

Memerhatikan perlindungan hak atas privasi dalam pengaturan dan praktik penyadapan di Indonesia¹

Oleh: Wahyudi Djafar²

A. Pengantar

Isu mengenai penyadapan kembali menghangat dalam beberapa waktu terakhir, bersamaan dengan proses pembahasan Rancangan KUHAP di DPR. Salah satu poin penting dalam materi rancangan KUHAP adalah rumusan mengenai pengaturan tata cara atau prosedur penyadapan yang dilakukan oleh aparat penegak hukum, terutama kepolisian, kejaksaan dan KPK. Terhadap rencana pengaturan ini, ada kekhawatiran yang muncul, khususnya dari KPK, bahwa rumusan aturan yang terlalu ketat mengenai prosedur penyadapan, akan dapat mengganggu pelaksanaan tugas KPK dalam penindakan kasus tindak pidana korupsi. Memang, harus pula diakui, selama ini praktik-praktik penyadapan sangat membantu bagi KPK, dalam pengungkapan kasus-kasus korupsi. Begitu pula dalam pemberantasan tindak pidana terorisme dan narkoba, baik Detasemen Khusus 88 Anti Teror atau pun Badan Narkotika Nasional, juga sangat mengandalkan penggunaan metode penyadapan dalam menelusuri kasus-kasus terorisme dan narkoba. Namun demikian, meski praktik penyadapan menjadi salah satu kebutuhan penting dalam penegakan hukum, perlindungan hak atas privasi warga negara juga musti diperhatikan.

Selain isu penyadapan yang berkaitan dengan penegakan hukum di tanah air, pemberitaan media juga diramaikan dengan terkuaknya praktik penyadapan yang dilakukan oleh intelijen Australia terhadap sejumlah pejabat Indonesia, termasuk Presiden Yudhoyono dan beberapa orang di lingkaran dekatnya. 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. Berdasarkan dokumen Snowden, *Der Spiegel* mempublikasikan pula dokumen rahasia NSA lainnya yang menguraikan kemampuan unit *Special Collection Service* (SCS).³ Dalam pemberitaannya diungkap kerja-kerja aktif dari agen-agen NSA di seluruh dunia, setidaknya di 80 lokasi. Di kawasan Asia Pasifik, setidaknya tiga negara diduga menjadi tempat bekerja dari unit SCS, termasuk negara tetangga kita, Singapura, Australia dan Korea Selatan. Tugas unit ini salah satunya adalah mengumpulkan pembicaraan dengan melakukan intersepsi terhadap kabel optik bawah laut.⁴

Praktik intervensi terhadap privasi, dalam bentuk *surveillance*, penyadapan/intersepsi komunikasi dan gangguan terhadap data pribadi telah menjadi salah satu persoalan besar yang mengemuka dalam beberapa tahun terakhir, terutama dengan semakin meningkatnya pemanfaatan teknologi informasi dan komunikasi khususnya internet. Pelapor khusus PBB

¹ Makalah disampaikan dalam Seminar “Kewenangan Badan Pemerintah dalam Melakukan Penyadapan serta Korelasinya dengan Pelanggaran HAM”, yang diselenggarakan oleh Komunitas peradilan semu *Atma Jaya Moot Court Guild* (AMG) Fakultas Hukum Universitas Katolik Indonesia Atma Jaya-Jakarta, pada Jumat, 21 Maret 2014.

² Peneliti dan Pengacara Publik pada Lembaga Studi dan Advokasi Masyarakat (ELSAM)— <http://elsam.or.id/>. Komunikasi lebih lanjut dapat melalui surel: wahyudi@elsam.or.id, twitter: @wahyudidjafar, atau laman: <http://wahyudidjafar.web.id/>.

³ 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>.

⁴ 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/.

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 pemindahtanganan 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.⁵

Dalam laporan tersebut, La Rue juga menyinggung soal kompleksitas hukum yang memberikan kewenangan pengamatan/pengawasan komunikasi, yang tersebar di dalam sejumlah peraturan perundang-undangan.⁶ Situasi ini telah berakibat pada rentannya perlindungan hak atas privasi tiap-tiap warga negara. Di berbagai negara, isu yang terkait dengan privasi serta pengaturan mengenai privasi telah mulai berkembang sebagai bagian yang utuh dari perkembangan sosial masyarakat. Bahkan, pengalaman di sejumlah negara demokratis menunjukkan, hukum positif dan jurisprudensi mengenai privasi telah muncul jauh sebelum privasi menjadi bagian yang utuh dari rejim hukum hak asasi manusia internasional.⁷

