Koleksi
Pusat Dokumentasi ELSAM

Praktek *Surveillance* dan *Unlawful Interception* sebagai Pelanggaran terhadap Hak Atas Privasi

Masitoh Indriani

A. Latar Belakang

Pesatnya perkembangan Teknologi Informasi (TI) membawa dampak terhadap pemanfaatan Internet di Indonesia. Menurut SGP, di tahun 2014 Indonesia merupakan salah satu negara pengguna Internet terbesar di dunia.[1] Besarnya angka tersebut menunjukkan bahwa masyrakat Indonesia telah melek Internet. Disisi lain, potensi permasalahan dalam pemanfaatan Internet menjadi salah satu modus baru dalam tindakan *Surveillance* (Pengawasan) dan *Interception* (Penyadapan).

Perkembangan pemanfaatan TI khususnya penggunaan Internet di Indonesia, memberikan sumbangsih terhadap perkembangan pola dan konsep privasi dalam ranah dunia siber. Sebelum mengenal Internet, masyarakat Indonesia memanfaatkan komunikasi intra personal secara langsung. Pola komunikasi konvensional ini berbasis kepada kepercayaan antar personal atau individu atau kelompok. Pasca membaiknya infrastuktur komunikasi serta dibarenginya dengan era *Internet Literate* yang diprakarsai oleh Kemeninfo, pola komunikasi masyarakat cenderung beralih dari metode konvesional *direct personal to personal* menjadi pola komunikasi *personal to personal IT based.*

Pola komunikasi tersebut akan memberikan dampak terhadap pemahaman bahwa ruang lingkup privasi akan mengikuti pola komunikasi yang telah terbentuk, bahwa semakin berkembangnya metode dan pola komunikasi yang dimaksud akan semakin mempersempit ruang privasi seseorang. Selaras dengan hal ini, ancaman terhadap privasi juga semakin menguat mengingat perkembangan IT, pola dan metode komunikasi tidak memperhatikan prinsip-prinsip pengaturan privasi melainkan kepada kecanggihan teknologi komunikasi yang tidak mengenal batasan.

Dalam kesaharian, sudah menjadi hal yang lazim bilamana kita menerima pesan singkat (*Short Message Services*/SMS) promo dari beberapa *provider* telepon selular ketika kita memasuki sebuah pusat perbelanjaan. Pertanyaan yang seringkali muncul, bagaimana provider telepon seluler tersbut mengetahui secara persis tempat yang kita kunjungi. Pertanyaan lain yang mengemuka adalah apakah terdapat *consent* antara *provider* telepon seluler dengan pengguna terkait dengan pesan singkat tersebut?

Kasus lain yang mengemuka adalah penangkapan koruptor dan teroris. Aparat penegak hukum memanfaatkan TI untuk memburu para koruptor dan teroris dengan cara menyadap segala aktivitas keseharian mereka terlepas dalam aktivitas keseharian tersebut mungkin terdapat beberapa aktivitas yang dapat dikategorikan sebagai aktivitas pribadi.

Isu hak atas privasi dalam kasus-kasus tersebut diatas begitu mengemuka ketika mencoba menggali lebih dalam bahwasanya adakah dasar hukum dalam melakukan kegiatan-kegiatan tersebut? Adakah kewenangan yang diberikan kepada para penegak hukum atau pun pihak provider dalam melaksanakan tugas dan fungsi yang melekat kepada mereka dengan

[1] Kathleen Azali, *Inside Indonesia: Boosting Youth Enterpreneurship in Creative Industries*, 2015, periksa juga Laporan APJII-PUSKAKOM UI, 2014, tersedia di http://www.apjii.or.id/read/content/info-terkini/301/pengguna-internet-indonesia-tahun-2014-sebanyak-88.html

mengatasnkaman kemanan nasional maupun untuk kegiatan yang bersifat promosi? Dalam hal ini apakah negara melakukan praktek *surveillance* terhadap warga negaranya?

B. *Surveillance* dan (*Unlawful*) *Interception* dalam Teori dan Praktek: Sebuah Pelanggaran Terhadap Privasi

I. Sejarah Surveillance

Surveillance pertama kali dikenalkan oleh Jeremy Bentham melalui isitilah *Panopticon*. Bentham merupakan salah satu penganut teori utilitarian yang mempercayai bahwa manusia secara intrinsik terikat untuk mencari kesenangan dan menghindari rasa sakit, dan bahwa nilai 'baik' dan 'buruk' didefinisikan oleh apa yang dianggap sebagai hal yang menyenangkan dan menyakitkan.[2] Lebih lanjut Bentham mengatakan bahwa:

> *"Alam telah menempatkan manusia di bawah pemerintahan dua tuan berdaulat, rasa sakit dan kesenangan. Hal ini untuk mereka sendiri untuk menunjukkan apa yang harus kita lakukan, serta untuk menentukan apa yang harus kita lakukan. Jika kita percaya bahwa untuk setiap tindakan kita akan ada reaksi dari orang lain, prinsip kami yang berlaku akan tidak bertindak dengan cara apapun yang menghasilkan reaksi negatif atau merugikan dari orang lain terhadap kita.Menerapkan prinsip ini untuk kejahatan, kita bisa mengatakan bahwa seseorang tidak akan melakukan kejahatan cenderung berarti satu menderita rasa sakit untuk melakukan tindakan, daripada mungkin kesenangan yang mungkin berasal darinya".*[3]

Lebih lanjut Bentham berujar bahwa sebagai bagian dari visi kontrol sosial yang bersifat rasional, perlu dilakukan upaya untuk merancang perangkat arsitektur yang disebut *Panopticon*, yang dalam Bahasa Yunani berarti merujuk pada arti '*all-seeing*'. *Panopticon* disini merupakan lembaga universal yang nantinya akan digunakan sebagai desain untuk meminimlakn jumlah pengawas yang diperlukan dan diusulkan untuk dimanfaatkan pada desain penjara, rumah sakit jiwa/mental dan sekolah.[4]

Pendekatan ini pada mulanya diharapkan dapat berhasil diterapkan dalam lingkungan yang melibatkan beberapa tingkat Surveillancedengan mengandalkan kunci efektivitas berupa sistem ketidakpastian. Desain *Panopticon* ini memastikan bahwa orang-orang yang diawasi tidak dapat melihat pengamat mereka. Mereka tidak memiliki cara untuk mengetahui apakah mereka sedang diawasi pada waktu tertentu, akan tetapi mereka mengethaui bahwa tidak ada wilayah yang bernama privasi. Tujuan psikologis sistem tersebut adalah bahwa subjek Surveillanceakan percaya bahwa pilihan logis mereka adalah untuk menyesuaikan diri. Dengan demikian setiap individu akan menjadi pengawas mereka sendiri.

