Modul 4:

Privasi & Keamanan di Internet

kemudi

Bab 1:

Ada Apa dengan Privasi?

I. Peduli Soal Privasi

Istilah privasi belum pernah sepopuler sekarang, terutama jika berbicara dalam konteks Indonesia. Seiring dengan perkembangan teknologi informasi dan bertambahnya layanan online yang diakses oleh masyarakat, istilah privasi menjadi lebih familiar. Apabila ingin menggunakan suatu layanan online seperti Gojek atau membuat akun sosial media seperti Facebook kita akan melihat kebijakan privasi (*privacy policy*) yang perlu disetujui oleh calon pengguna. Pertanyaannya kemudian, apakah para pendaftar membaca ketentuan tersebut?

Mungkin para pengguna melewati dan menyetujui kebijakan privasi begitu saja asal mereka bisa secepatnya terdaftar dan menggunakan layanan yang diinginkan. Kebiasaan tersebut sering diartikan secara keliru sebagai sikap pengguna yang tidak peduli soal privasi. Menurut Pew Research Center, separuh dari orang Amerika yang terkoneksi dengan internet tidak mengetahui apa itu kebijakan privasi. Privasi merupakan sebuah konsep yang rumit. Ketika pengguna layanan online luput membaca kebijakan privasi dan asal menyetujuinya, bukan berarti la tidak peduli. Privasi masih menjadi konsep yang asing bagi banyak pengguna layanan online, meskipun istilah ini sering menjadi bahan pembicaraan. Kesadaran tentang privasi juga lekat hubungannya dengan kebebasan berekspresi dan isu keamanan. Pemahaman tentang privasi berkembang seiring dengan kondisi masyarakat dan inovasi teknologi informasi. Kehadiran konsep ini berhubungan dengan konteks budaya di suatu wilayah karena apa yang dianggap 'hal pribadi' bisa berbeda di satu daerah dan lainnya. Privasi termasuk dalam komponen hak dasar dalam deklarasi hak asasi manusia (lihat lebih lanjut di sini).

Sikap tidak peduli dan menganggap bahwa privasi bukan sesuatu yang penting bisa didasari oleh ketidaktahuan tentang ancaman dan risiko terhadap privasi seseorang. Ada anggapan jika tidak ada yang disembunyikan, tidak ada yang perlu ditakuti (*if you have nothing to hide, you have nothing to fear)*. Privasi sering dipahami sebagai sesuatu yang 'perlu' dilindungi hanya bagi kalangan tertentu (misalnya selebriti dan aktivis). Siapa yang peduli rumah saya di mana dan siapa nama ibu kandung saya, jika saya bukan siapa-siapa? Pertanyaan semacam ini mungkin pernah terlintas atau terdengar dalam pembahasan privasi. Kenyataannya, meskipun kita bukan selebriti atau bagian dari kelompok oposisi pemerintah, ada berbagai

pihak yang peduli dan bahkan ingin mengetahui lebih jauh lagi tentang informasi pribadi kita. JIka informasi tersebut tidak penting, penyedia layanan dan pemerintah mungkin tidak akan membutuhkan informasi pribadi kita. Begitu pula dari sisi kita sebagai warga negara yang tentu membutuhkan layanan-layanan online tertentu untuk melancarkan aktivitas, seperti layanan email atau transfer data. Di sisi lain, informasi pribadi juga berkaitan dengan persoalan keamanan dari segi pengguna. Misalnya, beberapa akun sosial media dan surel memerlukan nomor ponsel untuk verifikasi dan memastikan keamanan akun penggunanya tidak dibobol oleh orang yang berniat buruk.

II. Memaknai Privasi

Privasi adalah konsep yang cukup rumit dan telah melalui perjalanan filosofis yang panjang. Sebagai bagian dari salah satu hak manusia yang paling mendasar, privasi otomatis menjadi kebutuhan penting seorang individu. Kebutuhan akan privasi terkait erat dengan integritas dan harga diri seseorang. Meskipun tidak mudah untuk mendefinisikan secara persis apa itu privasi, konsep ini mencakup hak-hak lain sesuai konteksnya, seperti: kebebasan untuk berpikir, hak atas kesendirian, hak untuk melindungi reputasi, serta hak untuk mengontrol tubuh sendiri. Privasi dimaknai sesuai dengan konteks yang berlaku, oleh karena itu pemaknaan akan konsep ini sangat beragam. Di era modern seperti sekarang, privasi terdiri dari dua dimensi yaitu isu yang berhubungan dengan identitas seseorang dan bagaimana informasi tersebut ditangani, terutama oleh pihak ketiga. Pembahasan privasi bergulir seiring dengan perkembangan teknologi. Guna memudahkan pemaknaan tentang privasi, kita bisa memaknainya secara mendasar sebagai konsep yang menjunjung tinggi kemandirian, otoritas, dan harga diri seseorang dengan menghargai keberadaan ruang pribadi (Unesco, 2012). Sederhananya, seseorang memiliki informasi atau melakukan sesuatu yang hanya ingin dia ketahui sendiri atau diceritakan hanya pada orang yang ia percaya dan ia memiliki kontrol terhadap informasi tersebut.

Konsep ini memang mulai sering dibicarakan setelah teknologi digital menjadi bagian dari keseharian masyarakat. Namun isu soal privasi bukanlah hal baru, perdebatan tentang konsep ini bahkan sudah ada sejak zaman kemunculan koran. Dalam makalah terkenal " The Right to Privacy" yang ditulis oleh Samuel Warren dan Louis Brandeis pada 1890, penulis merujuk pada koran yang menampilkan foto orang-orang. Mereka memperkenalkan hak atas kesendirian (*The Right to be Left Alone)* dan mengedepankan pentingnya perlindungan bagi seorang individu dan kepemilikan. Persoalan privasi juga berhubungan kuat dengan fungsi media dalam sistem demokrasi yang menjunjung tinggi kebebasan berekspresi. Di satu sisi, demokrasi menjamin kebebasan berekspresi, sedangkan di sisi lain, ia juga harus melindungi privasi seseorang. Kebebasan untuk berekspresi diseimbangkan dengan perlindungan privasi agar kebebasan tersebut tidak melanggar privasi seseorang. Dalam konteks lain, proteksi privasi penting untuk menjamin kebebasan berekspresi. Misalnya ketika seseorang mengungkapkan fakta yang berisiko membahayakan dirinya, informasi pribadi seperti alamat rumah, nomor telepon dan lainnya perlu dilindungi agar ruang pribadinya tidak diserang. Seiring dengan semakin pentingnya peran komputer dalam menjalankan rutinitas masyarakat modern, pemahaman soal privasi berkembang menjadi hak seseorang untuk menentukan kapan, bagaimana dan hingga sejauh mana informasi pribadinya bisa disebarkan atau dibagi ke pihak lain.

Pemaknaan tentang batasan ruang pribadi dan apa yang dianggap sebagai hal yang pribadi tentu tidak bisa disamaratakan dari satu budaya dengan budaya di wilayah lainnya. Privasi memang erat kaitannya dengan konsep kebebasan seorang individu dan dalam konteks budaya yang cenderung kolektif, batasan ruang pribadi bisa berbeda dengan budaya yang individualis. Apa yang dianggap pribadi bagi masyarakat di Inggris misalnya, belum tentu ditafsirkan sebagai sesuatu yang bersifat pribadi di tengah masyarakat Indonesia. Walaupun konteks bisa beragam, risiko pelanggaran privasi berlaku di seluruh kondisi. Mungkin kita pernah dihadapkan pada pelanggaran privasi namun kita belum menyadari bahwa itu adalah pelanggaran. Misalnya ketika tiba-tiba berbagai pihak dari perusahaan asuransi hingga penyedia layanan fitness menelpon atau menawarkan layananya padahal kita tidak pernah memberikan informasi nomor telepon ke pihak tersebut. Artinya, informasi kita bisa saja disalahgunakan atau dimanfaatkan oleh pihak ketiga tanpa sepengetahuan dan seizin kita.

