Memastikan perlindungan hak atas privasi dalam pertahanan siber[1]

Oleh: Wahyudi Djafar[2]

. . . intelligence is not an isolated activity. It is an integral part of government. It reflects the character of national constitutions and the societies in which it is set.[3]

A. Jaminan perlindungan hak atas privasi

Akhir-akhir ini pemberitaan media ramai dengan terkuaknya praktik intersepsi komunikasi yang dilakukan oleh intelijen Australia terhadap sejumlah pejabat Indonesia, termasuk Presiden Susilo Bambang Yudhoyono. Awal mula informasi ini berasal dari publikasi majalah Der Spiegel di Jerman, yang menerbitkan dokumen-dokumen dari Edward J. Snowden, mantan kontraktor *National Security Agency* (NSA) Amerika Serikat. Tidak hanya tindakan penyadapan telepon terhadap Presiden Yuhoyono dan orang-orang di lingkarannya, berdasarkan dokumen Snowden, Der Spiegel mempublikasikan pula dokumen rahasia NSA lainnya yang menguraikan kemampuan unit *Special Collection Service* (SCS).[4] Dalam pemberitaannya diungkap kerja-kerja aktif dari agen-agen NSA di seluruh dunia, setidaknya di 80 lokasi, 19 diantaranya di kota-kota besar Eropa, seperti Paris, Madrid, Roma, Praha dan Jenewa. Mereka juga memiliki dua pangkalan utama di Jerman, yang terletak di Berlin dan Frankfurt. Sementara di kawasan Asia Pasifik, Korea Selatan, Singapura, dan Australia ditengarai menjadi tempat bekerja dari unit SCS, termasuk mengumpulkan pembicaraan dengan melakukan intersepsi terhadap kabel optik bawah laut.[5]

Praktik intervensi terhadap privasi, dalam bentuk *surveillance*, intersepsi komunikasi dan gangguan terhadap data pribadi memang salah satu persoalan besar yang mengemuka dalam pemanfaatan tekonologi informasi dan komunikasi khususnya internet. Pelapor khusus PBB untuk kebebasan berpendapat dan berekspresi Frank La Rue, telah memberikan perhatian khusus terhadap soal ini, mengingat tingginya praktik pengamatan (*surveillance*), intersepsi komunikasi pribadi warga negara, serta pemindahtangan data pribadi secara sewenang-wenang. Dalam laporannya, La Rue menegaskan perlunya setiap negara memiliki undang-undang yang secara jelas menggambarkan kondisi-kondisi bahwa hak atas privasi dari individu bisa dibatasi di bawah kondisi-kondisi tertentu, dan tindakan-tindakan menyentuh hak ini harus diambil dengan dasar sebuah keputusan khusus. Keputusan ini diambil oleh otoritas negara yang dijamin secara jelas oleh hukum untuk melakukan tindakan tersebut.[6]

---

[1] Disampaikan dalam Seminar Nasional " Cyber Defence: Kepentingan Pertahanan Nasional dan Perlindungan Hak Privasi", diselenggarakan oleh Fakultas Hukum Universitas Airlangga Surabaya, 26 November 2013.

[2] Peneliti pada Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jakarta (http://elsam.or.id/). Komunikasi lebih lanjut dapat melalui @wahyudidjafar atau wahyudi@elsam.or.id.

[3] M. Herman, *Intelligence Services in the Information Age*, (London: Frank Cass, 2001), hal. 138.

[4] Lihat "N.S.A. Spying Scandal Hurts Close Ties Between Australia and Indonesia", dalam http://www.nytimes.com/2013/11/20/world/asia/nsa-spying-scandal-tarnishes-relations-between-indonesia-and-australia.html?ref=surveillanceofcitizensbygovernment.

[5] Lihat "Singapore, S Korea help NSA to collect data in Asia via undersea high speed optic cables – Snowden's leaks", dalam http://voiceofrussia.com/news/2013_11_25/Singapore-S-Korea-help-NSA-to-collect-data-in-Asia-via-undersea-high-speed-optic-cables-Snowden-s-leaks-5925/.

