

SADARCAH KITA, KALAU KITA SEDANG DIAWASI SEKARANG



■ OLEH **ANDI WIRA ALAMSYAH**
KEPALA SUB BAGIAN KETATAUSAHAAN AKN VI

Kita telah memasuki era baru dalam sejarah kapitalisme di mana pengawasan dan bisnis berjalan beriringan, di mana data adalah komoditas ekonomi yang paling berharga. Ekonomi data telah mengubah warga menjadi produk.

Setiap saat, pemerintah dan perusahaan memata-matai kita. Mereka melakukannya tanpa meminta izin dari kita ataupun tanpa memberitahu kita terlebih dahulu. Mereka mengumpulkan semuanya, seperti mengumpulkan informasi lokasi kita, preferensi seksual, masalah kesehatan, keyakinan politik, kapasitas kognitif, dan banyak lagi. Mereka ingin tahu segalanya tentang kita, bagaimana kita berpikir, dan bahkan di mana kita sakit.

Karena informasi ini sangat berharga, membuat kepada siapapun pemegang informasi tersebut memiliki kekuatan untuk memberikan pengaruh atas hidup kita. Informasi ini dapat mereka gunakan untuk membujuk atau memengaruhi kita untuk membelanjakan uang atau mendorong kita untuk memilih preferensi kandidat politik tertentu. Dan lebih buruknya lagi, hal ini terjadi di masa otonomi dan demokrasi saat ini.

Kita mungkin sudah sadar bahwa kita sedang dimata-matai. Pernahkan kita merasa bahwa ada suatu masa kita sedang membicarakan sesuatu yang sangat spesifik suatu hari – katakanlah, liburan ke Bali – dan kemudian disajikan iklan hotel yang berada di Bali ataupun paket tawaran wisata ke Bali tak lama setelah itu.

Atas kejadian tersebut, apakah kita menyadari seberapa dalam pelanggaran privasi itu? Mari sejenak kita cari tahu dengan menjalani hari-hari biasa di bawah pengawasan perusahaan atau pemerintah.

Apa hal pertama yang kita lakukan ketika bangun di pagi hari? memeriksa telepon kita, *kan*? Saat menghidupkan ponsel, kita memberi tahu

sejumlah institusi, termasuk produsen ponsel, penyedia layanan, dan semua perusahaan yang aplikasinya telah kita unduh, bahwa kita sekarang sudah bangun. Mereka juga tahu di mana, dan dengan siapa kita bangun.

Jika memakai jam tangan pintar di malam hari, kita sebenarnya diawasi bahkan sebelum kita bangun. Arloji melacak pergerakan dan detak jantung kita saat tidur, serta aktivitas seksual apa pun yang mungkin kita lakukan.

Lebih lanjut, katakanlah setelah bangun, kita suka sarapan di depan TV. Jika memiliki *smart TV*, maka itu mengumpulkan data tentang kebiasaan menonton kita, dan meneruskannya ke produsen dan pihak ketiga yang tertarik lainnya. Para peneliti menemukan bahwa satu TV Samsung telah berkomunikasi dengan lebih dari 700 alamat internet setelah dinyalakan hanya selama 15 menit. Dan itu bukan hanya TV kita. Hampir semua hal yang terhubung ke internet mengumpulkan data tentang kita. Konsol *game*, *e-book*, dan alat elektronik lainnya yang berhubungan dengan internet adalah agen perusahaan di rumah sendiri.

Setelah rutinitas pagi selesai, kita masuk ke mobil untuk pergi bekerja. Dalam perjalanan – tidak ada kejutan di sini – mobil sibuk mengumpulkan data. Mobil melacak segala sesuatu mulai dari tempat yang kita kunjungi, berat badan, gerakan mata, dan bahkan jenis musik yang ingin kita dengarkan.