Ketika kita menggunakan satu layanan dan memberikan informasi pribadi ke pihak penyedia layanan, diasumsikan kita percaya pada pihak penyedia layanan bahwa mereka tidak akan menyalahgunakan atau menyebarkan informasi kita. Persoalan privasi juga mempunyai dimensi gender yang seringkali luput untuk diperhatikan. Berbagai kajian telah menyadarkan risiko yang berpotensi menggunakan teknologi informasi untuk mencederai privasi perempuan demi kepentingan seksual atau kekerasan dalam bentuk ancaman. Seperti yang terjadi pada kasus Revenge Porn -atau di forum online seperti Kaskus kerap disebut dengan istilah 'barisan sakit hati', ketika sekelompok orang menyebarkan foto-foto pribadi yang eksplisit secara seksual dari para perempuan yang menjadi korban ancaman mereka. Berbagai bentuk pelanggaran terhadap privasi inilah yang kemudian membangun kesadaran akan pentingnya privasi.

Terkait dengan contoh kasus di atas, baca kutipan artikel di bawah ini:

“ Sukabumi -
Seorang pria berinisial RNG (28) diamankan Satuan Reserse dan Kriminal (Satreskrim) Polres Sukabumi Kota dari kediamannya di daerah Ciomas, Kabupaten Bogor sekira pukul 04.30 WIB, Rabu (1/7/2015). RNG dilaporkan mantan kekasihnya sendiri berinisial MA (20) warga Kelurahan Gunungparang, Kecamatan Cikole, Sukabumi, Jawa Barat.

Saat digelandang ke ruang penyidik RNG terus menghindari sorot kamera sejumlah media, ia diduga menjadi pelaku penyebar foto bugil MA melalui sejumlah akun di jejaring sosial. Pasalnya dalam laporan korban kepada polisi, pelaku sempat beberapa kali melakukan pengancaman untuk menyebarkan foto-foto pribadi korban ke jejaring sosial.

Dalam laporan polisi, korban menyebut jika pelaku telah menyebar foto-foto pribadinya ke sejumlah media sosial diantaranya Pinterest, Facebook, Instagram dan Twitter. “Atas ulah pelaku, korban merasa tak tenang kemudian membuat laporan polisi. Dalam keterangannya korban juga mengaku pernah diancam oleh pelaku jika tak segera meminta maaf maka foto-foto pribadinya akan disebar,” imbuh Diki Budiman.

Sementara itu pelaku sempat membantah semua tudingan yang ditujukan kepadanya terkait penyebaran foto-foto pribadi mantan kekasihnya. Namun ketika polisi memeriksa lebih jauh akhirnya ia mengakui semua perbuatannya.

Dari keterangan pelaku diketahui jika dirinya marah terhadap sang mantan, status pacaran yang terjalin selama dua tahun harus kandas di tengah jalan. Meski begitu, pelaku mengakui tak ada orang ketiga diantara mereka yang menjadi penyebab hubungan tersebut harus berakhir. “Tanpa sebab tanpa alasan, dia putusin saya,” aku RNG dihadapan penyidik. “

(sumber: http://news.detik.com/berita/2958022/hubungan-berakhir-pria-ini-sebar-foto-bugil-sang-mantan-di-medsos)

Diskusikan pertanyaan berikut (20 menit):

1. Menurut peserta, apakah foto-foto seperti kasus di atas merupakan bagian dari privasi perempuan dan (mantan) kekasihnya ?
2. Mengapa pelaku menggunakan foto-foto tersebut untuk mengancam kekasihnya?
3. Terkait dengan jenis kelamin dan gender, pihak mana yang lebih rentan dalam situasi tersebut, laki-laki atau perempuan?

Tugas

Analisis Informasi yang Dikumpulkan oleh Facebook dan Google

Facebook dan Google, dua layanan online yang tidak bisa dipisahkan dari keseharian. Kita tahu cara menggunakannya, tapi apakah kita tahu informasi apa saja yang dikumpulkan oleh Facebook dan Google? Mungkin kita sudah terlanjur membuat akun, menggunakannya selama bertahun-tahun, dan terlalu bergantung kepada kedua layanan tersebut. Tidak ada kata terlambat, sekarang saatnya kita melek tentang apa yang mereka ketahui tentang diri kita. Tugas ini akan berkaitan dengan bab selanjutnya. Berikut langkah-langkahnya:

1. Buka kedua tautan berikut: Google (https://www.google.com/intl/id/policies/privacy/) dan Facebook (https://www.facebook.com/about/privacy/)
2. Untuk laman bahasa Indonesia, silakan lihat pengaturan sesuai akun kamu
3. Baca bagian: “Informasi yang Kami Kumpulkan” (untuk Google) dan “Informasi Apa Saja yang Kami Kumpulkan?” (untuk Facebook)
4. Buat daftar informasi apa saja yang dikumpulkan oleh masing-masing platform
5. Setelah mendaftar informasi apa saja yang mereka kumpulkan dari kamu, jawab pertanyaan berikut:
    a. Apakah kamu telah memperkirakan dan mengetahui sebelumnya bahwa kedua platform ini mengumpulkan informasi tersebut?
    b. Setelah mengetahui informasi apa saja yang dikumpulkan oleh Facebook dan Google, apakah kamu merasa khawatir bahwa informasi tersebut disimpan dan digunakan sesuai kepentingan platform?
    c. Apakah kamu percaya bahwa Facebook dan Google menyimpan informasimu dengan aman dan tidak akan disalahgunakan?
    d. Setelah mengetahui daftar tersebut, apakah kamu ingin mengontrol informasi apa saja yang ingin kamu bagi?

Bab 2:

Apa yang Mereka Ketahui tentang Kita

I. Privasi Online

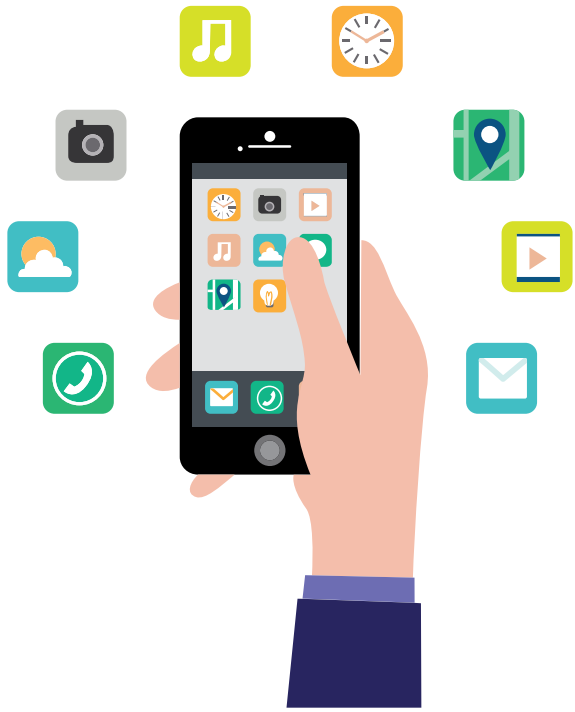
Tugas di sesi sebelumnya membantu kita merinci apa saja informasi yang kita bagi ke pihak Facebook dan Google. Jangan lupa membayangkan bahwa proses pengumpulan data tersebut dilakukan terus menerus 24 jam, 7 hari seminggu. Di era digital, informasi pribadi bukan hanya sebatas data seperti nomor telepon, alamat rumah, tanggal lahir, nama keluarga (orang tua atau ibu kandung), dan lainnya. Informasi pribadi juga bisa diambil dari:

- data transaksi keuangan online (kartu kredit dan perbankan),
- kondisi kesehatan (seperti penggunaan aplikasi kesehatan),
- foto atau gambar yang diunggah online,
- wajah (dari foto yang diunggah di media sosial),
- lokasi (seperti media sosial Foursquare),
- alamat protokol internet (IP Address),
- bahkan kata kunci yang kita ketik saat menggunakan mesin pencari.