B. Pengertian atas konsep privasi

Sebelum privasi diperdebatkan sebagai sebuah konsep hukum, konsep ini telah memiliki akar historis yang luas dalam diskusi antropologis dan sosiologis, yang sekaligus menunjukkan luasnya penghargaan dan pelestarian konsep tersebut dalam berbagai budaya dan masyarakat. Dalam studi-studi awal mengenai konsep privasi, dengan sudut pandang antropologi dan sosiologi, Indonesia, khususnya Jawa dan Bali, juga menjadi satu rujukan menarik, perihal betapa unik dan ragamnya karakteristik atas konsep privasi dalam masyarakat. Hal ini sebagaimana dikemukakan Alan Westin dengan merujuk studinya Clifford Gertz, yang menelaah dan mendalami konsep-konsep privasi dalam kehidupan masyarakat Jawa dan Bali.⁸ Secara umum, para ahli telah bersepakat, bahwa hampir semua budaya pada dasarnya menghargai privasi, meski bentuk dan cara penghargaan tersebut bervariasi antara satu tempat dengan tempat lainnya.

Secara konseptual, mengutip Jeffrey Reiman, nilai privasi didefinisikan sebagai perlindungan kebebasan, kepribadian moral, dan kehidupan batin yang beragam dan kritis. Dalam konteks pemikiran politik, merujuk pada gagasan Aristoteles, konsep privasi berangkat dari perbedaan antara konsep 'publik' dan 'privat'. Dikotomi antara publik dan privat ini ditempuh sebagai upaya untuk membedakan antara wilayah politik dan dengan kehidupan domestik. Lebih jauh, gagasan aristoteles ini terimplementasi dengan adanya 'polis' dan 'provinsi' sebagai kursi pemerintah dan kegiatan politik, yang merupakan manifestasi dari ruang publik. Sedangkan kebalikannya dikenalkanlah 'oikos' sebagai manifestasi dari ruang privat, pribadi atau rumah tangga.

Berangkat dari beragam konsepsi antropologis, sosiologis, dan filosofis tersebut, Alan Westin (1967) secara sederhana mendefinisikan hak atas privasi sebagai klaim dari individu, kelompok, atau lembaga untuk menentukan sendiri mengenai kapan, bagaimana, dan sampai sejauhmana informasi tentang mereka dikomunikasikan kepada orang lain.

⁵ Lihat Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/14/23), paragraf 59, dapat diakses di <http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf>.

⁶ Ibid, paragraf 56.

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 Alan Westin, "The origins of modern claims to privacy", dalam Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, (Cambridge: Cambridge University Press, 1984), hal. 64-65.

Keluasan cakupan privasi bisanya menjadikan banyaknya pengaturan mengenai privasi di suatu negara, baik dalam jenis maupun tingkatnya.⁹ Pengertian dan cakupan konsep privasi lainnya yang sering menjadi rujukan adalah rumusan yang dikembangkan oleh William Posser, dengan merujuk setidaknya pada empat bentuk gangguan terhadap diri seseorang:¹⁰

- (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 konsep hukum, risalah awal mengenai privasi muncul seiring dengan perkembangan perlindungan privasi dalam hukum, terhitung semenjak tahun 1890, ketika Samuel Warren dan Louis Brandeis menulis sebuah artikel dengan judul "The Right to Privacy", di Harvard Law Review.¹¹ Dalam tulisan tersebut Warren dan Brandeis secara sederhana mendefinisikan hak atas privasi sebagai 'hak untuk dibiarkan sendiri' (*the right to be let alone*). Gagasan ini kemudian mendapatkan justifikasi dan pengakuan dengan adanya beberapa gugatan hukum yang kemudian memeberikan pembenaran tentang perlunya perindungan hak atas privasi, terutama dengan sandaran alasan moralitas.¹²

Lebih jauh hak privasi bertujuan untuk melindungi orang-orang dari kemungkinan terlukanya perasaan dan kepekaan mereka, akibat orang lain menemukan hal-hal yang benar atas diri seseorang, tetapi memalukan atau fakta yang sangat pribadi, sebagai konsekuensi dari perilaku yang ofensif. Jurisprudensi Mahkamah Agung Amerika Serikat menyebutkan adanya dua dimensi dalam privasi: (i) kepentingan individu dalam menghindari pengungkapan hal-hal pribadi; dan (ii) keinginan dan kemerdekaan seseorang dalam membuat beberapa jenis keputusan penting.¹³

C. Jaminan perlindungan atas hak privasi

Dalam perkembangan hukum internasional hak asasi manusia, 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

⁹ Lihat A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), hal. 7-8.