Setelah tiba di tempat kerja, kita *log on* ke komputer dan memeriksa *email*. Kita mungkin tidak berpikir dua kali untuk membuka *email*, tetapi tahukah kita bahwa sekitar 40 persen di antaranya berisi pelacak? Dengan membuka *email*, kita

mengizinkan pihak ketiga untuk mengidentifikasi dan melacak aktivitas kita di internet. Sepulang dari kantor kita bertemu dengan teman dalam suatu *café* yang meminta kita melakukan *scanning barcode* sebelum masuk *café* tersebut, hal ini juga menunjukkan kita sedang apa, bersama siapa, dan berada di mana. Artinya pengawasan di mana-mana telah menjadi fakta kehidupan abad kedua puluh satu. Dan hampir tidak mungkin untuk dihindari.

Mungkin kita pernah mendengar cerita tentang Alexa Amazon yang merekam percakapan pribadi orang-orang dan mengirimkannya ke orang-orang secara acak di daftar kontak mereka. Alexa Amazon menggunakan rekaman suara untuk melatih dan meningkatkan asisten suara. Klip audio Alexa juga digunakan untuk mempersonalisasi pengalaman kita dan membuatnya lebih akurat dan bermakna. Namun, di sisi privasi, ada banyak hal yang menakutkan. Hal ini karena karyawan Amazon dan kontraktor pihak ketiga dapat mendengarkan rekaman suara Echo kita. Selama bertahun-tahun, asisten suara populer seperti Siri Apple, Asisten Google, dan Amazon Alexa telah meningkat secara signifikan. Dan semua ini berkat pelatihan algoritme menggunakan banyak data suara dari pengguna seperti kita.

Kondisi tersebut adalah beberapa contoh bahwa perusahaan melakukan pengawasan terhadap kehidupan kita, dan itu cukup meresahkan. Lebih lanjut Pada tanggal 15 Mei 2021 lalu, banyak pengguna Whatsapp menjadi khawatir dengan kebijakan barunya, yaitu mengarah pada kebijakan integrasi data pengguna, seperti nomor telepon, layanan yang terkait dengan informasi, lokasi, dan juga data transaksi dengan Facebook. Akibatnya, jutaan pengguna beralih ke aplikasi lain. Atas isu tersebut Whatsapp melakukan klarifikasi dan menyatakan bahwa kebijakan yang baru tidak akan memasukkan data percakapan dan informasi pengguna. Whatsapp juga menyatakan bahwa mereka menjamin kebijakan privasi pengguna. Mereka akan melindungi pesan-pesan

di dalam platform. Namun pengumuman ini tidak menghentikan eksodus para penggunanya.

Aktivitas kita ini sebenarnya hal yang biasa saja sebelum abad 21, bahkan hingga akhir 1990-an, TV tetaplah TV, mobil tetaplah mobil. Alat-alat tersebut tidak tertarik pada kita. Mereka tidak mendengarkan percakapan atau melacak gerakan kita. Pada 1990-an, perangkat kita masih melayani kita, bukan sebaliknya.

Namun memasuki ekonomi data baru pada abad kedua puluh satu, ekonomi pengawasan mengejutkan kebanyakan orang. Seolah-olah kita semua bangun pada suatu pagi dengan kenyataan baru yang lebih suram.

Jadi, bagaimana kita masuk ke kondisi ini? Nah, pemain kunci dalam cerita ini adalah Google.

Sebelum Google naik ke tampuk kekuasaan di awal 2000-an, data pribadi belum memiliki nilai komersial. Perusahaan memang memiliki akses ke beberapa data pribadi penggunanya karena data adalah produk sampingan dari aktivitas digital – atau pembuangan data. Tapi itu tidak untuk digunakan atau hanya digunakan untuk meningkatkan layanan mereka.

Google mengubah itu. Pada tahun 2000, Google menemukan bahwa pencarian yang dilakukan penggunanya dapat digunakan untuk menjual iklan bertarget. Untuk pertama kalinya, sebuah perusahaan mulai menggunakan data pribadi untuk membangun profil yang tepat pada pengguna individu dan menjual informasi ini kepada pihak ketiga.