Terjemahan percakapan di ilustrasi di atas:

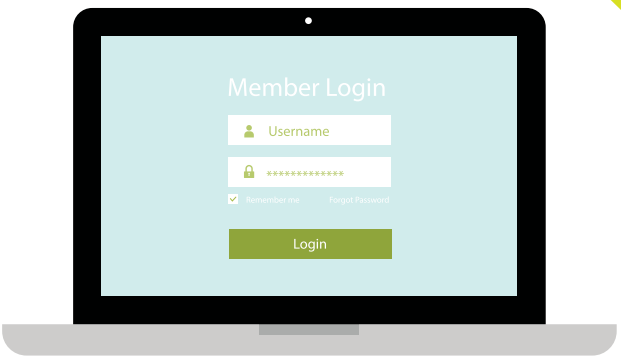
iPhone terbaru akan mendeteksi jari kamu.
NSA (National Security Agency-Amerika Serikat): "Mereka (pembeli/pengguna) akan membayar 650 dolar."
CIA (Central Intelligence Agency- Amerika Serikat): "Untuk memberikan sidik jari mereka ke kita"

Konsep privasi menjadi semakin penting dibicarakan di era seperti sekarang, karena kemunculan teknologi yang mampu merekam dan menyimpan bentuk baru dari informasi pribadi, contohnya sidik jari, wajah dan bahkan retina mata seseorang. Proses merekam dan menyimpan tersebut tidak hanya dilakukan dalam skala kecil tapi juga skala besar. Bayangkan berapa banyak pengguna ponsel seperti iPhone yang menggunakan sidik jari atau pengguna Facebook yang mengidentifikasi atau *tag* wajah seseorang (lihat ilustrasi di atas). Penggunaan internet yang digabungkan dengan pemakaian ponsel semakin menyebar ke berbagai lini kehidupan juga melancarkan jalan tersebut, bahkan dengan kemampuan penyebaran yang lebih luas dari yang pernah kita bayangkan. Di antara berbagai bentuk medium komunikasi, ponsel merupakan salah satu medium yang paling personal dan identik dengan kepemilikan ruang pribadi. Keberadaan internet dan penggunaan ponsel memungkinkan untuk:



- Mengumpulkan informasi pribadi dalam bentuk-bentuk baru
- Menjembatani dan mendorong pengumpulan dan penentuan lokasi informasi pribadi
- Membangun kapasitas baru bagi pemerintah dan pihak swasta untuk menganalisis informasi pribadi
- Melahirkan peluang komersial baru untuk menggunakan dan mengolah informasi personal
- Mengakibatkan tantangan regulasi baru mengingat karakteristik internet yang lintas batas geografis

Fenomena pengumpulan informasi pribadi dalam bentuk baru juga menciptakan kecenderungan yang ganjil terkait dengan pemahaman dan penerapan konsep privasi. Dalam tingkatan konsep atau abstrak, orang-orang memahami risiko pelanggaran privasi dan pentingnya perlindungan privasi, namun pada praktiknya mereka seolah tidak peduli dengan privasi (Turow, 2014). Seperti yang telah dikemukakan di sesi sebelumnya, ada jarak antara kesadaran privasi pada level konsep dengan apa yang orang-orang lakukan saat online. Batasan yang publik dan yang privat di internet memang tipis dan tidak mudah untuk konsisten terhadap batasan tersebut. Fakta ini tidak bisa dipungkiri karena Internet menjadi medium yang mengakomodasi dua kebutuhan, medium untuk berkomunikasi (seperti e-mail , pesan instan dan telepon) dan medium untuk mempublikasikan sesuatu (media sosial, blog, mengunggah foto, dll). Dengan kemampuan interaktif, lintas batas dan kecepatan yang dimiliki Internet, pihak pemerintah juga menggunakannya untuk memudahkan pengelolaan administrasi dan kebutuhan interaksi dengan warga (Cth: melayangkan keluhan langsung ke pemerintah, pemilu, identitas warga, dll).



Dengan aplikasi internet yang begitu masif dalam mengumpulkan informasi, kunci dari konsep privasi adalah kontrol pengguna/warga terhadap informasi pribadinya, penghormatan batas privasi dan perlindungan terhadap informasi tersebut. Ibaratnya seorang teman baik yang dipercaya untuk menyimpan rahasia dan menjamin rahasia yang disimpan tidak akan disebarkan. Para penyedia layanan, baik pihak swasta maupun pemerintah, harus melindungi informasi yang kita berikan, bagaimanapun caranya. Sayangnya, pihak swasta seringkali menyajikan kebijakan privasi yang rumit sehingga menyebabkan pengguna enggan mengkajinya lebih dalam (Fernback & Papacharissi, 2007).

Ilustrasi kasus pembobolan data informasi pribadi di ranah digital:

"Data pemilih Filipina yang mencakup 70 juta orang dibocorkan peretas, sebulan sebelum pemilihan umum. Data pribadi, termasuk sidik jari dan paspor milik sekitar 70 juta orang dikabarkan telah bocor. Komisi Pemilihan Umum Filipina (COMELEC) memastikan situs internetnya diretas pada akhir bulan Maret.

Kelompok peretas Anonymous Philippines menyatakan bertanggung jawab terhadap serangan itu.Kelompok tersebut ingin menggarisbawahi "kerapuhan" sistem, termasuk terkait penggunaan mesin pemilihan otomatis yang akan digunakan pada 9 Mei mendatang. LulzSec Philippines, kelompok peretas kedua, diduga mengunggah seluruh bank data COMELEC di internet beberapa hari kemudian. COMELEC menyatakan tidak ada data sensitif yang dikeluarkan, kata sejumlah laporan.

Meskipun demikian, perusahaan keamanan internet Trend Micro meyakini kejadian ini adalah pembobolan data terkait pemerintah terbesar dalam sejarah Filipina dan pemerintah telah meremehkan masalah ini."

(sumber: http://www.bbc.com/indonesia/dunia/2016/04/160411_dunia_filipina_pemilu)

Diskusikan pertanyaan berikut (25 menit):

1. Menurut peserta, kemungkinan apa saja yang bisa terjadi jika ada pihak yang memiliki data sebanyak kasus di atas? Apa yang kira-kira bisa dilakukan oleh pihak tersebut?
2. Apa yang seharusnya dilakukan oleh pemerintah Filipina?

Untuk informasi tentang kasus kebocoran data skala besar lainnya bisa lihat di situs http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Eksperimen (Tugas)

Mau tahu siapa yang membuntuti dan 'kepoin' jejak bayangan digital kamu? Ikuti instruksi berikut:

1. Buka *browser* yang biasa kamu gunakan (cth: Opera, Firefox, Safari, Internet Explorer, Chrome)
2. Buka situs ini https://www.ghostery.com/try-us/download-browser-extension/
3. Unduh ekstensi/ *adds-on* Ghostery sesuai dengan *browser* kamu (biasanya langsung otomatis mengarahkan sesuai *browser* yang kamu gunakan), klik 'Add to (*browser* kamu)i'
4. Ekstensi akan langsung aktif terpasang di *browser*
5. Beraktivitaslah seperti biasa dengan browser-mu , kunjungi situs-situs yang ingin kamu lihat atau gunakan
6. Cari simbol bergambar 'hantu' di dekat area untuk mengetik domain *website*
7. Setiap kamu mengunjungi suatu website, perhatikan simbol hantu tersebut. Biasanya akan muncul angka dalam lingkaran merah (lihat gambar 1)
8. Klik simbol hantu tersebut dan lihat 'Ghostery Found ... Trackers'
9. Di kolom tersebut Ghostery menampilkan siapa saja yang sedang melacak kamu di situs tersebut.
10. Kamu bisa memilih siapa yang boleh dan tidak boleh melacak aktivitasmu. Jika menginzinkan akan ditandai dengan tombol biru. Jika kamu ingin menghentikan pelacak tersebut, geser tombolnya ke kanan sampai berwarna merah.
11. Jika ingin mengetahui lebih lanjut siapa pelacak tersebut, klik pelacak dan tautan 'click here for more information'
12. Coba kunjungi lebih dari 1 situs dan cek siapa saja yang melacakmu. Kemudian jawab pertanyaan berikut:
    a. Ada berapa banyak pihak yang melacakmu?
    b. Apakah ada pelacak yang kamu izinkan? Apa alasannya?
    c. Apakah ada pelacak yang tidak kamu izinkan? Apa alasannya?
    d. Bagaimana pendapatmu tentang pelacakan tersebut?