Pro kontra yang timbul terhadap pendapat Bentham ini adalah ketika untuk mengamankan perilaku yang diinginkan dan untuk mencegah tindakan yang tidak diinginkan, masyarakat akan dengan secara tegas memberlakukan perangkat hukum yang ketat. Namun, pernyataan ini akan terjawab ketika Bentham menganggap bahwa harus terdapat pengaturan berupa undang-undang yang harus mengakomodasi keamanan atau dalam hal ini adalah rasa kebahagiaan dari orang perseorangan sehingga muncul adanya jaminan terhadap rasa kebahagiaan tersebut.[5]

Selain teori yang dikemuakan oleh Bentham, sebagai perbandingan adalah teori yang diutarakan oleh Faucoult dan Orwell. Faucoult dan Orwell berpendapat bahwa ide Panopticon dianggap ideal bilamana terdapat kekuasaan yang diatur di masyarakat modern. Selanjutnya, Faucolt berpendapat bahwa ide tersebut bukan hanyasebuah model untuk sebuah lembaga atau

---

[2] Jeremy Bentham, *Panopticon or the Inspection-House*, Dodo Press, 2008.

[3] *Ibid*.

[4] *Ibid*.

[5] *Ibid*.

institusi, akan tetapi sesuatu yang secara prinsip terdapat pengaturan kekuasaan kepada masyarakat.[6]

> *"The Panopticon...harus dipahami sebagai model digeneralisasikanya sebuah fungsi, cara mendefinisikan hubungan kekuasaan dalam kehidupan sehari-hari manusia ....Dalam hal ini Bentham menyajikan sebagai lembaga tertentu, tapi Panopticon adalah diagram mekanisme kekuasaan yang harus dikurangi untuk menjadi bentuk yang ideal fungsinya, harus disarikan dari setiap hambatan atau gesekan yang muncul, serta harus diwakili sebagai sistem arsitektur sebuah politik teknologi...".*[7]

Dari pandangan ahli tersbut dapat disimpulkan bahwa akar dan dasar pemikiran tentang *Surveillance* adalah sekumpulan prinsip-prinsip yang dapat diterapkan dalam setiap lingkup masyarakat yang membutuhkan beberapa tingkat pengaturan/regulasi. Tujuan dari kegiatan Surveillanceini adalah untuk mencegah dari berbagai potensi ancaman, sistem Surveillanceserta dampak yang ditimbulkan. Selain itu, Orwell menyimpulkan bahwa inti pembahasan dari *Surveillance* merupakan gabungan dari pengawasan sistem (kapital), birokrasi serta penataan masyarakat modern.[8]

Beberapa contoh desain *Panopticon* yang digunakan dalam kehidupan keseharian kita adalah misalnya pusat perbelanjaan modern. Pusat perbelanjaan adalah ruang terbuka yang luas yang dirancang sedemikian rupa untuk mempromosikan tingkat visibilitas dan keamanan yang sangat baik. Selain itu adalah *Lift*, dalam hal ini desain *Lift* seringkali adalah berupa desain dalam ruangan tertutup yang tertutup sedemikian rupa dan dilapisi kaca. Sebuah contoh utama dari mata *panopticon* yang digagas oleh Bentham.

II. Perkembangan Surveillance

Sementara itu di era yang lebih modern, David Lyon berpendapat bahwa *surveillance* merupakan sebuah satu kesatuan proses pengumpulan data personal, terlepas apakah hal tersebut teridentifikasi atau tidak dengan tujuan untuk mempengaruhi dan mengatur objek pengawasan.[9] Lebih lanjut dia mengemukakan bahwa *Surveillance* tersebut dilakukan secara sistematik dan rutinuntuk memperoleh informasi detail dengan tujuan tidak hanya untuk mempengaruhi dan mengatur melainkan juga mengarahkan objek pengawasan.[10]

Dari berbagai pendapat yang ada, sesungguhnya *Surveillance* mempunyai dua sisi wajah yang berbeda. Hal ini dapat dijelaskan bahwa kegiatan *Surveillance* dimana didalamnya juga termasuk *Interception*, adalah bukti nyata tentang pengklasifikasian kegiatan yang bersifat positif dan negatif. Dalam pengertian positif, *Surveillance* memberikan jaminan tentang keamanan dan kenyamanan di ranah publik dan sebagai pola represntasi dari era modern serta simbol dari pola tata kelola pemerintahan yang lebih maju. Sedangkan dalam pandangan negatif, *Surveillance* dipandang sebagai tindakan pengawasan yang menciptakan rasa kekhawatiran dan mengancam kebebasan individu di ranah publik.

Pada awal dipraktekannya Surveillance, kegiatan ini bertujuan untuk mengatur informasi personal.[11] Pihak atau pelaku *Surveillance* memanfaatkan TI dengan tujuan untuk mendapatkan data detail tentang keseharian seseorang misalnya data finansial, catatan kesehatan, preferensi pilihan terhadap produk tertentu, transaksi elektronik , data komunikasi telepon, alamat tempat kediaman, latar belakang etnis, latar belakang pendidikan hingga catatan kriminal.[12]

---

[6] *Ibid*.