[6] Lihat Laporan Frank La Rue Paragraf 59, A/HRC/14/23, dapat diakses di http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf.

Di berbagai negara, isu yang terkait dengan privasi serta pengaturan mengenai privasi telah mulai berkembang sebagai bagian yang utuh dari perkembangan sosial masyarakat. Oleh karena itu, dapat dipahami di sejumlah negara demokratis, hukum positif dan yurisprudensi mengenai privasi telah muncul jauh sebelum privasi menjadi bagian yang utuh dari rejim hukum hak asasi manusia internasional.[7] Hal ini mungkin menjelaskan mengapa hampir tidak terdapat rujukan khusus dalam berbagai dokumen PBB mengenai cakupan pengertian dari konsep privasi.

Westin (1967) secara sederhana mendefinisikan hak atas privasi sebagai klaim dari individu, kelompok, atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sampai sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain. Keluasan cakupan privasi bisanya menjadikan banyaknya pengaturan mengenai privasi di suatu negara, baik dalam jenis maupun tingkatnya.[8] Pengertian dan cakupan konsep privasi lainnya yang sering menjadi rujukan adalah rumusan yang dikembangkan oleh William Posser, dengan merujuk setidaknya pada empat hal:[9]

(a) Gangguan terhadap tindakan seseorang mengasingkan diri atau menyendiri, atau gangguan terhadap relasi pribadinya
(b) Pengungkapan fakta-fakta pribadi yang memalukan secara publik
(c) Publisitas yang menempatkan seseorang secara keliru dihadapan publik
(d) Penguasaan tanpa ijin atas kemiripan seseorang untuk keuntungan orang lain.

Dalam perkembangan hukum HAM internasional, perlindungan hak atas privasi diatur dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia, yang menegaskan:

> Tidak seorangpun boleh diganggu secara sewenang-wenang dalam urusan pribadi, keluarga, rumah tangga atau hubungan surat-menyuratnya, juga tidak boleh dilakukan serangan terhadap kehormatan dan reputasinya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau penyerangan seperti itu.

Dalam perumusan yang lebih singkat dan lugas, perlindungan hak atas privasi ditegaskan melalui pengaturan dalam Kovenan Internasional Hak-hak Sipil dan Politik, khususnya dalam Pasal 17, yang menyebutkan:

> (1) Tidak boleh seorang pun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah atau hubungan surat-menyuratnya, atau secara tidak sah diserang kehormatan dan nama baiknya.
> (2) Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan seperti tersebut di atas.

Dalam konteks hukum Indonesia, perlindungan terhadap hak atas privasi telah diakui sebagai salah satu hak konstitusional warga negara, sebagaimana ditegaskan UUD 1945, setelah dilakukannya amandemen. Ketentuan Pasal 28G ayat (1) UUD 1945 menyatakan:

[7] Mengenai perkembangan gagasan privasi, lihat Harry Henderson, *Privacy in the information Age, Revised Edition*, (New York: Facts On File, Inc, 2006), hal 6-16.
[8] Lihat A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), hal. 7-8.
[9] William Prosser, sebagaimana dikutip dalam DeCew, Judith, "Privacy", The Stanford Encyclopedia of Philosophy (Fall 2012 Eds), Edward N Zalta (ed). Dapat diunduh pada http://plato.stanford.edu/archives/ fall2012/entries/privacy/.

> "Setiap orang berhak atas perlindungan diri pribadi,[10] keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi manusia".