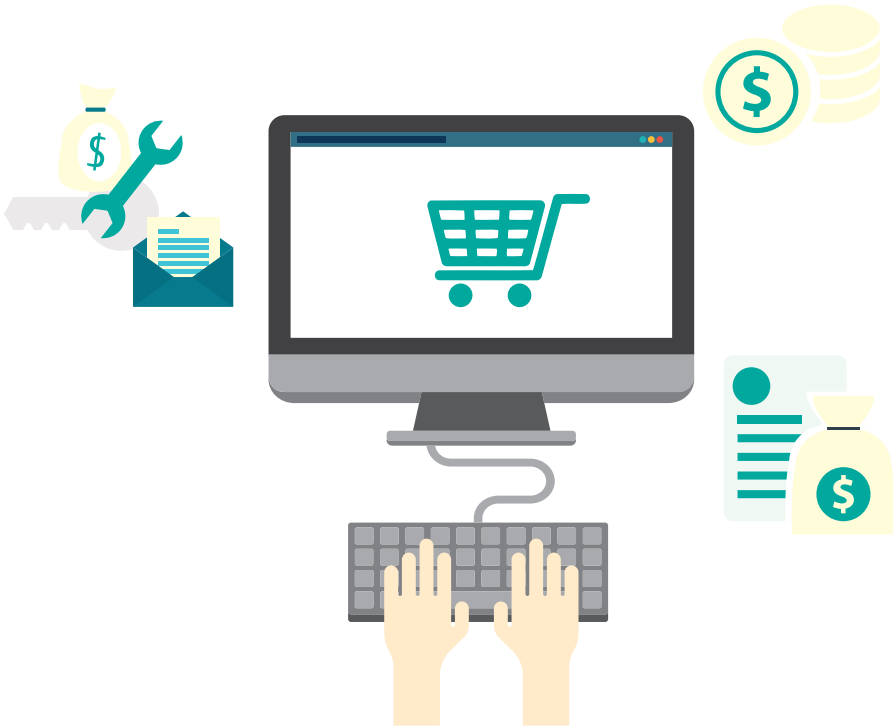
Bab 3:

Menelusuri Jejak & Bayangan Digital

I. Jejak Digital dan Risiko Pengintaian

Informasi Pribadi sebagai Alat Tukar

Seperti kata pepatah, tidak ada makan siang yang gratis, transaksi jasa memerlukan alat tukar. Di era digital, informasi adalah alat tukar yang ampuh untuk mengakses layanan-layanan online yang tersedia. Internet dirayakan sebagai simbol keterbukaan dan kebebasan. Pengguna bisa mengakses beragam pengetahuan dan layanan dengan gratis tanpa perlu membayar dengan uang. Mengapa para penyedia layanan dan konten online mau memberikan layanannya



secara cuma-cuma? Model ekonomi yang berlandaskan pada informasi (*information economy*) menjadikan informasi sebagai komoditas yang berharga. Informasi tersebut bisa dimanfaatkan untuk berbagai hal yang menguntungkan. Sebelum keberadaan internet begitu masif seperti sekarang, sebuah perusahaan membutuhkan biaya yang cukup banyak untuk melakukan survei guna mengetahui perilaku konsumennya. Sedangkan saat ini, pengguna dengan sukarela memberikan informasi tersebut secara langsung dan tidak langsung. Penyedia layanan seperti Google misalnya, bisa mengetahui apa yang sedang kamu cari dan butuhkan, di mana kamu berada, apa film, musik, buku favorit kamu, dan masih banyak lagi. Fasilitas interaktif atau layanan yang disediakan oleh pemerintah juga menerapkan cara serupa agar mereka bisa membaca warganya dengan lebih baik. Setiap kita online, kita meninggalkan jejak bayangan yang terus direkam.

Tugas di sesi sebelumnya membantu kamu untuk menyadari dan memahami seberapa banyak informasi yang bisa direkam dan dipantau ketika kamu melakukan aktivitas online. Jika beberapa waktu belakangan mulai sering mendengar istilah Big Data dan bertanya-tanya apa maksudnya. Nah, tugas tersebut juga bisa memberikan ilustrasi, berapa banyak data yang dikumpulkan oleh sebuah platform online jika kamu menggunakannya minimal 10 jam sehari, 7 hari seminggu, 30 hari sebulan, dll. Dan tentunya bukan hanya data kamu saja yang mereka kumpulkan, ada milyaran informasi pengguna yang mereka kumpulkan. Terbayang kan betapa 'besar' (Big) datanya. Data tersebut digunakan oleh penyedia layanan untuk menyediakan slot atau layanan beriklan oleh pihak yang ingin mengiklankan produknya. Tapi sebelum mereka menjual slot iklan tersebut, mereka terlebih dahulu mengolah data yang dikumpulkan untuk membangun profil tentang kamu sebagai subyek data. Layanan iklan ini menyumbangkan salah satu pemasukan terbesar bagi platform seperti Facebook misalnya, mendapatkan keuntungan sebesar 1 trilyun dolar di awal tahun 2016 dan 80% -nya adalah penerimaan dari iklan *mobile* (lihat di sini).

Memang ada beberapa keuntungan dari merekam informasi tersebut, di antaranya seperti: kita bisa mendapatkan rekomendasi sesuai dengan pencarian yang kita mau (misalnya sesuai lokasi, harga, dll), keamanan akun atau sebagai bentuk konfirmasi bahwa pengakses akun tersebut benar-benar kamu dan bukan orang lain, dan menyimpan informasi agar kita tidak perlu lagi memasukkannya (cth: tanggal lahir, alamat, dll).

1. Privasi dan Risikonya (Taksonomi Privasi)

Daniel J. Solove, seorang pakar hukum dari George Washington University merumuskan taksonomi privasi agar kita bisa lebih memahami persoalan dan aktivitas yang berisiko terhadap pelanggaran privasi. Subyek data adalah kita sebagai individu yang memberikan informasi. Berikut taksonomi untuk memudahakan kita memahami persoalan privasi.

a. Pengumpulan informasi

Informasi bisa dikumpulkan sebelum dan sewaktu kita mengakses sebuah layanan atau konten.

i. **Pengawasan**: Melihat, mendengarkan, atau merekam aktivitas seseorang.

ii. **Interogasi**: Menanyakan atau menggali informasi dengan berbagai cara.

b. Pemrosesan informasi

Setelah dikumpulkan, informasi disimpan, diolah, dan dimanfaatkan sesuai dengan tujuan yang dimaksud. Berikut risiko dan permasalahan yang bisa terjadi dalam fase ini:

i. **Agregasi**: Menggabungkan atau mengombinasikan berbagai potongan informasi untuk kemudian menjadikannya data tentang seseorang. Seperti merangkai bagian *puzzle*.

ii. **Identifikasi**: Mengaitkan informasi dengan individu-individu tertentu.

iii. **Ketidakamanan**: Ketidakmampuan untuk melindungi informasi yang disimpan dari pembobolan atau akses yang tidak dikehendaki.

iv. **Penggunaan kedua**: Menggunakan informasi yang disimpan untuk satu kepentingan yang berbeda dari seharusnya tanpa persetujuan subyek data.

v. **Eksklusi**: Subyek data gagal atau tidak bisa mengakses data miliknya yang telah disimpan dan tidak diberikan izin untuk mengontrol pengaturan dan penggunaannya.

c. Diseminasi informasi

i. **Pelanggaran kerahasiaan**: Melanggar perjanjian untuk merahasiakan informasi yang disimpan.

ii. **Membocorkan rahasia**: Mengungkap informasi sesorang yang sebenarnya dan mempengaruhi cara orang lain dalam menilai karakter individu tersebut.

iii. **Ekspose**: Mengungkapkan fungsi tubuh, kondisi fisik atau ketelanjangan seseorang.

iv. **Meningkatkan aksesibilitas**: Membuat informasi yang disimpan menjadi lebih mudah di akses oleh pihak lain.

v. **Pemerasan:** Mengancam untuk membocorkan rahasia demi kepentingan tertentu.

vi. **Apropriasi**: Penggunaan identitas subyek data untuk kepentingan dan tujuan orang lain.

vii. **Distorsi**: Menyebarkan informasi yang salah dan menyesatkan tentang si subyek data.

d. Invasi

i. **Intrusi**: Mulai menganggu dan menyerang ruang pribadi seseorang.

ii. **Mempengaruhi keputusan**: Ketika pihak luar mulai mencoba untuk mempengaruhi keputusan seseorang.

Untuk konteks Google, risiko yang paling rentan dialami oleh pengguna adalah dalam proses agregasi, distorsi, eksklusi dan penggunaan kedua (Tene, 2007). Mungkin kamu bertanya-tanya, pernahkah Google melanggar janjinya? Simak studi kasus berikut:

II. Studi Kasus

" KOMPAS.com — Google menghadapi tuduhan serius di Belanda. Pemerintah setempat telah melakukan investigasi yang menghasilkan penilaian bahwa Google melanggar kebijakan privasi penggunanya.