¹⁰ William Prosser, "Privacy: A Legal Analysis", dalam Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, (Cambridge: Cambridge University Press, 1984), hal. 167.

¹¹ Lihat Samuel Warren dan Louis Brandeis, *The Right to Privacy*, dalam Harvard Law Review Vol. IV No. 5, 15 Desember 1890, tersedia di <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Gagasan dua orang pengacara Boston ini sebenarnya berangkat dari ide yang dicetuskan oleh hakim Thomas Cooley, yang menulis *Treatise on the Law of Torts* (1880), yang memperkenalkan pertama kali mengenai istilah 'hak untuk dibiarkan sendiri'.

¹² Sebagai contoh dalam kasus *Demay v. Roberts*, 46 Mich. 160, 9 N.W. 146 (1881), ketika seorang hakim Michigan menyatakan hak atas privasi dalam melahirkan. Juga kasus *Manola v. Stevens* (1890), dalam perkara tersebut seorang hakim New York mengeluarkan perintah pengadilan untuk melarang publikasi foto seorang aktris dengan celana ketat.

¹³ Lihat William G. Staples (ed.), *Encyclopedia of Privacy*, (Westport: Greenwood Press, 2007), hal. 397-398.

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:

“Setiap orang berhak atas perlindungan diri pribadi,¹⁴ 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

Secra detail dalam bagian penjelasan Pasal 31 UU Hak Asasi Manusia secara jelas diuraikan mengenai pengertian ‘tidak boleh diganggu’, dengan 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

¹⁴ Pasal yang dirujuk adalah pasal yang sama dalam dokumen UDHR, dalam hal ini term ‘privacy’ diterjemahkan sebagai ‘diri pribadi’.

dilakukan oleh otoritas yang ditunjuk dalam undang-undang tersebut, (e) hanya dilakukan atas dasar kasus per kasus.¹⁵

Panduan tersebut juga menegaskan adanya larangan praktik pengambilan dan penguasaan data pribadi tanpa didasarkan pada undang-undang oleh pihak lain, baik otoritas publik, maupun 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.¹⁶

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 1981.¹⁷ Pengadopsian ini diperkuat dengan lahirnya berbagai jurisprudensi yang dilahirkan oleh pengadilan HAM Eropa.¹⁸ Perkembangan serupa juga terjadi pada mekanisme HAM regional kawasan Amerika.

D. Ancaman terhadap perlindungan hak atas privasi

Di Indonesia sendiri, beberapa peraturan perundang-undangan memungkinkan aparat negara untuk melakukan praktik *surveillance* dan penyadapan terhadap warga negara.¹⁹ Tiadanya kesatuan hukum yang mengatur mengenai hal tersebut telah menciptakan kerentanan dari tindakan peyalahgunaan wewenang yang dilakukan aparat negara.²⁰ Selain oleh badan pemerintah, gangguan terhadap privasi juga sangat mungkin dilakukan antar-individu atau antar-badan privat, misalnya praktik penyadapan yang dilakukan terhadap individu oleh individu lainnya, atau tindakan penyadapan oleh korporasi terhadap korporasi lainnya yang menjadi saingan bisnisnya. Sedangkan praktik penyadapan yang dilakukan oleh badan pemerintah biasanya dilakukan untuk dua tujuan, penegakan hukum atau pelaksanaan fungsi intelijen dengan alasan keamanan nasional.

¹⁵ 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.unhcr.ch/tbs/doc.nsf/\(Symbol\)/23378a8724595410c12563ed004aeecd?Opendocument](http://www.unhcr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument).

¹⁶ Khusus di Amerika Serikat, Komisi Perlindungan Privasi, yang dibentuk oleh parlemen federal, menerbitkan sebuah laporan pada 1977, yang isinya mengenai daftar penerapan informasi yang adil, yang mengatur pengumpulan, penyimpanan, dan penggunaan informasi pribadi seseorang. Laporan tersebut merekomendasikan: (1) tidak diperkenankannya, pembentukan sistem data secara rahasia, yang materinya berisi informasi pribadi; (2) informasi pribadi hanya boleh dikumpulkan untuk tujuan yang sempit dan spesifik; (3) informasi pribadi hanya boleh digunakan dan konsisten dengan tujuan utama pengumpulan informasi; (4) informasi pribadi harus dikumpulkan hanya dengan persetujuan dari orang-orang yang dikumpulkan informasinya atau kuasa hukumnya, (5) informasi pribadi tidak boleh dibagikan kepada pihak ketiga tanpa pemberitahuan atau persetujuan; (7) demi akurasi dan relevansi, durasi penyimpanan informasi pribadi harus dibatasi; (8) individu harus memiliki akses ke informasi pribadi tentang diri mereka sendiri dan harus diizinkan untuk memperbaiki kesalahan; dan (9) orang-orang yang mengumpulkan data pribadi harus memastikan keamanan dan integritas data dan sistemnya. Lihat William G. Staples (ed.), *Encyclopedia of Privacy*, (Westport: Greenwood Press, 2007), hal. 399.