Selain itu, jaminan yang sama juga dirumuskan dengan sedikit berbeda dalam UU No. 39 Tahun 1999 tentang HAM, khususnya melalui pasal-pasal berikut:

Pasal 29 ayat (1)	setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya
Pasal 30	Setiap orang berhak atas rasa aman dan tenteram serta perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu
Pasal 31 ayat (1) Pasal 31 ayat (2)	Tempat kediaman siapapun tidak boleh diganggu Menginjak atau memasuki suatu pekarangan tempat kediaman atau memasuki suatu rumah bertentangan dengan kehendak orang yang mendiaminya, hanya diperbolehkan dalam hal-hal yang telah ditetapkan dengan undang-undang
Pasal 32	Kemerdekaan dan rahasia dalam hubungan surat menyurat termasuk hubungan komunikasi sarana elektronika tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan perundang-undangan

Lebih lanjut dalam bagian penjelasan Pasal 31 secara jelas diuraikan mengenai pengertian 'tidak boleh diganggu' merujuk pada kehidupan pribadi (privasi) di dalam tempat kediamannya. Penjelasan ini menegaskan tempat kediaman individu sebagai wilayah yang dijamin perlindungannya sebagai bagian dari kehidupan pribadi. Namun tidak terdapat rujukan lebih jauh apakah pengertian tempat kediaman merujuk pada domisili atau juga termasuk dalam pengertian yang lebih faktual merujuk pada tempat dimana individu tersebut sedang berada.

Berikutnya dalam Komentar Umum atas Pasal 17, Komite Hak Sipil dan Politik PBB sebagaimana dirumuskan dalam Komentar Umum No. 16, menegaskan mengenai sifat relatif dari perlindungan hak atas privasi, yang sangat tergantung pada konteks sosial masyarakatnya. Dokumen ini memberikan batasan-batasan yang lebih mendetail mengenai pengertian 'gangguan yang sewenang-wenang' atau 'melawan hukum' (*unlawfull interference*) terhadap privasi. Dalam pengertian tersebut terkandung unsur-unsur: gangguan atas privasi hanya dapat dilakukan dalam kasus-kasus yang ditetapkan oleh undang-undang; gangguan yang diterapkan atas dasar undang-undang harus memenuhi beberapa prasyarat berikut: (a) sesuai/tidak bertentangan dengan ketentuan dan tujuan dari Konvenan, (b) logis dalam konteks tertentu, (c) menguraikan secara detail kondisi-kondisi khusus yang membenarkan adanya gangguan atas privasi, (d) hanya dapat dilakukan oleh otoritas yang ditunjuk dalam undang-undang tersebut, (e) hanya dilakukan atas dasar kasus per kasus.[11]

Panduan tersebut juga menegaskan adanya larangan praktik pengambilan dan penguasaan data pribadi tanpa didasarkan pada undang-undang oleh pihak lain, baik otoritas publik, maupun

[10] Pasal yang dirujuk adalah pasal yang sama dalam dokumen UDHR, dalam hal ini term 'privacy' diterjemahkan sebagai 'diri pribadi'.
[11] Lihat CCPR/C/GC/16, General comment No. 16, Article 17: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation, selengkapnya dapat diakses di http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument.

badan-badan privat. Data pribadi ini mencakup data yang terdapat dalam komputer, data bank maupun data-data yang terdapat dalam perangkat lain. Dalam konteks ini, setiap individu memiliki hak untuk mengetahui dan memperoleh kepastian mengenai data pribadi yang tersimpan secara otomatis dalam file data, untuk kepentingan apa data tersebut dikumpulkan dan badan/institusi yang memegang kendali atas data-data pribadi mereka. Dengan demikian setiap individu memiliki hak untuk meminta perbaikan atau penghapusan data pribadi apabila data yang dikumpulkan keliru atau proses pengumpulannya bertentangan dengan undang-undang.

Standar perlindungan mengenai data pribadi ini telah pula berkembang pada level mekanisme HAM di tingkat regional. Mekanisme HAM Eropa misalnya mulai mengembangkan perangkat perlindungan melalui pengadopsian Konvensi Dewan Eropa tahun 1981.[12] Pengadopsian ini diperkuat dengan lahirnya berbagai yurisprudensi yang dilahirkan oleh pengadilan HAM Eropa.[13] Perkembangan serupa juga terjadi pada mekanisme HAM regional kawasan Amerika.