Google mengumpulkan informasi perilaku pengguna di internet untuk tujuan pemasangan iklan. Dengan informasi tersebut, iklan bisa ditujukan ke pengguna yang tepat. Investigasi yang dilakukan oleh Data Protection Agency (DPA) Belanda ini dilakukan selama tujuh bulan. DPA menuduh Google melakukan kegiatan pengumpulan data melalui mesin pencarinya tanpa disadari oleh pengguna.

Hasilnya, Google dianggap kurang informatif tentang data yang dihimpun oleh raksasa mesin pencari ini. Dikutip dari *Engadget,* Jumat (29/11/2013), peraturan kebijakan privasi Google terakhir diperbarui pada dua tahun lalu. Selain mesin pencari Google, DPA juga menemukan fakta yang sama di layanan Gmail dan YouTube. Beberapa data tersebut sifatnya sensitif, seperti informasi pembayaran, data lokasi, dan informasi perilaku pengguna dalam berselancar internet di berbagai situs web.

Sebelumnya, otoritas Perancis juga telah melakukan investigasi pada 2012, dan hasilnya sama. Di Eropa sendiri, total ada enam negara yang keberatan dengan metode pengumpulan data yang dilakukan Google. Google mengatakan bahwa pihaknya telah mematuhi hukum yang berlaku di Eropa. Namun, hal itu masih harus dibuktikan Google di sesi dengar pendapat dengan DPA."

(sumber: http://tekno.kompas.com/read/2013/12/02/1508296/Google.Disebut.Melanggar.Hak.Pengguna.demi.Iklan)

Diskusikan pertanyaan berikut:

1. Bagaimana pendapatmu terkait kasus pelanggaran privasi oleh Google tersebut?
2. Apa yang seharusnya dilakukan oleh Google?
3. Apa yang seharusnya dilakukan oleh pengguna?

Eksperimen 2 (Tugas)

Siapa yang melacak jejakmu?

Disadari atau tidak, meskipun kamu bukan seorang selebriti, selalu ada pihak yang melacak jejakmu. Misalnya saat kamu membaca berita di situs-situs berita favorit. Mau tahu siapa saja yang bisa dan sedang melacak jejakmu? Ikuti Instruksi berikut:

1. Buka situs Trackography* di https://trackography.org
2. Pilih opsi 'I can do this alone'
3. Kamu akan melihat gambar peta dunia, Klik peta 'Indonesia'.
4. Di kolom sebelah kiri, pilih situs media Nasional atau Internasional yang sering kamu kunjungi. Klik kotak situs tersebut.
5. Kemudian klik kotak 'Companies' di sebelah Kanan.
6. Lihat perusahaan mana saja dan apa saja yang mereka lakukan terhadap informasi kamu.
7. Berikut panduan keterangannya:
   a. *National Laws*: Hukum negara mana yang mengatur perusahaan tersebut.
   b. *Profiling*: Apakah perusahaan bisa membangun informasi milikmu menjadi subyek data?
   c. *Data retention*: Berapa lama perusahaan tersebut menyimpan data informasi milikmu?
   d. *Third Parties*: Apakah pihak ketiga bisa mengakses datamu tanpa perlu seizin kamu?
   e. *Support DNT (Do Not Track)*: Do Not Track (DNT) adalah HTTP header yang memungkinkan kamu untuk memberi sinyal pada website agar tidak mentracking kamu. Apakah perusahaan tersebut mematuhi kebijakan ini?

** Trackography adalah sebuah proyek dari Tactical Tech yang bertujuan untuk meningkatkan transparansi tentang industri data online dengan menggambarkan siapa yang melacak kita ketika kita menjelajahi internet.*

Bab 4:

Internet Pasca-Snowden (Pengawasan Digital)

Pada 1996, John Perry Barlow, seorang penyair dan salah satu pendiri Electronic Frontier Foundation (organisasi non-profit untuk memperjuangkan hak-hak digital), mendeklarasikan kemerdekaan dunia maya. Proklamasi tersebut ditujukan kepada pihak pemerintah dunia industrial dan mengagungkan kebebasan serta kemandirian yang ditawarkan oleh dunia maya. Di dalam dunia maya, pemerintah tidak punya kuasa dan andil untuk mengatur penduduknya. Keberadaan dunia maya, menurut Barlow, menjanjikan dunia yang lebih adil dan manusiawi, berbeda dengan dunia yang dihasilkan dari pemerintahan. Sekitar awal 1990-an, internet tidak lagi hanya dikonsumsi oleh segelintir kalangan akademisi, peneliti atau insinyur teknologi. Kehadiran internet di tengah masyarakat umum menawarkan optimisme di segala bidang. Dunia maya memang mengubah segalanya, melahirkan dunia baru yang berbeda dengan yang pernah ada sebelumnya. Perkembangan pesat teknologi membuka arus informasi, komunikasi tanpa batas, dan bahkan dianggap mampu membawa perubahan sosial. Optimisme terhadap perubahan semakin menjadi ketika internet didaulat sebagai salah satu faktor penting dalam meruntuhkan rezim tirani di timur tengah, yang dikenal dengan istilah 'Arab Spring'. Setelah rangkaian 'Arab Spring', media massa mulai menjadikan jejaring sosial seperti Twitter dan Facebook sebagai pemicu perubahan.

Sampai akhirnya muncul seseorang warga negara Amerika bernama Edward Snowden. Ia adalah mantan pegawai badan intelijen Amerika Serikat (CIA) yang kemudian menjadi pegawai kontraktor yang disewa oleh Badan Keamanan Nasional Amerika Serikat (NSA). Pada 2013, tanpa sepengetahuan pemerintah AS, Snowden membocorkan dokumen rahasia yang membuka informasi tentang program dan rencana pengawasan global NSA. Tidak hanya pemerintah AS, informasi tersebut juga mengungkap kerja sama aliansi lima intelijen antara AS, Australia, Britania Raya, Kanada, dan Selandia Baru. Program-progam rahasia tersebut digagas guna mengintai seluruh warga negaranya dan pengguna layanan-layanan seperti Google dan Yahoo. Snowden dikenal sebagai *whistleblower* - orang 'dalam' yang membocorkan informasi penting untuk kepentingan publik. Dengan bocornya informasi pengawasan global tersebut,internet tidak lagi sama. Publik mulai dihadapkan pada kenyataan bahwa dunia maya tidak merdeka dari tangan pemerintah, sebaliknya, pemerintah cenderung bermaksud untuk mengawasi gerak-gerik warganya dengan lebih dekat. Dan keberadaan teknologi memfasilitasi niatan tersebut. Hak atas privasi, sebagai konsekuensinya, menjadi lebih penting dan mendesak dari sebelumnya.

Pengawasan Digital (Digital Surveillance)

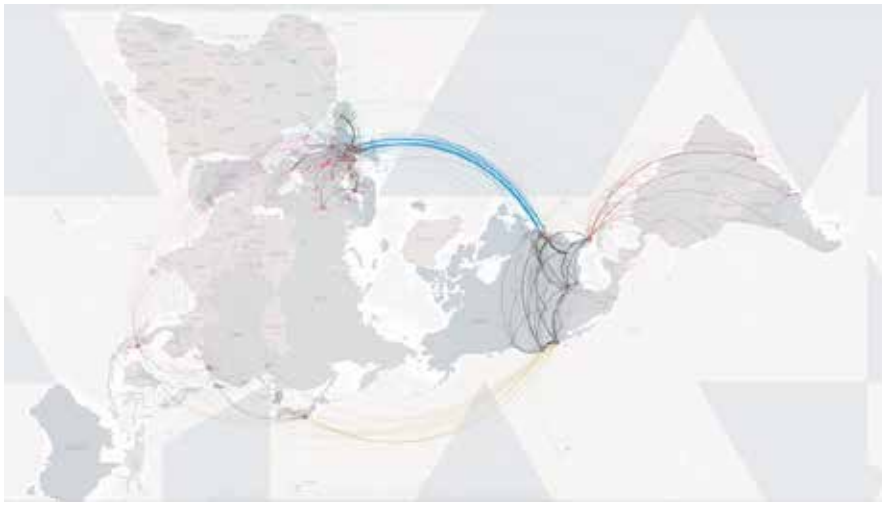
Pengawasan (Surveillance) adalah memantau aktivitas, perilaku, atau proses bertukar informasi yang dilakukan oleh masyarakat dan biasanya dilakukan untuk kepentingan seperti mempengaruhi, mengatur, mengarahkan, atau melindungi mereka (David, 2007). Dalam konteks digital, pengawasan seperti yang dilakukan dengan penyadapan, dilakukan dengan memanfaatkan teknologi digital dan jaringannya. Mengingat infrastruktur internet dan perusahaan-perusahaan penyedia layanan serta konten cenderung terpusat dan berada dalam pengaruh Amerika Serikat, tentu informasi yang dibocorkan oleh Snowden menjadi lebih masuk akal.