¹⁷ Lihat Pasal 8 Council of Europe Convention 1981.

¹⁸ Lebih jauh lihat, European Court of Human Rights, 2011, Internet: case law of the European Court of Human Rights, mencakup analisis atas semua kasus terkait internet dan kebebasan berekspresi serta perlindungan privasi sampai pertengahan tahun 2011.

¹⁹ Penyadapan (*wiretapping*) sebenarnya adalah istilah tradisional untuk intersepsi terhadap percakapan telepon. Pada mulanya, praktik ini dilakukan dengan memasang sebuah alat pada jaringan radio atau kantor telepon. Namun demikian dalam perkembangannya pengertian penyadapan tidak lagi terbatas pada intersepsi telepon, tetapi juga alat-alat elektronik lainnya. Lihat Whitfield Diffie dan Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, (Massachusetts: The MIT Press, 1998).

²⁰ 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>.

Buruknya perlindungan hukum terhadap hak atas privasi ini, diperburuk dengan kemungkinan massifnya praktik surveillance yang dilakukan oleh agensi intelijen pemerintah. Baru-baru ini militer Indonesia, melalui Badan Intelijen Strategis (BAIS) 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 mengoperasikannya, baik yang bertugas di dalam negeri maupun kantor-kantor Atase Pertahanan Indonesia di luar negeri.²¹

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).²² Teknologi ini dianggap sebagai salah satu yang paling canggih di pasar saat ini. Dalam promosinya Gamma Group menawarkan teknologi 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.²³

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 mentranskripsinya, 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.²⁴

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

Informasi lainnya juga menyebutkan adanya bantuan dari pemerintah Amerika Serikat, yang telah mengeluarkan dana sedikitnya 57 juta dollar AS, dari tahun 2006 hingga tahun 2008,

²¹ Lihat “Kemhan: Pengadaan Alat ANTI SADAP Untuk Amankan Informasi Strategis TNI”, dalam <http://www.kemhan.go.id/kemhan/?pg=31&id=1203>.

²² Lihat <https://www.gammagroup.com/> dan <http://www.finfisher.com/FinFisher/index.html>.

²³ 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.

²⁴ Lihat Finfisher promo videos, dalam <https://www.youtube.com/watch?v=qc8i7C659FU>.

²⁵ Lihat “You Only Click Twice: FinFisher’s Global Proliferation”, dalam <https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/>.

guna pembentukan *Integrated Maritime Surveillance System* (IMSS). Kerjasama kemiteraan ini merancang sebuah sistem 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.²⁶

Selain menggunakan teknologi 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.²⁷

Selain tingginya ancaman instruksi terhadap kehidupan pribadi oleh alat-alat negara, dalam bentuk surveillance dan intersepsi komunikasi, dalam hal perlindungan data pribadi, bila dibandingkan dengan negara-negara ASEAN lainnya, Indonesia juga paling tertinggal dalam penciptaan regulasi perlindungan data pribadi. Akibatnya data pribadi seseorang acapkali dipindahtangankan tanpa persetujuan dari pemilik data. Selain problem regulasi, mayoritas publik di Indonesia juga belum menjadikan data pribadi sebagai bagian dari properti dan hak asasi manusia yang wajib dilindungi.²⁸ []

²⁶ Lihat "Exploring Communications Surveillance in Indonesia", dalam <https://citizenlab.org/2013/10/igf-2013-exploring-communications-surveillance-indonesia/>.

²⁷ Teknologi ini telah digunakan di 83 negara (20 negara dengan baik ProxySG dan PacketShaper, 56 negara dengan PacketShaper, dan 7 negara dengan ProxySG).

²⁸ Perlindungan mengenai data pribadi (khususnya elektronik) hanya diatur secara terbatas di dalam Pasal 26 UU ITE dan PP No. 82 Tahun 2012.