B. Problem hukum yang bersinggungan dengan hak atas privasi di Indonesia

Sebelum amandemen UUD 1945, perlindungan terhadap hak atas privasi, khususnya yang berupa komunikasi pribadi seseorang diatur di dalam Bab XXVIII KUHP tentang Kejahatan Jabatan terutama di dalam Pasal 430 sampai dengan 434. Khusus mengenai larangan penyadapan terhadap komunikasi jarak jauh melalui alat, diatur di dalam Pasal 433, yang melarang penyadapan telepon dan telegraf secara ilegal. Ketentuan ini kemudian dipertegas dengan lahirnya UU No. 36 Tahun 1999 tentang Telekomunikasi. Salah satu hal baru yang muncul dalam undang-undang ini adalah terkait dengan adanya larangan melakukan penyadapan informasi. Dalam ketentuan Pasal 40 UU No. 36 Tahun 1999 disebutkan, "*Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun*". Pada penjelasannya ditegaskan bahwa informasi merupakan bagian dari hak pribadi yang harus dilindungi, oleh karena itu penyadapan harus dilarang.[14] Namun dalam kerangka penegakan hukum, khusus untuk tindak pidana tertentu, yang diancam dengan hukuman di atas lima tahun, penyadapan informasi sebagai upaya pengungkapan kejahatan dan pengumpulan alat bukti dapat dilakukan. Operator telekomunikasi dalam melakukan penyadapan bersandar pada permintaan tertulis dari Jaksa Agung, Kepala Kepolisian RI, atau penyidik untuk tindak pidana tertentu sebagaimana diatur undang-undang.[15]

Pasca-amandemen konstitusi, hak atas privasi diakui Indonesia sebagai salah satu hak konstitusional warga negara yang harus dilindungi. Perlindungan ini ditegaskan di dalam Pasal 28 G ayat (1) UUD 1945, yang diantaranya menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi (privasi), keluarga, kehormatan, martabat, dan harta bendanya (termasuk data-data pribadi). Pernyataan tersebut juga ditegaskan di dalam Pasal 32 UU No. 39 Tahun 1999 tentang HAM, yang antara lain menyatakan bahwa kemerdekaan dan rahasia komunikasi melalui sarana elektronik tidak boleh diganggu kecuali atas perintah hakim atau kekuasaan lain yang sah menurut undang-undang.

[12] Lihat Pasal 8 Council of Europe Convention 1981.
[13] Lebih jauh lihat, European Court of Human Rights, 2011, Internet: case law of the European Court of Human Rights, mengcover analisis atas semua kasus terkait internet dan kebebasan berekspresi serta perlindungan privacy sampai pertengahan tahun 2011.
[14] Penyadapan menurut undang-undang ini adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah.
[15] Lihat Pasal 42 UU No. 36 Tahun 1999 tentang Telekomunikasi.

Intersepsi komunikasi secara melawan hukum yang dilakukan di internet juga dilarang menurut hukum Indonesia. Larangan ini ditegaskan di dalam Pasal 31 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam ketentuan tersebut dinyatakan bahwa setiap orang dilarang untuk melalukan intersepsi atau penyadapan atas informasi atau dokumen elektronik dalam suatu komputer atau sistem elektronik milik orang lain. Intersepsi komunikasi hanya dibolehkan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan atau institusi penegak hukum lainnya. Pelanggaran terhadap ketentuan tersebut diancam pidana penjara selama-lamanya 10 tahun dan/atau denda sebanyak-banyaknya 800 juta rupiah.[16]

Namun demikian ketiadaan aturan tunggal tentang tata cara penyadapan di Indonesia telah menciptakan kerentanan terhadap tindakan intersepsi komunikasi pribadi warga negara, termasuk komunikasi menggunakan internet, seperti surat elektronik serta bermacam perangkat media sosial. Sampai hari ini, Indonesia sedikitnya memiliki dua belas peraturan perundang-undangan yang di dalamnya mengatur tentang penyadapan/intersepsi komunikasi dengan tata cara yang berbeda-beda. Perbedaan pengaturan mengenai penyadapan ini misalnya nampak sangat nyata antara UU Pemberantasan Tindak Pidana Terorisme, UU Narkotika, UU Komisi Pemberantaras Tindak Pidana Korupsi, dan UU Intelijen Negara. Centang-perenangnya hukum penyadapan di Indonesia ini telah membuka celah yang lebar bagi praktik campur tangan terhadap komunikasi pribadi warga negara, termasuk yang menggunakan internet.[17]

