2013, diunduh pada 23 Januari 2014.

Liputan6.com, "Ini Alasan Australia Sadap Ani Yudhoyono", http://news.liputan6.com/read/774976/ini-alasan-australia-sadap-ani-yudhoyono, diunduh pada 23 Januari 2014.

Metro TV News.com, "Bendera Australia dibakar di Ambon", dalam http://www.metrotvnews.com/metronews/read/2013/11/27/6/197393/Bendera-Australia-Dibakar-di-Ambon, diunduh pada 23 Januari 2014.

Merdeka.Com, "Pengakuan Philip Dorling", , http://www.merdeka.com/peristiwa/4-aksi-spionase-asing-di-indonesia-yang-menggemparkan/pengakuan-philip-dorling.html, diunduh pada 26 Juli 2014.

Okezone, "Indonesia Ajukan Resolusi Penyadapan ke PBB" , dalam http://international.okezone.com/read/2013/11/19/411/899285/indonesia-ajukan-resolusi-penyadapan-ke-pbb, diunduh pada 23 Januari 2014.

"Penyadapan", Hukum Acara Pidana dan Peraturan Terkait", dalam http://acarapidana.bphn.go.id/proses/penyadapan/?s=penyadapan&type=all, diunduh pada 4 Februari 2014.

The Age, "Singapore, South Korea revealed as Five Eyes spying partners", 25 November 2013, dalam http://www.theage.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html, diunduh pada 22 Juli 2014.