[7] Ibid, hal. 205.

[8] David Lyon, Surveillance Study: an Overview, Polity, 2007, hal. 46.

[9] David Lyon dalam Collin J. Bennet, *The Privacy Advocate: Resisting the Spread of Surveillance*, the MIT Press, Cambridge, Massachusetts, 2008, hal. 11.

[10] *Ibid*.

[11] David Lyon, *The Electronic Eye: the Rise of Surveillance Society*, Polity Press, 1998.

[12] *Ibid*, hal. 84.

Kesemua aktivitas pengumpulan data tersebut memberikan kesimpulan bahwa TI telah memberikan sumbangsih nyata terhadap praktek *Surveillance*.

Dalam prakteknya sekarang, beberapa negara maju seperti Inggris dan Amerika Serikat membuat praktek *Surveillance* menjadi alat pengawas perilaku bagi masyrakat sipil. Inggris menerpakna sistem Big Brother dengan memasang berbagai alat perekam di wilayah publik seperti jalan raya, bandara, stasiun kereta api, pusat perbelanjaan hingga perkantoran. Sedangkan di Amerika Serikat, pasca kejadian 9/11 , AS lebih ketat dalam menerapakn pola pengawasannya sampai pada ttitik tertentu dianggap menciderai wilayah privasi warga negaranya.[13] Belum lagi pasca kasus Wikileaks dan pembocoran data oleh kontraktor National Security Agency (NSA) Edward Snowden. Hal tersebut selaras dengan apa yang diutarakan oleh Lloyd bahwa:

> *"...an appropiate balance between privacy is expressed in the term of the right to be left alone and surveillance representing the wish to discover informatiaon about another, is difficult to define. Although initially appearing as opposite..."*[14]

Praktek *Surveillance* yang bersifat publik di Indonesia tidak sedetail seperti yang telah dilakukan oleh Inggris dan AS, terdapat beberapa hal yang menjadi diskusi umum terkait dengan pelanggaran hak privasi warga negaranya. Diskursus pelanggaran hak privasi warga negara ini mengemuka ketika perkembangan teknologi informasi di Indonesia berada pada tahap yang *urgent*. Sehingga diskursus yang selama ini ada, menjadi sebuah pertanyaan, apakah memang benar bahwa *Surveillance* yang dilakukan oleh pihak *State* maupun *Corporate* telah melanggar hak privasi seseorang?

Pelanggaran terhadap Hak atas Privasi merupakan salah satu persoalan yang penting dimana *Surveillance* menjadi salah satu penyebab terlanggarnya hak atas privasi tersebut. Salah satu mekanisme legal yang menjamin hak atas privasi terhadap *Surveillance* adalah terdapatnya pengaturan yang bersifat baku yang harus diterima oleh pelanggan. Disisi lain privasi merupakan hak warga negara mana pun untuk mengontrol informasi peribadinya dan mengambil keputusan tentang hal itu, baik untuk menyimpan maupun untuk membukanya kepada publik. Karena hal tersebut, privasi yang merupakan hak asasi yang mendasar menjadi kabur pemaknaanya bila dihadapkan pada kondisi apa yang ditawarkan dalam persyaratan yang bersifat baku tersebut.

Selain itu, pelanggaran terhadap hak atas privasi juga terkait dengan kebudayaan dan gaya hidup suatu negara juga mempengaruhi praktik terkait dengan privasi. Sehingga dalam bebrapa hal, terdapat anggapan bahwa isu *Surveillance* merupakan pelanggaran terhadap hak tas privasi tergantung terhadap penerapan dan pengaturan terhadap privasi.

Jovan Kurbalija memperkenalkan segitiga privasi dimana terdapat 3 (tiga) hubungan antar entitas yang menggambarkan pola *Surveillance* sebagai bentuk pelanggaran hak atas privasi.[15] Segitiga ini memperlihatkan tentang pola hubungan yang tercipta antara entitas individu, dunia industri dan negara atau pemerintah. Hubungan pertama adalah antara individu dengan sektor industri, hubungan ini menggambarkan pola *Surveillance* yang dilakukan oleh sektor industri kepada para individu, baik metode maupun contohnya. Hubungan kedua adalah persamaan pola *Surveillance* Negara dengan sektor Industri. Hubungan ketiga adalah antar individu dimana munculnya resiko pelanggaran terhadap hak atas privasi dari satu individu ke individu lainnya.

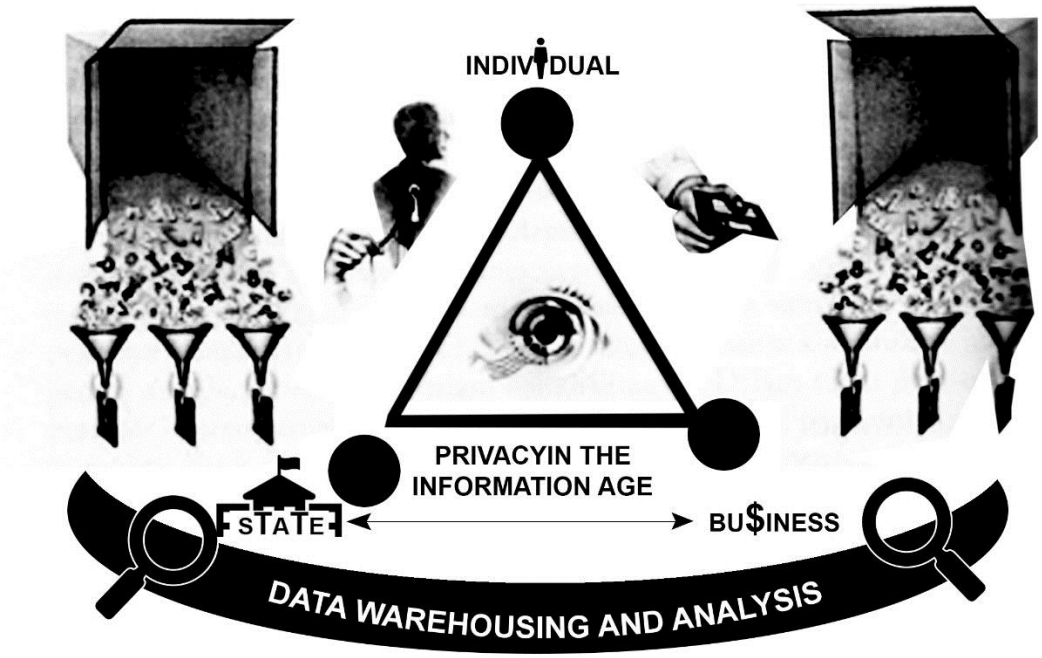
---

[13] *Ibid*.