Selain masalah centang-perenang hukum penyadapan, problem lain yang mengemuka dalam perlindungan privasi di Indonesia adalah tidak memadainya perlindungan terhadap data pribadi warga negara. Bahkan sampai saat ini, Indonesia belum memiliki peraturan perundang-undangan yang secara khusus menjamin perlindungan data pribadi seseorang. Ketentuan mengenai perlindungan data pribadi seseorang, khususnya yang dalam bentuk elektronik diatur secara terbatas di dalam Pasal 26 UU Informasi dan Transaksi Elektronik. Dalam ketentuan tersebut ditegaskan bahwa pemindahtanganan data pribadi seseorang harus dilakukan berdasarkan persetujuan dari orang yang bersangkutan, kecuali ditentukan lain oleh peraturan perundang-undangan. Namun pelanggaran terhadap ketentuan ini tidak diancam dengan pidana, hanya diberikan ruang untuk melakukan ganti kerugian.[18] Lemahnya pengaturan mengenai perlindungan data pribadi berakibat pada maraknya praktik pembocoran dan pemindatangan data pribadi seseorang di Indonesia, khususnya untuk kepentingan komersial.[19]

C. Meningkatnya penggunaan metode surveillance dan intersepsi komunikasi dalam pengumpulan informasi keamanan

Kaitannya dengan praktik surveillance dengan alasan keamanan nasional, Militer Indonesia sendiri, melalui Badan Intelijen Strategis (BAIS) baru-baru ini telah menjalin kontrak kerjasama dengan Gamma TSE, sebuah perusahaan keamanan yang berpusat di Inggris, yang menyediakan banyak perangkat pengamatan—surveillance. Kementerian Pertahanan menyebutkan, kerjasama sebesar 5,6 juta dollar AS dengan Gamma TSE ini mencakup pembelian peralatan komunikasi data yang dilengkapi dengan encryptor dan decryptor, peralatan surveillance yang dilengkapi dengan source code serta peralatan pengamanan komunikasi. Kerjasama ini juga mencakup paket pelatihan bagi personel yang

[16] Lihat Pasal 31 ayat (2) jo. Pasal 47 UU ITE.
[17] Lihat Wahyudi Djafar, Protecting privacy rights from wiretapping, The Jakarta Post, 21 Februari 2013, dapat diakses di http://www.thejakartapost.com/news/2013/02/21/protecting-privacy-rights-wiretapping.html. Lihat Laporan Pelapor Khusus PBB untuk kebebasan berekspresi dan berpendapat, Frank La Rue, A/HRC/23/40, dapat diakses di http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.
[18] Lihat Pasal 26 ayat (2) UU ITE.
[19] Lihat Wahyudi Djafar, Kita Perlu UU Perlindungan Data Pribadi, dalam http://www.hukumpedia.com/ham/kita-perlu-uu-perlindungan-data-pribadi-hk51da54d24bb82.html.

mengoperasikannya, baik yang bertugas di dalam negeri maupun kantor-kantor Atase Pertahanan Indonesia di luar negeri.[20]

Gamma TSE yang merupakan bagian dari Gamma International menjual peralatan intersepsi kepada pemerintah dan lembaga penegak hukum secara eksklusif. Teknologi mereka dikenal dengan FinFisher Suite (termasuk Trojan untuk menginfeksi PC, ponsel, konsumen elektronik lainnya, termasuk server, serta menyediakan pula konsultasi teknis).[21] Teknologi ini dianggap sebagai salah satu yang paling canggih di pasar saat ini. Dalam promosinya Gamma Group menawarkan tekonlogi intrusi internet (teknologi informasi) dan solusi pemantauan jarak jauh, mereka juga mengatakan hanya menjual secara eksklusif untuk penegakan hukum dan badan-badan intelijen. Berdasarkan data dari Citizen Lab, saat ini setidaknya terdapat 25 negara yang telah menggunakan teknologi ini, termasuk Indonesia.[22]