Ternyata hal ini menjadi model bisnis yang luar biasa menguntungkan. Atas bisnis ini Google memperoleh pendapatan sebesar 19 juta dolar pada tahun 2000, pada tahun 2004, perusahaan itu meraup 3,2 miliar dolar atau mengalami peningkatan laba 3.590 persen hanya dalam empat tahun. Google telah belajar bagaimana mengubah data *exhaust* menjadi emas dan lebih lanjut perusahaan lainnya dengan cepat mengikutinya. Warisan model bisnis Google telah menentukan perkembangan internet.



Memasuki ekonomi data baru pada abad kedua puluh satu, ekonomi pengawasan mengejutkan kebanyakan orang. Seolah-olah kita semua bangun pada suatu pagi dengan kenyataan baru yang lebih suram.

Dan bukan lagi hanya dunia *online* yang diuntungkan – industri non-digital secara tradisional semakin mengadopsi model bisnis ini. Oleh karena itu, setiap perusahaan mengeluarkan versi pintar dari perangkat mereka. Nike dan Under Armour, misalnya, juga merilis sepatu pintar pertama mereka, mungkin agar mereka bisa masuk ke dalam permainan data.

Inilah yang dimaksud dengan kapitalisme pengawasan. Kita telah memasuki era baru dalam sejarah kapitalisme di mana pengawasan dan bisnis berjalan beriringan, di mana data adalah komoditas ekonomi yang paling berharga. Ekonomi data telah mengubah warga menjadi produk.

Tapi, kapitalisme pengawasan merugikan privasi kita. Dan itu adalah harga yang tidak harus dibayar oleh individu atau masyarakat. Pihak yang mendapatkan informasi pribadi, memberikan kekuasaan kepada mereka atas kita. Saat kita membagikan informasi pribadi dengan orang yang kita cintai, kita memercayai mereka untuk hanya menggunakan informasi ini dengan cara yang menguntungkan kita. Misalnya, seorang teman mungkin menggunakan pengetahuannya tentang selera dan minat kita untuk merekomendasikan sebuah buku. Namun sebagian besar pihak ketiga tidak memiliki kepentingan itu terhadap kita. Mereka tidak mengumpulkan data untuk menguntungkan kita.

Mereka menggunakan data tersebut untuk memengaruhi, mendiskriminasi, dan untuk mengambil uang dari kita. Penggunaan data pribadi yang paling terdokumentasi dengan baik, seperti yang telah penulis sebutkan, adalah iklan bertarget. Pihak ketiga menggunakan pengetahuan yang sangat spesifik dan sangat sensitif tentang kita untuk menampilkan iklan yang disesuaikan di seluruh internet, di aplikasi, dan di umpan media sosial kita. Iklan ini sering dirancang untuk menargetkan kita secara khusus di tempat yang menyakitkan, dan hal tersebut memiliki dampak yang signifikan pada hidup kita. Misalnya, beberapa orang melihat iklan pengacara perceraian karena perangkat mereka tahu bahwa mereka bertengkar dengan pasangannya dan menghabiskan lebih sedikit waktu bersama. Contoh lain, bahwa terdapat juga konten yang tidak dirancang untuk menjual apa pun kepada kita, melainkan untuk memengaruhi pilihan politik dan perilaku memilih kita. Inilah yang terjadi pada pemilu Amerika Serikat Tahun 2016.

Cambridge Analytica menggunakan data pribadi jutaan pengguna Facebook untuk mengo-

barkan perang propaganda *online* guna memengaruhi hasil pemilu demi kliennya – Donald Trump. Data pribadi memungkinkan Cambridge Analytica untuk mengidentifikasi orang-orang yang disebutnya sebagai “dapat dibujuk” dan kemudian secara khusus menargetkan mereka dengan propaganda khusus dan berita palsu.