[14] Ian J. Lloyd, *Information Technology Law*, 6th edition, Oxford University Press, 2011

[15] Jovan Kurbalija, *an Introduction to Internet Governance*, 6th Edition, Diplo Foundation, 2014.

Figure 1 : Segitiga Privasi (Kurbalija, 2014)



Individu vs Sektor Industri

Kegiatan *Surveillance* dalam hubungan antara individu dengan sektor individudapat dilihat bahwa terdapatnya pemberian *consent* yang tidak disadari oleh para individu untuk memberikan data pribadi mereka. Para individu ini harus menerima sebuah terms and conditions yang bersifat memaksa karena merupakan salah satu persyaratan yang harus dilakukan dan dapat dikategorikan sebagai sebuah perysratan baku. Misalnya adalah pemberian data pribadi dalam pembukaan rekening bank dan pembayaran online dengan memanfaatkan kartu kredit. Selanjutnya dibawah ini akan dibahas mengenai pola atau jenis *Surveillance* yang melibatkan sektor industri dengan individu.

1. *Online Marketing*

Jenis kegiatan *Surveillance* yang seringkali digunakan oleh dunia industri adalah melalui Online Marketing. Salah satu contoh dari online marketing adalah *advertisement targeting* (*ad-targeting*). *Ad-targeting* adalah kegiatan yang dilakukan oleh kalangan industri dengan menarget para *potential consumer* untuk memasarkan produk barang dan jasa tertentu. Latar belakang dipilihnya para pelaku industri memanfaatkan teknologi ini adalah karena ad-targeting dianggap memberikan keakurasian dalam promosi dan pemasaran serta berbiaya rendah.

Kegiatan *ad-targeting* yang sering dialami oleh para pelanggan adalah pemanfaatan teknologi *cookies* pada aktivitas *serach engines*. Pola sejarah pencarian (*search history*) kita di Internet tercatat dengan bantuan teknologi *Cookies*[16]. Sebagai hasilnya, aktivitas pencarian kita akan terekam dan akan terlihat di kegiatan daring selanjutnya, misalnya akan tertampil ditampilan surat elektronik, media sosial maupun platform *online* lainnya.

Hal ini seperti yang diutarakan oleh Randal C. Picker yang menyatakan bahwa media sosial memberikan sumbangan besar dalam pengembangan teknologi ad targeting yang

[16] Cookies adalah kumpulan file kecil yang disimpan di dalam komputer pengguna. Cookies dirancang untuk sedemikian rupa untuk menyimpan data spesifik pada situs web tertentu, sehingga dapat diakses balik oleh server website yang pernah dikunjungi.

mengakibatkan adanya persaingan Kebijakan Privasi di ranah media sosial.[17] Picker mencontohkan adanya persaingan antara Facebook dengan Google dengan memanfaatkan preferensi pencarian pelanggan dimana di sisi yang lain para pelanggan tidak menyadari bahwa aktivitas pencarian mereka telah diketahui, dicatat dan dimanfaatkan dalam pengembangan bisnis model *provider*.

Selain contoh tersebut diatas adalah adanya pengembangan teknologi yang didasarkan pada lokasi geografis pelanggan atau biasa disebut sebagi *Mobile Phone Ad Targeting*. *Mobile Phone Ad Targeting* adalah teknologi marketing yang beroperasi di sistem perangkat iOS dan Android dan mempunyai fitur melakukan *ad–targeting* dalam jarak 100 meter seperti halnya *apps downloads*, *landing pages* atau *driving directions* yang muncul ketika pelanggan membuka sebuah aplikasi di perangkat mobile nya.[18]

Kegiatan online marketing lainnya yang mempunyai pola pemanfaatan teknologi yang sama dengan *Mobile Phone* adalah *Geographic Messaging Services Platform* (GMSP) dengan memanfaatkan teknlogi smart phone atau mobile devices pelanggan. Menurut Convert Digests, GMSP adalah:

> *"...as a hosted service, tracks opt-in subscribers' locations on behalf of the service provider and pushes mobile content to the subscriber when and where is appropriate based on the advertising campaign developed and managed by the 1020 Placecast platform".*[19]

Teknologi serupa dengan GMSP adalah *Location-Based Marketing* (LBM). LBM merupakan teknik online marketing yang menarget pengguna telepon seluler dalam area geografis tertentu dengan tujuan untuk meningkatkan efektivitas promo dan pemasaran sektor industri tertentu.[20] Cara kerja dari LBM adalah dengan memanfaatkan teknologi *bluetooth* atau wifi yang ada di dalam perangkat mobile pelanggan. LBM juga memberikan kemudahan bagi provider untuk menarget pelanggan dalam jarak yang sangat dekat.

Praktek di Amerika dan Uni Eropa, terdapat pengaturan khusus tentang ad targeting dengan memperhatikan beberapa prinsip perlindungan terhadap hak atas privasi consumer, misalnya terdapatnya pengturan berupa opsi atau pilihan '*do not track*' atau '*reject cookies*'. Di Amerika Serikat sendiri pada Desember 2010 Federal Trade Commission (FTC)[21] memperkenalkan mekanisme pengaturan untuk perlindungan privasi para pelanggan untuk tidak turut serta dalam program OBA[22].