Berbasis teknologi FinFisher, sebuah komputer atau smartphone dari jarak yang jauh dapat terinfeksi Trojan, yang kemudian dikuasai oleh instansi pemerintah melalui komando dan kontrol server. Sebuah komputer dapat terinfeksi melalui pemberitahuan palsu untuk update software, email berbahaya atau melalui akses fisik ke mesin. Finfisher juga menawarkan teknologi untuk menginfeksi seluruh warung internet untuk mengamati semua pengguna. Ketika diinstal, hampir tidak mungkin untuk menghapus Trojan, juga tidak ada cara yang aman untuk menghindari Finfisher pada mesin yang telah terinfeksi. Perangkat lunak ini dikatakan mampu melewati metode umum dan deteksi anti-virus. FinFisher juga dapat mendengarkan pembicaraan melalui Skype sekaligus mentranskipnya, chatting dan email terenkripsi dan bahkan mampu menghidupkan mikrofon komputer atau webcam dari jarak jauh. Dengan teknologi FinFisher, bahkan dimungkinkan untuk mendapatkan akses ke file terenkripsi pada hard drive.[23]

Tidak hanya kerjasama dengan Gamma TSE, militer Indonesia juga terus berusaha untuk meningkatkan kemampuan pengamatan mereka melalui sejumlah program kemitraan. Kemitraan ini antara lain dilakukan dengan pemerintah Amerika Serikat, yang telah mengeluarkan dana sedikitnya 57 juta dollar AS, dari tahun 2006 hingga tahun 2008, guna pembentukan *Integrated Maritime Surveillance System* (IMSS). Sistem ini dirancang untuk memerangi terorisme, penyelundupan, dan pembajakan di perairan Indonesia. IMSS dilengkapi dengan kamera pengintai, radar permukaan, GPS, dan kombinasi lainnya dari berbagai sensor, perangkat, dan platform teknis lainnya untuk memonitor lalu lintas maritim.[24]

Dalam praktinya, rupa-rupanya yang memanfaatkan teknologi FinSpy tidak hanya institusi intelijen dan penegak hukum, tetapi juga sejumlah perusahaan penyedia layanan internet (ISP). Menurut penulusuran yang dilakukan oleh Citizen Lab terbukti sejumlah ISP di Indonesia telah memanfaatkan teknologi ini untuk mengamati konsumennya. Perusahaan-perusahaan ISP

[20] Lihat "Kemhan:Pengadaan Alat ANTI SADAP Untuk Amankan Informasi Strategis TNI", dalam http://www.kemhan.go.id/kemhan/?pg=31&id=1203.
[21] Lihat https://www.gammagroup.com/ dan http://www.finfisher.com/FinFisher/index.html.
[22] Negara-negara tersebut meliputi Australia, Bahrain, Bangladesh, Britain, Brunei, Canada, the Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, the United Arab Emirates, the United States and Vietnam. Selengkapnya lihat "Researchers Find 25 Countries Using Surveillance Software", dalam http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/?_r=0.
[23] Lihat Finfisher promo videos, dalam https://www.youtube.com/watch?v=gc8i7C659FU.
[24] Lihat "Exploring Communications Surveillance in Indonesia", dalam https://citizenlab.org/2013/10/igf-2013-exploring-communications-surveillance-indonesia/.

tersebut meliputi: PT Telkom untuk IP 118.97.xxx.xxx, PT Matrixnet Global untuk IP 103.28.xxx.xxx, Biznet untuk IP 112.78.143.34 dan 112.78.143.26.[25]

Selain menggunakan tekonlogi FinFisher, penelitian Citizen Lab juga menemukan instalasi PacketShaper di Indonesia pada jaringan Indosat (http://202.155.63.62/) dan PT Telkom (http://203.130.193.156/login.htm), serta instalasi CacheFlow pada PT Telkom (http://180.252.181.1). Paket instalasi tersebut merupakan teknologi dari Blue Coat Systems, sebuah perusahaan berbasis di California yang menyediakan keamanan jaringan dan optimasi peralatan dengan fungsionalitas jaringan dengan kemungkinan penyaringan dan pengamatan. Layanan ini memiliki kemampuan untuk memantau dan mengendalikan lalu lintas jaringan, menyaring lalu lintas aplikasi berdasarkan kategori konten, memblokir konten, dan memonitor serta merekam komunikasi pribadi.[26]