1. Siapa yang Mengawasi?

Ssaat ini, ada dua pihak yang mampu dan punya peluang melakukan pengawasan massal, yaitu pihak swasta dan negara (pemerintah). Pihak swasta bisa berasal dari penyedia layanan dan konten online, penyedia layanan internet atau pemilik infrastruktur internet. Motivasinya bisa karena ingin mengetahui perilaku online pelanggannya atau informasi lain yang bisa menguntungkan perusahaan tersebut. Sedangkan pihak negara biasanya diwakili oleh lembaga penegak hukum atau badan intelijen. Pengintaian ini biasanya dilakukan untuk memantau potensi tindakan kriminal, terorisme, atau bahkan untuk mengawai oposisi pemerintah (aktivis, jurnalis, dll). Seperti yang telah dibocorkan oleh Snowden, pengawasan tidak hanya berlaku di satu teritori, tetapi juga lintas teritori. Pengawasan massal secara global dilakukan oleh 'Five Eyes' (Lima Mata) yaitu meliputi: NSA milik pemerintah Amerika Serikat, Communications Security Establishment (CSE) milik pemerintah Kanada, Global Communications Headquarter milik pemerintah Britania Raya, Defense Signals Directorate (DSD) lembaga pemerintah Australia, dan pemerintah Selandia Baru dengan Government Communications Security Bureau (GCSB).

2. Bagaimana Cara Mereka Mengawasi?

Internet memiliki infrastruktur yang berbeda dengan medium komunikasi yang pernah ada sebelumnya (cth: surat, telepon). Saluran komunikasi sebelumnya memiliki infrastruktur yang terpisah satu sama lainnya. Dengan keberadaan internet, kebutuhan mengirim pesan, menelepon, dan bahkan membaca berita, semua dilakukan dalam satu infrastruktur jaringan. Semua aktivitas komunikasi tersebut dikirim menjadi suatu paket data yang ditransfer melalui jaringan. Hal ini memudahkan pengintai untuk memata-matai aktivitas komunikasi seseorang hanya dengan satu saluran. Faktanya, meskipun seseorang ingin mengirim surel dari Jakarta ke Belanda, jika pengirim dan penerima menggunakan layanan milik perusahaan Amerika Serikat, lalu linta pengiriman akan melewati infrastruktur di negara tersebut sebelum sampai ke penerima. Infrastruktur tulang punggung (*backbone*) internet juga cenderung terpusat (lihat gambar di bawah ini).



Peta Internet Global 2012

(sumber: http://global-internet-map-2012.telegeography.com)

Banyak jalan untuk mengintip apa yang sedang kita lakukan di internet. Bisa dengan menyadap melalui tulang punggung internet, kerjasama dengan pemilik kabel serat optik, dan cara lain yang mampu mengintip isi paket data dalam proses perpindahan. Cara tersebut dikenal sebagai Upstream Collection. Berdasarkan dokumen yang dibocorkan oleh Snowden, operasi pengawasan memasang perangkat keras yang berfungsi untuk mengawasi di berbagai titik pemeriksaan dalam tulang punggung internet. Selain cara tersebut, dengan teknologi seperti Deep Packet Inspection (DPI), yang mampu memeriksa lalu lintas internet secara otomatis berdasarkan kata kunci atau kode tertentu. Meskipun teknologi ini bisa digunakan untuk mencegah virus atau serangan yang bisa merusak lalu lintas, ada berbagai bukti juga bahwa DPI digunakan oleh pemerintah untuk kepentingan tertentu. Pada tahun 2013, pemerintah Malaysia yang dikuasai oleh Barisan Nasional contohnya, menggunakan DPI untuk menyadap lawan politiknya dalam masa menjelang pemilu (Wagstaff, 2013).

3. Untuk Apa Kita Diawasi?

Saat merespon kontroversi NSA, Presiden Amerika Serikat, Barack Obama, mengeluarkan pernyataan bahwa warga negara harus bisa memilih privasinya atau keamanannya. Bagaimana menurutmu?

Pada sesi-sesi sebelumnya, disimpulkan bahwa hak atas privasi merupakan salah satu hak asasi manusia. Oleh karena itu tugas negara adalah melindungi serta menjamin hak warganya. Pihak pemerintah sering menggunakan keamanan sebagai dalih untuk mendasari tindakan-tindakan yang melanggar hak atas privasi. Faktor-faktor seperti terorisme, kejahatan di dunia maya, atau ancaman bagi negara mendorong program pengawasan massal. Sedangkan pihak swasta, memanfaatkan pengawasan untuk keuntungan perusahaannya, misalnya untuk mengalahkan kompetitornya lewat jalur belakang atau membatasi pilihan pengguna internet. Di sesi sebelumnya kita juga sudah membahas pentingnya kontrol pribadi terhadap segala informasi dan data yang kita punya. Dengan adanya pengawasan massal, kontrol tersebut berpindah tangan ke perusahaan dan negara. Keduanya ingin membangun profil pribadi dari serpihan data yang mereka kumpulkan, profil tersebut akan menjadi sasaran dalam mencapai kepentingan mereka.

Negara memang wajib menjamin keamanan warganya, tapi kalau negara justru membatasi dan bisa membahayakan warganya, tentu lain cerita. Seperti pemerintah Republik Rakyat Cina yang selalu mengawasi seluruh warganya, membatasi ekspresi warga dan berusaha menyingkirkan lawan politiknya. Keberadaan program seperti ini menjadikan kekuasaan semakin terpusat dan melakukan tindakan semena-mena. Konsekuensinya, memudahkan pemerintah untuk menjadi otoriter dan melanggar hak asasi manusia warganya. Privasi dan kebebasan berekspresi saling berkaitan, jika ada seorang jurnalis yang mengungkap kasus korupsi diawasi terus-menerus oleh lawannya, besar kemungkinan dirinya dan bahkan keluarganya berada dalam bahaya.

Dengan kenyataan bahwa internet bukan dunia impian yang merdeka dan bebas campur tangan dari pemerintah dan pihak lainnya, masihkah kamu berpendapat bahwa tidak ada yang perlu ditakuti jika tidak ada yang kamu sembunyikan?

Patut dicatat, bahwa privasi bukan semata soal rahasia atau menyembunyikan informasi tertentu. Privasi adalah tentang otonomi, kuasa, dan kontrol yang memungkinkan kita untuk memutuskan bagaimana kita ingin memperlihatkan diri kita (myshadow.org) . Pelanggaran privasi bahkan bisa berdampak pada risiko lanjutan seperti kehilangan kesempatan pekerjaan, hanya karena satu kesalahan yang pernah kamu lakukan di masa lampau muncul di internet, memberi peluang untuk *cyber-bullying*, dituduh atas sesuatu yang belum tentu kamu lakukan, serta risiko lainnya.

Studi Kasus

Baca artikel di bawah, kemudian diskusikan pertanyaan berikut:

1. Bagaimana pendapatmu terhadap temuan Citizen Lab tersebut?
2. Apakah kamu mengizinkan negara atau pihak perusahaan melakukan tindakan tersebut?
3. Dengan adanya informasi seperti ini, bagaimana tingkat kepercayaanmu terhadap negara dan perusahaan penyedia layanan internet (*provider*) yang kamu gunakan?

"Hasil investigasi media Australia membeberkan laporan bahwa pemerintah Indonesia diduga menggunakan aplikasi pengintai (*spyware*) yang diletakkan di pusat data (*data center)* di Sidney sebagai bagian dari program "memata-matai" warga. Media *Australian Broadcasting Corporation (ABC)* pada Selasa, (26/1/2016) memberitakan bahwa pemerintah Indonesia menggunakan sebuah aplikasi pengintai bernama FinFisher sebagai alat untuk mengumpulkan informasi dari sejumlah orang.

Seorang peneliti bernama Bill Marzcak dari Citizen Lab Universitas Toronto mengatakan informasi yang berhasil dikumpulkan oleh FinFisher akan diarahkan ke pusat data Australia bernama Global Switch, sebelum dikirim ke Indonesia.