Dari data yang dilaporkan oleh We Are Social, jumlah populasi total orang Indonesia adalah 255.5 juta jiwa dengan presentase urbanisasi sebesar 50%. Sedangkan jumlah *mobile*

---

[17] Randal C. Picker, *Online Advertising, Identity and Privacy*, University of Chicago Law & Economics Working Paper No. 475., Juni 2009, tersedia pada http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1428065&download=yes atau tersedia juga di The Chicago Working Paper Series Index: http://www.law.uchicago.edu/Lawecon/index.html

[18] ThumbVista, a mobile Marketing & Advertising Company, http://www.thumbvista.com/mobile-advertising-company/ , lihat juga http://www.huffingtonpost.com/brian-honigman/how-sms-text-messaging-retains_b_3697107.html

[19] GMSP pertama kali dipekenalkan oleh perusahaan Alcatel Lucent yang kemudian dikembangkan oleh Bell Lab, sebuah jasa penyedia layanan telekomunikasi yang berbasis di Amerika Serikat , tersedia di http://mobiledevdesign.com/mobile-apps/platform-delivers-location-based-mobile-messaging

[20] Asosiasi Location Based Marketing, tersedia di http://www.thelbma.com/

[21] FTC adalah dalah lembaga independen pemerintah Amerika Serikat, yang didirikan oleh Federal Trade Commission Act. Misi utama dari FTC adalah mempromosikan perlindungan konsumen dari penghapusan dan pencegahan praktek bisnis anti persaingan sehat.

[22] OBA atau *Online Behavioral Advertising* adalah teknik pengumpulan preferensi pelanggan di Amerika Serikat yang menggunakan metode penargetan perilaku *consumer*, yang melibatkan pengelola *website* dan para pengiklan yang bertujuan untuk meningkatkan efektivitas iklan dengan menggunakan informasi perilaku web-browsing dari seorang pelanggan.

connection di tahun yang sama adalah 308.2 juta jiwa dengan total penetrasi sebesar 121%, serta 62 juta didalamnya sebagai pengguna aktif media sosial berbasis mobile connections.[23]

Besarnya angka penggunaan internet mobile memberikan kontribusi permasalahan privasi dan perlindungan data pribadi pada perangkat mobile tersebut. Komunikasi mobile atau seluler yang mempunyai karakteristik unik berupa IMEI[24] dan IMSI[25] memberikan peluang bagi provider maupun pihak ketiga lainnya untuk melakukan *data tracking* dan *data gathering* si pengguna. Sebagai contoh adalah data tracking berupa sms[26] atau pesan promosi lainnya ketika user berada di tempat publik seperti pusat perbelanjaan. Acapkali user tanpa sadar menerima pesan berupa tawaran diskon dari *tenants* yang berada di pusat perbelanjaan tersebut.

Pertanyaan muncul ketika bagaiamana provider atau pihak ketiga tersbut mengetahui lokasi rela time (*real time locaction*) dimana user berada. Contoh lain yang lebih marka adalah penawaran fasilitas kartu kredit oleh berbagai bank melalui telepon secara langsung ke nomor seluler atau *mobile* para *users*, sama halnya diatas, bagaiamana bank-bank yang dimaksud memperoleh nomor seluler para *users*, apakah perolehan data pribadi berupa nomor seleluer tersebut sepengathuan oleh *users*?

2. *Cloud Computing*

Dikenalkannya berbagai inovasi TI seperti *Cloud Computing System* juga mendukung berubahnya pola interaksi diantra para users. Dengan memanfaatkan 'space' kosong yang ditawarkan oleh berbagai apkikasi *cloud computing*, para users tidak perlu melakukan penyimpanan data (*data storage*) secara manual dengan menggunakan hard drive nya. Para user cukup memanfaatkan space tersebut untuk menyimpan data secara daring. Sebagai contoh, aplikasi daring Dropbox dan Google Drive menawarkan fasilitas penyimpanan data daring menjadi magnet tersendiri bagi para *users* dengan dalih menghemat *space disk* di perangkat *hardware* para *users* serta kemudahan akses karena adanya tingkat mobilitas yang tinggi.

Persoalan yang mengemuka dalam *cloud computing system* ini adalah pihak provider mempunyai akses penuh terhadap data yang tersimpan didalam program tersebut. Kemampuan pihak provider mengelola dan mengamankan data menjadi tantangan tersendiri terhadap isu privasi yaitu sejauh mana keamanan data para user akan terlindungi. Meskipun pada prakteknya pihak provider telah membuat perjanjian *privacy consent* yang menyebutkan bahwa provider tidak akan menyalahgunakan (*misuse*) data tersebut,[27] terdapat sebuah klausula yang sifatnya mementahkan pernyataan tersebut yaitu bahwa pihak user harus tunduk terhadap semua ketentuan dari *provider*. Hal ini merupakan pernyataan yang bersifat kontraproduktif terhadap pernyataan sebelumnya.

Selain itu, dengan dikenalkannya teknologi *Cloud Computing* semakin membuat Hak atas Privasi semakin terancam. *Cloud Computing* adalah teknlogi gabungan penyimpanan data yang berbasis pda Internet. Lebih lanjut *Cloud Computing* memungkinkan seluruh koleksi sumber daya komputasi seperti aplikasi, ruang penyimpanan dan pengolahannya untuk dikirimkan atau di transfer lmelalui media Internet. *Cloud Computing* merupakan perkembangan teknologi penyimpanan dan pemrosesan data *users* yang saling menhubungkan para users di seluruh

---

[23] We Are Social, Digital in Indonesia, 2015 Report, available at http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

[24] IMEI adalah singkatan dari *International Mobile Station Equipment Identity*. IMEI terdiri dari 15 digit angka. IMEI membawa informasi tentang ponsel yang bersangkutan seperti pabrik pembuat ponsel, model ponsel, dsb.