Dalam konteks keamanan nasional, secara prinsipil institusi keamanan, khususnya intelijen memang sudah sepatutnya memiliki kewenangan dan kemampuan untuk melakukan pengamatan—*surveillance* dan intersepsi komunikasi, sebagai bagian dari kerja pengumpulan informasi. Namun demikian, undang-undang nasional harus secara tegas mengatur mengenai hal-hal berikut ini:[27] (1) tindakan intersepsi yang dapat dilakukan, (2) tujuan melakukan intersepsi, (3) kategorisasi objek—individu yang dapat dilakukan intersepsi,[28] (4) ambang kecurigaan—bukti permulaan, yang diperlukan untuk membenarkan penggunaan tindakan intersepsi, (5) pengaturan mengenai pembatasan durasi dalam melakukan tindakan intersepsi, (6) prosedur otorisasi—perijinan, dan (7) pengawasan serta peninjauan atas tindakan intersepsi yang dilakukan.

Perlindungan hak atas privasi warga negara tetap harus menjadi perhatian utama di dalam setiap pembentukan kebijakan dan aktivitas pertahanan yang memanfaatkan teknologi informasi dan komunikasi. Hal ini sejalan dengan perkembangan teori keamanan itu sendiri, yang mengarah pada konsepsi keamanan yang ditekankan kepada kepentingan keamanan pelaku-pelaku bukan negara (*non-state actors*).[29] Konsepsi ini berkembang setelah menurunnya ancaman militer terhadap kedaulatan negara, dan sebaliknya ada peningkatan ancaman terhadap keamanan manusia pada aspek lain, seperti kemiskinan, penyakit menular, bencana alam, kerusakan lingkungan hidup dan lainnya.[30] Wacana ini memperluas *refferent object* dari keamanan yang tidak lagi terfokus pada negara, melainkan termasuk pentingnya keamanan manusia (*human security*).[31] Konsep ini berkait erat dengan kewajiban negara untuk menjamin perlindungan dan pemenuhan hak asasi manusia setiap warganya. [ ]

---

[25] Lihat "You Only Click Twice: FinFisher's Global Proliferation", dalam https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

[26] Teknologi ini telah digunakan di 83 negara (20 negara dengan baik ProxySG dan PacketShaper, 56 negara dengan PacketShaper, dan 7 negara dengan ProxySG).

[27] Martin Scheinin, Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, including on their Oversight, (UN Human Rights Council, 2010), hal. 19.

[28] Sejumlah negara memberikan jaminan khusus terhadap individu-individu pertentu, khususnya mereka para jurnalis dan advokat, dari tindakan pengumpulan informasi intelijen—khususnya terkait dengan kerja-kerja intersepsi komunikasi. Lihat Germany Criminal Code, G10 Act, sect. 3b; sects. 53 and 53a.

[29] Lihat Edy Prasetyono, Konsep-Konsep Keamanan", dalam Indra J Piliang, Edy Prasetyono, Hadi Soesastro (eds), *Merumuskan Kembali Kebangsaan Indonesia*, (Jakarta: CSIS, 2006), hal. 267-269.

[30] Lihat Bob Sugeng Hadiwinata, Transformasi Isu dan Aktor di dalam Studi Hubungan Internasional: Dari Realisme hingga Konstruktivisme, dalam Yulius P Hermawan (ed), *Transformasi dalam Studi Hubungan Internasional: Aktor, Isu dan Metodologi*, (Yogyakarta: Graha Ilmu, 2007), hal. 13.

[31] Lihat Barry Buzan, Ole Waever dan Jaap Wilde, *Security: a New Framework for Analysis*, (Boulder Colorado: Lynne Rienner, 1998).