Menurutnya, *server proxy* dalam pusat data "Global Switch" di Ultimo, Sydney, digunakan untuk mengaburkan pengguna sebenarnya dari aplikasi pengumpan tersebut, dalam hal ini adalah lembaga pemerintahan Indonesia. Hasil penyelidikan ABC mengungkapkan bahwa Indonesia merupakan salah satu pelanggan terbesar FinFisher, dan salah satu lembaga yang menggunakannya adalah Lembaga Sandi Negara.

Namun masih belum jelas lembaga pemerintah Indonesia mana yang harus bertanggung jawab terhadap penggunaan aplikasi pengintai tersebut di Global Switch. Baik pihak ASIO, Global Switch, dan Lembaga Sandi Negara belum mau membuka suara atas temuan ini.

FinFisher dibuat oleh perusahaan Inggris bernama Gamma International dan dipasarkan sebagai alat yang sangat canggih yang dapat mengakses komputer para tersangka kriminal dan terorisme secara diam-diam. Program FinFisher digambarkan oleh sang distributor, Gamma International UK Ltd., sebagai alat agar pemerintah dapat melakukan pengintaian jarak jauh.

Masalah terdeteksinya FinFisher yang dilakukan oleh lembaga di Indonesia sebenarnya isu lama yang sempat mencuat pada 2013. Tahun itu, *Tempo.co* mengutip Mashashi Crete-Nishihata peneliti lain dari Lembaga Citizen Lab yang menyebutkan bahwa lembaga yang dipimpinnya mendeteksi adanya pengoperasian aplikasi pengintai FinFisher di beberapa negara, termasuk Indonesia.

Dalam laporannya yang dirilis Maret 2013, Citizen Lab menemukan delapan *server* FinFisher di Indonesia, pada tiga penyedia jasa Internet (*Internet service provider* (ISP)) yang berbeda yaitu PT Telkom, PT Matrixnet Global dan Biznet.

Namun pihak Telkom dan Biznet langsung membantah hasil laporan tersebut. "Dari Biznet tidak ada policy seperti itu. Kita sedang cek IP address itu punya siapa," kata Presiden Direktur Biznet Network Adi Kusma kepada *Kompas.com*.

Hal senada juga diungkapkan pihak Telkom. "Bahwa Telkom tidak mempunyai server untuk melakukan *monitoring* atau memata-matai pelanggan," ujar Slamet Riyadi, yang saat itu menjabat Head of Corporate Communication and Affair Telkom.

Selain Indonesia, Citizen Lab mencatat, aplikasi pengumpan FinFisher terdeteksi di 25 negara, yaitu Australia, Bahrain, Banglades, Brunei, Kanada, Republik Cek, Estonia, Etiopia, Jerman, India, Jepang, Latvia, Malaysia, Meksiko, Mongolia, Belanda, Qatar, Serbia, Singapura, Turkmenistan, Uni Emirat Arab, Inggris, Amerika Serikat, dan Vietnam.

Menurut lembaga Privacy International, FinFisher -baru-baru ini digunakan oleh pemerintah Uganda untuk mengumpulkan "rentetan informasi" tentang lawan-lawan politik dan "mengontrol media" seperti yang diberitakan *RadioAustralia*, Selasa (27/1/2016).

Di Bahrain, pemerintah setempat dituduh menggunakan teknologi ini untuk mengintai tiga aktivis muda sementara mereka tinggal di Inggris. Ketiga aktivis itu mengatakan, sebagai hasil dari pengintaian tersebut, mereka dikejar tanpa henti dan disiksa di tangan otoritas Bahrain.

(sumber: https://beritagar.id/artikel/sains-tekno/isu-quotspywarequot-finfisher-di-indonesia-kembali-mencuat)

Bab 5:

Saatnya Kamu Pegang Kendali! (Langkah Dasar Menjaga Privasi Online)

Memegang Kendali Data Pribadi

Setelah pelacakan digital, Snowden, pengawasan digital, dan semua permasalahan dan risiko yang terkait dengan privasi di sesi-sesi sebelumnya, pertanyaannya kemudian apakah privasi adalah sebuah kemustahilan di era digital ini?

Seperti yang telah dikemukakan di sesi sebelumnya, kunci dari privasi adalah kontrol terhadap data pribadimu. Kamulah yang menentukan informasi mana yang bisa diketahui orang lain dan mana yang tidak. Semakin besar kendali yang kamu pegang terhadap data-data pribadimu, semakin kamu bisa menjamin privasi dirimu sendiri. Meskipun internet seolah memfasilitasi pengawasan digital atau melacak jejak digitalmu, perlu diketahui bahwa internet juga diciptakan dengan landasan keterbukaan dan keamanan. Praktik seperti penyadapan dalam jaringan atau menjadikan internet sebaga sesuatu yang tertutup adalah tindakan yang mencederai landasan tersebut.

Menjaga privasi dimulai dari diri sendiri. Menjadi lebih sensitif terhadap perangkat dan layanan yang kamu gunakan ketika mengakses internet adalah sebuah kebutuhan. Berikut beberapa langkah sederhana untuk mulai mencoba memegang kendali dan membiasakan diri untuk mengubah kebiasaan sehari-hari. Sehingga kita tidak menempatkan diri kita dan orang-orang di sekitar kita (yang sering berkomunikasi dengan kita) dalam posisi yang rentan untuk diawasi atau dimanfaatkan pihak yang tidak bertanggung jawab.

Sebelum menjalankan langkah-langkah di sesi ini, patut diingat bahwa:

- Seperti diungkapkan oleh lembaga Electronic Frontiers Foundation, keamanan bukan dicapai dengan membeli, melainkan dibangun dalam sebuah proses. Keamanan dan kendali bukan tentang perangkat atau *gadget* apa yang paling mahal atau paling canggih.
- Ponsel adalah perangkat paling umum di Indonesia untuk mengakses internet. Pada kenyatannya, ponsel pada dasarnya memang tidak aman. Dalam artian bahwa ponsel memang didesain untuk menginformasikan lokasi kita. Pertukaran informasi atau penyimpanan informasi di ponsel memang rentan terhadap risiko penyadapan. (untuk informasi lebih lanjut tentang ini kamu bisa menyimak video ini: https://www.youtube.com/watch?v=ucRWyGKBVzo)
- Adanya fitur seperti Screencapture di ponsel atau desktop juga mengakibatkan risiko tersendiri. Misalnya, meskipun akun instagram sudah dikunci agar *private,* foto yang kamu unggah tetap bisa digandakan oleh orang-orang yang mengikutimu. Begitu juga dengan Whatsapp yang sudah memiliki fitur enkripsi *end-to-end* (dari pengirim ke penerima), tetap ada risiko pesanmu direkam dan disebarluaskan dalam bentuk foto hasil Screencapture.
- Ponsel pribadimu adalah propertimu, berhati-hatilah terhadap orang yang ingin meminjam atau melihat ponselmu karena ini modus yang kerap dilakukan orang yang berniat negatif (cth: menyadap).
- Kamu perlu mengevaluasi seberapa rentan kamu terhadap risiko keamanan. Pikirkan kembali saluran komunikasi apa yang kamu gunakan (cth: e-mail, surat, telepon, skype, dll), cek lagi bagaimana dan di mana lokasi menyimpan data-data pribadimu terutama untuk informasi yang sensitif (cth: di komputer, hard disk, cloud, dll).

- Pernah melihat pemberitahuan di satu situs yang menyatakan bahwa situs tersebut menggunakan 'cookie'. Cookie adalah serangkaian teks yang disimpan pada komputer kamu oleh situs yang sedang kamu kunjungi. Biasanya Cookie menyimpan pengaturan atau preferensi kamu untuk suatu situs tertentu (cth: bahasa yang dipilih atau lokasi (negara)). Ketika mengunjungi situs itu lagi, situs tersebut sudah menyimpan informasi kamu sebelumnya. Kamu bisa memilih untuk mengaktifkan atau menonaktifkan fungsi Cookie.