[25] IMSI (International Mobile Subscriber Identity) adalah 15 digit kode unik yang secara internasional digfunakan untuk mengidentifikasi pengguna dalam sebuah jaringan GSM. IMSI merupakan kode yang bersifat unik dengan artian bahawa tidak akan ada nomor IMSI yang sama diseluruh dunia.

[26] SMS adalah suatu fasilitas untuk mengirim suatu pesan dan menerima singkat berupa teks melalui perangkat nirkabel, yaitu perangkat komunikasi telepon selular.

[27] Periksa Dropbox Privacy Policy

dunia.[28] Pemanfaatan *Cloud Computing* ini juga dilirik oleh provider besar seperti Google dengan fitur Google Drive, Dropbox dan Windows Aure karena dianggap memberikan keuntungan yang cukup besar. Hal ini diungkapkan oleh Soghoian:

> *"The cloud computing model brings a number of important benefits to service providers: reduced piracy, the ease of denying access to troublesome users, protection of sensitive technology and intellectual property, the ability to serve carefully targeted advertising to customers and increased security."*[29]

Dengan kemudahan yang ditawarkan oleh *Cloud Computing System*, perpindahan data termasuk didalamnya data pribadi menjadi semakin berisiko tinggi mengingat sifat Internet yang tidak mengenal batas (*borderless*). Hal ini sangat kontras ketika proses perpindahan data yang dimaksud dilakukan tanpa sepengetahuan subjek data atau dalam hal ini adalah pelanggan. Memang para penyedia layanan *Cloud Computing* ini telah memberikan sebuah pengaturan khusus terkait dengan pemanfaatannya dalam *Privacy Policy*, namun kebijakan tersebut sangat pro kepada penyedia layanan disebabkan dari teknologi yang ditawarkan *Cloud Computing* tersebut. Sebagai contoh, Google yang menawarkan Google Drive sebagai salah satu penyedia layanan *Cloud Computing* mempunyai kebijakan privasi kontra produktif dengan jasa yang ditawarkan.

3. Social Media

Sejalan dengan maraknya pemanfaatan cloud computing adalah pemanfaatan sosial media sebagai platform baru model komunikasi. Facebook, WhatsApp, Twitter, Path, Instagram, Pinterest, Google+ adalah contoh media sosial yang paling jamak dimanfaatkan oleh masyarakat Indonesia. Data dari We Are Social menyebutkan bahwa terdapat 72.7 Juta pengguna Internet aktif di Indonesia[30] dengan rincian 72 juta pengguna aktif media sosial, 308,2 Juta pengguna pernagkat mobile dengan 62 juta didalamnya sebagai *active mobile social accounts*.[31] Laporan lain menunjukkan bahwa Facebook menempati urutan pertama sebagai platform media sosial paling aktif digunakan oleh orang Indonesia diikuti dengan aplikasi WhatsApp di urutan kedua dan Twitter di urutan ketiga.

Data tersebut menunjukkan bahwa begitu besar jumlah pengguna internet khususnya social media yang dimanfaatkan oleh masyarakat Indonesia. Media sosial menjadi sebuah tren bukan tanpa adanya sebab. Fasilitas yang ditawarkan berbagai penyedia media sosial memberikan alternatif model baru cara berinteraksi melalui konten popluer berbasis layanan gratis. Konten populer yang disediakan pleh provider media sosial menerapkan konten yang mengandung data dan informasi pribadi para *users*.

Contoh yang paling mutakhir praktek *Surveillance* terhadap pengguna Social Media pemanfaatan aplikasi baik itu yang berbasis perangkat Android maupun perangkat iOS. Para *users* tersebut dapat memanfaatkan aplikasi yang dikehendaki dengan persyaratan tertentu yaitu adanya *Permission Access* ke data personal yang ada di perangkat para users. Permission Access ini disetiap aplikasi mempunyai akses yang berbeda, ada beberapa aplikasi yang mempersyaratkan atau meminta akses ke data personal berupa poto, lokasi real time, wifi information, SMS, nomor kontak hingga alamat email yang ada di perangkat *mobile* para users, namun ada beberapa juga yang hanya mempersyaratkan akses ke masuk ke beberapa item tertentu saja.

---

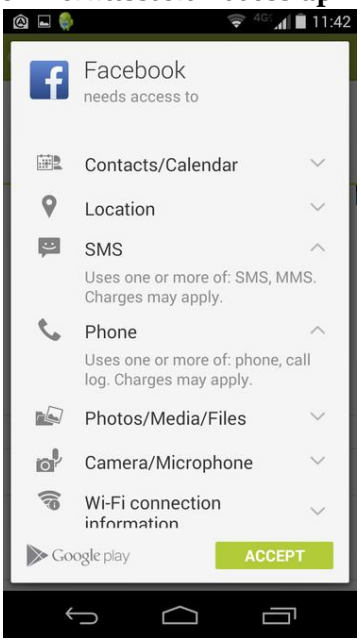
[28] Christopher Soghoian, C*aught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, August 20109, Vol. 8., Journal on Telecomm and High Tech., L. 359., Berkman Center Research Publication No. 2009-07. Tersedia di http://ssrn.com/abstract=1421553

[29] *Ibid*, hal. 364.

[30] We Are Social Report, January 2015 available at http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

[31] Ibid

Figure 2: Contoh *Permission Access* aplikasi Facebook



Persyaratan *Permission Access* ini biasanya tergantung dengan jenis layanan yang ditawarkan oleh aplikasi yang bersangkutan. Permasalahan yang ditimbulkan adanya *Permission Access* adalah bahwa para users tidak diberikan pilihan untuk *decline* atau *reject*, sifat dari *Permission Access* ini adalah baku atau dengan kata lain adalah persyaratan '*take it or leave it*'. Lebih lanjut, bahwa persyaratan baku semacam ini tidak memberikan ruang partisipasi *consumers* untuk lebih menjaga kerahasiaan data personalnya. Para *consumers* dihadapakan pada posisi yang tidak berimbang.