Langkah dasar untuk menjaga privasi dan keamanan:

1. Selalu cek *update* dan jaga 'kebersihan' perangkatmu

Sebisa mungkin *update* terus sistem operasi dan versi terbaru dari aplikasi dan perangkat lunak yang kamu gunakan. Versi terbaru memperbaiki kelemahan di versi sebelumnya, termasuk fungsi yang menjaga keamanan. Selain *update*, kamu juga perlu rajin membersihkan perangkatmu dari virus. Kolektif teknologi, Tactical Tech menganjurkan perangkat lunak antivirus yang gratis atau yang Free/Open Source, agar kita tidak terjebak dengan lisensi yang harus terus diperbaharui. Salah satu rekomendasinya adalah Avast!. Perangkat lunak ini juga tersedia untuk sistem operasi Mac OS dan Android.

2. Gunakan kata sandi (*password*) yang unik dan solid

Jangan menggunakan tanggal lahir atau informasi personal yang standar untuk dijadikan kata sandi. Bayangkan satu kalimat atau hal paling aneh sekalipun yang diketik dengan kombinasi alfabet, angka, huruf kapital dan huruf kecil. Pilih kata sandi yang panjang dan rumit. Masih ingat bahasa yang dianggap 4L4y ? Nah justru cara ini bisa melindungi kamu dari pembobol *password.* Misalnya daripada memilih kata sandi seperti 'Iloveyou' sebaiknya modifikasi jadi '1 L0v3 Y0u 4 Th0u54Nd t1M35'. Gunakan kata sandi yang seunik mungkin dan terus perbaharui minimal tiga bulan sekali. Semakin unik, teka-teki kata sandi kamu semakin sulit dipecahkan oleh peretas.

3. Mengakses internet dengan aman, selalu gunakan HTTPS

Saat menggunakan browser, perhatikan ketika kamu menulis domain atau mau mengunjungi suatu website, ada HTTP atau HTTPS sebelum nama domainnya (cth: https://duckduckgo.com). Selalu pilih HTTPS, karena format ini mengenkripsi koneksi antara browser kamu dan situs yang dituju, sehingga menjadi lebih sulit untuk diintip oleh pihak yang 'kepo' dengan aktivitas online kamu. Untuk memastikan browser kamu menggunakan HTTPS, kamu

bisa memasang tambahan (*adds-on*) seperti HTTPS Everywhere di browser laptop atau bahkan ponsel pintarmu.

4. Menjadi anonim dengan menggunakan TOR Browser

Untuk menghindari pihak-pihak pengintai jejak digital, kita harus bermain petak umpet. Di negara-negara otoriter yang masih membatasi akses warganya terhadap informasi dan memantau ruang gerak para oposisi pemerintah, petak umpet adalah sebuah keharusan. Misalnya seorang jurnalis yang ingin mengungkap praktik korupsi para penguasa dan usahanya dianggap berbahaya bagi para koruptor, ia harus bermain petak umpet di dunia nyata dan dunia maya. TOR Browser menyembunyikan keberadaan (lokasi) dan aktivitas *browsing*-mu dari para penyedia layanan internet. TOR Browser membuatmu jadi anonim dalam menjelajah online, konsekuensinya, kehadiranmu bisa saja ditandai dengan bendera merah (*red flag*).

5. Mengetahui dan memantau di mana saja kamu menyimpan datamu

Terkadang kita suka asal menyimpan dan mengunggah data tanpa mengingat dan menyadari di mana data tersebut disimpan. Mulai sekarang, kamu bisa mulai mendaftar dan mengingat di mana saja kamu menyimpan data pribadimu, seperti foto-foto, informasi sensitif pribadi, informasi kesehatan, dsb. Setelah memetakan di mana datamu, pilih tempat penyimpanan yang aman dari gangguan dan ancaman pihak yang tidak diinginkan. Sekalipun datamu disimpan di *hard drive* eksternal, simpan di tempat yang aman dan kunci dengan kata sandi (biasanya disediakan sesuai merk *hard drive*-nya).

Langkah-langkah untuk meningkatkan kendali

1. Mengubah pengaturan awal di semua akun yang kamu punya (cth: Gmail, Facebook, Twitter, Linkedin, Tumblr, Snapchat, Instagram, dll.)

Cek semua akun di berbagai layanan online dan jejaring sosial (minimal yang sering kamu gunakan). Pengaturan awal (*default*) biasanya didesain agar kamu membagi informasi sebanyak-banyaknya (cth: lokasi, foto, dan data lainnya). Mulai cek pengaturan privasi di layanan online dan jejaring sosial tersebut. Pilih informasi apa yang mau kamu bagi dan tidak.

2. Pasang ekstensi atau *add-ons* untuk menghadang para '*tracker*' atau pelacak jejak digitalmu

Agar aktivitas di situs yang kamu kunjungi menjadi lebih privat, luangkan sedikit waktu untuk memasang ekstensi di *browser* yang kamu gunakan. Beberapa ekstensi juga menginformasikan berapa dan siapa saja yang melacak jejakmu. Keuntungan lainnya adalah menghadang iklan-iklan yang mengganggu aktivitas jelajah online. Berikut beberapa pilihan ekstensi yang bisa diunduh dan dipasang sesuai *browser* yang kamu gunakan : Ghostery, Privacy Badger, dan Disconnect.

3. Gunakan sarana dan layanan alternatif

Jika kamu ingin mengurangi ketergantungan dengan layanan yang disediakan oleh perusahaan-perusahaan besar yang memanfaatkan datamu atau mengurangi peluang untuk diintai melalui perusahaan tersebut, solusi paling konkrit adalah menggunakan layanan alternatif yang Free dan/atau Open Source. Layanan-layanan ini mengutamakan privasi, gratis atau kalaupun berbayar tidak mahal, dan tidak menjual data pribadimu. Berikut beberapa layanan alternatif pengganti layanan yang mungkin sering kamu gunakan:

a. Surel/e-mail selain Gmail, Hotmail, atau Yahoo: Riseup, Espiv, dan Posteo.
b. Pesan instan selain Whatsapp, Facebook Messenger, LINE, Snapchat, dll.: Signal, Surespot, Chatsecure.
c. Mesin pencari selain Google dan Yahoo: DuckDuckGo, SearX, StartPage
d. Browser selain Chrome dan Safari: Firefox, TOR Browser
e. Dokumen kolaboratif selain Google Drive: Etherpad, Riseup Pad
f. *Video Conference* selain Google Hangout: Jitsi
g. Peta online selain Google Maps: OpenStreetMap

4. Evaluasi segala usahamu, terus terapakan langkah dasar untuk menjaga privasi dan ajak teman-temanmu!

Upaya untuk menjaga privasi juga menantang kamu untuk keluar dari zona nyaman yang diciptakan oleh pihak-pihak yang rentang mengeksploitasi informasi pribadimu dan kegiatan online yang kamu lakukan. Cek secara berkala apakah upaya yang kamu lakukan sudah cukup efektif dan temukan sarana dan cara paling sesuai dengan kebutuhanmu. Terus berusaha untuk

menerapkan langkah-langkah paling mendasar seperti di atas. Kunci dari keamanan data pribadimu adalah kesadaranmu dalam mengendalikan informasi tersebut.

Perlu diingat juga bahwa privasi, seperti di sesi paling awal, bukan hanya soal diri kamu sendiri, tetapi juga orang-orang terdekatmu. Enkripsi komunikasi harus dilakukan dari ujung ke ujung, dari pengirim ke penerima, jadi ajak orang-orang terdekatmu untuk mengadopsi langkah-langkah di atas agar bisa saling melindungi informasi pribadi.

Sekarang, sudah siap untuk keluar dari zona nyamanmu yang tidak aman?

Eksperimen (Tugas)
Perbandingan Mesin Pencari

1. Buka dua tab di *browser* (Firefox, Opera, Chrome, Safari, dll.) komputermu
2. Untuk Tab ke-1 masuk ke https://google.com
3. Untuk Tab ke-2 masuk ke https://duckduckgo.com
4. Ketik kata/kalimat kunci untuk pencarian yang kamu inginkan (cth.: Privasi, Internet, dll.)
5. Lihat hasil dari masing-masing mesin pencari
6. Jawab pertanyaan berikut:
    a. Berapa banyak hasil pencarian yang ada di tab 1 dan tab 2?
    b. Apa dan bagaimana perbedaan hasil pencariannya (minimal untuk 15 hasil pencariaan pertama) ?
    c. Menurut kamu, mengapa hasil pencarian kedua mesin pencari tersebut berbeda?
    d. Mesin pencari di tab mana yang membuatmu merasa lebih aman?
    e. Apakah kamu tertarik menggunakan layanan mesin pencari alternatif? Jelaskan alasannya!


kemudi