Dari beberapa contoh *ad-targeting*, sistem *cloud computing* dan *mobile connection* tersebut diatas, nampak jelas bahwa industri diuntungkan dengan membaiknya infrastuktur pendukung, memberikan kesempatn dan peluang baru dalam berbagai tindakan yang nantinya menintervensi privasi pelangga serta akan melakukan apa yang disebut sebagai *Surveillance* perilaku para pelanggan dengan memanfaatkan teknologi tertentu dan menawarkan kebijakan yang bersifat baku.

Negara - Sektor Industri

Hal penting yang perlu digarisbawahi pada hubungan ini adalah terdapatnya kesamaan pola *Surveillance* yang dilakukan oleh dua sektor ini. Negara mengumpulkan data warga negara melalui berbagai program, misalnya terkait dengan penyelenggaran peridentitasan nasional. Permasalahan akan muncul bilamana dan sejauh mana Negara atau pemerintah akan melindungi data pribadi tersebut?

Sedangkan sektor industri melakukan *Surveillance* ke para pegawai serta ke para pelanggan. Surveillance kepada para pegawai disini dilakukan untuk mengawasi aktivitas keseharian para pegawai bai ksecara langsung amupun tidak. Secara langusng dapat kita amati dengan pemasangan CCTV sebagai alat kontrol perilaku, alat presensi berupa *finger print*, kartu identitas pegawai dan bentuk lainnya yang memanfaatkan TI sebagai basis operasionalnya. Secara tidak langusng dapat dilihat pada praktik penyadapan melalui email, telepon kantor hingga telepon seluler prbadi.

Pada akhirnya pola *Surveillance* antara Negara dengan sektor industri akan menjadi sebuah simbiosis mutualisme dimana terdapat penukaran data dari sektor industri ke Negara. Tukar menukar data dalam hal ini pada dasarnya untuk mencegah kegiatan terlarang seperti halnya terorisme, namun pertanyaan mendasar adalah mengenai tata cara perolahan data yang

dimaksud. Apakah tata cara tersebut secara hukum dibenarkan? Bagaimana perlindungan negera kepada warga negara nya terkait dengan hak atas privasi mereka?

Individu vs Individu

Aspek terakhir dari perlindungan privasi menurut segitiga ini adalah adanya resiko dari para individu. Bahwa individu mempunyai kapasaitas untuk melakukan *surveillance* ke sesama individu. Maraknya perkembangan IT serta pekembangan ekonomi memberikan kemudahan bagi para individu untuk mampu membeli peralatan *surveillance* yang dimaksud. seperti halnya ketika Kurbalija mengutip tentang temuan the Economist bahwa teknologi telah menyebabkan adanya 'demokratisasi penyadapan'[32]. Hal ini dapat dilihat bahwa para individu memang telah terbukti melakukan aktivitas *Surveillance* kepada sesama baik dengan cara penyadapan, pengintaian dan spionase elektronik.

Bentuk atau Pola Penyadapan yang dipraktekkan oleh individu adalah berupa penyadapan komunikasi dan tindakan pengintaian. Penyadapan secara sederhana dapat dilakukan oleh para individu dengan memanfaatkan teknologi penyadapan sederhana yaitu penyadapan dengan menggunakan alat tertentu dan penyadapan dengan menggunakan aplikasi atau software tertentu. Penyadapan diantara para individu ini sebenarnya terjadi akibat adanya ketidakpercayaan yang timbul akibat pemanfaatan teknologi yang menggiring perilaku sesama individu untuk saling mengawasi satu sama lainnya, belum lagi ada kemudahan yang ditawarkan oleh jasa penyedia layanan seperti the Truth Spy.

Figure 3: Contoh Iklan the Truth Spy



Penyadapan dengan menggunakan alat tertentu yaitu berupa alat *interceptor*. Cara kerja alat ini adalah dengan cara memanfaatakn frekuensi sinyal yang tertangkap oleh alat komunikasi. Selanjutnya dengan dilengkapi *Radio Frequency Triangulation Locator* yang berfungsi untuk menangkap sinyal secara akurat, alat ini juga dilengkapi dengan sebuah *software Digital Signal Processing* yang membuat pemrosesan algoritma bisa berjalan cepat dan mudah. Sehingga, pengguna alat ini dapat menangkap sinyal dan trafik atau jalur data dari alat komunikasi selular dan mengincar spesifikasi target tertentu. Jadi, alat ini bisa menyadap berbagai pembicaraan di ponsel-ponsel yang sinyalnya masih tertangkap di dalam jangkauan alat tersebut.

Sementara itu penyadapan yang dilakukan dengan bantuan software tertentu yang biasa disebut dengan software mata-mata (*spy software*). Seperti halnya sebuah program jahat semacam trojan dan malware, spyware mampu melacak aktivitas ponsel dan mengirimkan

[32] *Ibid*, hal. 151.

informasi tersebut kepada pihak ketiga, dalam hal ini adalah si penyadap. Oleh karenanya, aplikasi spyware menyebabkan baterai dan pulsa ponsel bakal cepat terkuras. Program ini dapat menonaktifkan program tertentu di dalam ponsel, bahkan menghapus informasi yang tersimpan dalam ponsel tanpa sepengetahuan pemilik ponsel. Beberapa fitur yang ditawarkan Spy software ini antara lain Ambience Call Listening, Live Call Recording, Track WhatsApp, GPS Tracking Location, Manage Call, Monitor Internet Activities, Record Apps Usage, Key Logger, Remotely Control, Record SMS message, Read Contact History, View Multimedia Files, Auto Answer (Spy-Answer), View Notes Contents dan masih banyak lagi fitur lainnya.[33]

Dari berbagai pola praktek Surveillance dan Interception terhadap pelanggaran Privasi, permasalahan utama dalam hal ini terlihat bahwa sebgian besar perlindungan hak atas privasi terlalu fokus terhadap pelanggaran yang dilakukan oleh negara dan sektor industri. Pengaturan individu yang melakukan *surveillance* terhadap sesama individu belum tersentuh. Sebagai contoh bahwa Amerika Serikat dan Jerman adalah dua negara yang sudah mengadopsi peraturan yang mencegah tentang adanya tindakan kegiatan *surveillance* perorangan. Kedepannya, diharapkan Indonesia mampu untuk membuat serta menerapkan peraturan yang dimaksud.

C. Pengaturan *Surveillance* dan *Interception*: *Existing Condition* dan Prinsip-Prinsip Pengaturan

Pengaturan *Surveillance* termasuk didalamnya adalah kegiatan *Interception* di Indonesia tersebar dalam berbagai peraturan perundangan, antara lain di UU ITE, UU KPK, UU Anti Terorisme UU Narkotika, UU ITE, UU Intelijen Negara, sampai dengan peraturan menteri dimana aturan terbaru adalah tentang pengaturan penggunaan *drones* di wilayah publik hingga peraturan yang bersifat teknis.

Banyaknya pengaturan ini mempengaruhi dan mengakibatkan banyaknya perbedaan penafsiran apa itu S*urveillance* dan *Interception* baik dari segi pengertian, pengaturan hingga lembaga mana yang paling berwenang dalam melakukan tindakan *Surveillance* dan Intersepsi. Belum lagi terdapat fakta bahwa tindakan ini juga dilakukan oleh entitas swasta dalam hal ini korporasi hingga orang perseorangan.

Permasalahan yang timbul dari pengaturan ini adalah tidak adanya pengaturan prinsip-prinsip standar perlindungan terhadap privasi seseorang. Beberapa prinsip yang perlu dikedepankan dalam pengaturan *surveillance* dan *interception* menyangkut tentang kewenangan, tujuan dan pemanfaatan, dan hal teknis terkait dengan tata cara, pengawasan, serta mekanisme komplain bilamana terjadi kerugian dari pihak ketiga terhadap kegiatan *Surveillance* dan *Interception* tersebut.

Di Indonesia, terdapat beberapa kali kesempatan pengujian materiil pasal-pasal yang berkaitan dengan Surveillance dan Interception ke Mahkamah Konstitusi (MK) seperti halnya pengujian terhadap UU No. 11 Tahun 2008 tentang ITE[34] dan UU No. 30 Tahun 2002 tentang KPK[35]. Putusan MK tersebut secara garis besar memuat tentang prinsip-prinsip dasar tindakan *Surveillance* dan *Interception*, yaitu antara lain:

a. otoritas resmi yang ditunjuk dalam Peraturan perundang-undangan untuk memberikan izin melakukan tindakan Surveillancedan intersepsi;
b. jangka waktu yang pasti dalam melakukan *Surveillance* dan intersepsi;
c. pembatasan penanganan materi hasil penyadapan;
d. pembatasan pihak-pihak yang mempunyai akses penyadapan.

---

[33] The Truth Spy adalah salah satu jasa penyedia layanan Spyware yang menawarkan layanan Spware dengan berbasis sistem operasi Android dan IOS. Informasi lebih lengkap dapat dilihat di laman http://thetruthspy.com/

[34] Putusan Perkara No. 5/PUU-VIII/2010

[35] Putusan Perkara No 006/PUU-I/2003, Putusan Perkara No 012-016-019/PUU-IV/2006

Sementara itu, unsur-unsur yang harus ada didalam pengaturan *Interception* antara lain:

a. wewenang untuk melakukan, memerintahkan maupun meminta penyadapan;
b. tujuan penyadapan secara spesifik;
c. kategori subjek hukum yang diberi wewenang untuk melakukan penyadapan;
d. pengaturan izin dari otoritas sebelum melakukan tindakan *Surveillance* dan *Interception*;
e. tata cara pengawasan dan *Interception*;
f. penggunaan hasil penyadapan, dan
g. mekanisme komplain bilamana terjadi kerugian yang timbul dari pihak ketiga atas dilakukannya tindakan penyadapan tersebut, serta pengaturan lain berupa sanksi pelanggaran, dan mekanisme internal untuk menjamin HAM seperti penyadapan dalam keadaan mendesak, keikutsertaan pihak ketiga dalam teknis penyadapan dan hal lainnya yabng dirasa penting dalam pengaturan intersepsi ini.

D. Kesimpulan

Berkembangnya Teknlogi Informasi dan infrastruktur penunjangnya memberikan pengaruh yang besar terhadap pola perilaku komunikasi masyarakat. Pola perilaku komunikasi masyarakat sekarang ini didominasi dengan penggunaan berbagai *gadget* yang berbasis atau bertumpu pada jasa layanan *provider* dimana bila ditelaah lebih dalam, terdapat berbagai potensi pelanggaran yang terjadi. Salah satunya adalah pelanggaran hak atas privasi. Pelanggaran hak atas privasi terjadi bilamana terjadi penyalahgunaan pemanfaatan teknologi baik secara sengaja maupun tidak dimana pelanggaran hak atas privasi merupakan salah satu persoalan yang penting dimana *Surveillance* dan *Interception* menjadi salah satu penyebab terlanggarnya hak atas privasi tersebut.

Praktek *Surveillance* dan *Interception* yang melanggara hak atas privasi yang terjadi saat ini tidak hanya berpusat atau dipraktekkan oleh Negara atau Pemerintah yang mempunyai kewenangan, namun ternyata juga terjadi atau dipraktekkan oleh kalangan korporasi bahkan oleh sesama individu. Praktik *Surveillance* dan *Interception* tersebut sejatinya diperlukan penyeimbang berupa pengaturan yang ideal dengan mempertimbangkan prinsip-prinsip pengaturan yang baik serta mampu melindungi *users*.[]