Perusahaan lain menggunakan data pribadi kita, bukan untuk memengaruhi, tetapi untuk mendiskriminasi kita. Kita mungkin tidak menyadari hal ini, tetapi perusahaan pemeringkat konsumen menyimpan skor rahasia berdasarkan data kita. Skor ini digunakan oleh semua jenis perusahaan untuk menentukan hal-hal tertentu, seperti aplikasi transportasi Go-Jek menyimpan jejak perjalanan dan kebiasaan pemesanan makanan kita. Yang nantinya akan diperingkat, dan diberikan pelayanan sesuai dengan peringkat kita.



Pihak ketiga menggunakan pengetahuan yang sangat spesifik dan sangat sensitif tentang kita untuk menampilkan iklan yang disesuaikan di seluruh internet, di aplikasi, dan di umpan media sosial kita.

Ketimpangan adalah inti dari ekonomi data. Melalui data kita, kita ditargetkan dan diperlakukan secara berbeda. Kita harus peduli dengan privasi kita karena kurangnya privasi menurunkan kebebasan, kesetaraan, dan demokrasi kita sendiri.

Pengaturan tentang privasi data di negara kita harus segera dilakukan, penulis mengibaratkan data kita sama dengan asbes, asbes adalah zat yang berguna, tahan lama, dapat ditambang dengan murah, dan tahan terhadap api, itulah sebabnya asbes pernah digunakan di mana-mana dalam konstruksi. Namun terdapat masalah, asbes memiliki kekurangan yang cukup besar yaitu mematikan bagi manusia karena serat asbes yang terhirup dapat memperburuk jaringan paru-paru yang memicu luka.

Data pribadi adalah asbes dunia digital. Data kita dapat ditambang dengan murah, dan juga sangat berguna untuk memprediksi dan meme-

ngaruhi perilaku manusia. Tapi seperti asbes, data pribadi adalah komoditas beracun. Ketika bocor ke dunia, itu dapat merusak kehidupan, menghancurkan bisnis, dan mengancam keselamatan publik.

Saat ini, bisnis tidak memiliki banyak insentif untuk berinvestasi dalam menjaga keamanan data penggunanya. Keamanan siber bisa mahal, dan ketika ada kebocoran data, biasanya pengunalah yang paling dirugikan.

Mungkin kita pernah mendengar tentang kebocoran data besar-besaran pada tahun 2015 dari situs kencan Ashley Madison (<https://www.cnnindonesia.com/teknologi/20150825133725-185-74342/anggota-ashley-madison-bunuh-diri-hingga-gugat-rp-10-t>), aplikasi ini merupakan layanan yang membantu orang yang sudah menikah berselingkuh. Situs ini berhasil diretas, dan peretasnya memutuskan untuk menghukum penggunanya dengan mengumumkan datanya ke publik, di mana saat itu terdapat lebih dari 30 juta akun. Hal ini mengakibatkan banyak pernikahan yang hancur, keluarga yang hancur, dan beberapa pengguna layanan bahkan mengambil nyawa mereka sendiri. Dan seperti kita lihat sekarang, perusahaan itu relatif tidak terkena dampaknya, karena *AshleyMadison.com* masih beroperasi sampai sekarang.

Kita mungkin tidak memiliki rahasia gelap seperti perselingkuhan atau kegiatan kriminal. Jadi kita aman dari kebocoran data, apakah demikian? Yah, tidak. Segala macam data tentang kita bisa sangat merusak hidup kita jika jatuh ke tangan yang salah. Seorang penjahat dengan rincian bank kita bisa membersihkan rekening kita. Dengan *scan* paspor, atau identitas kita bisa dicuri. Ujung-ujungnya, selama data pribadi kita ada, maka rentan untuk disalahgunakan. Dan dalam beberapa kasus, mengumpulkan data juga dapat digunakan untuk membunuh.

Sebagai contoh ketika Perang Dunia Kedua. Pada saat itu, Nazi menginvasi negara baru, salah satu hal pertama yang mereka lakukan adalah menjarah catatan sensus negara tersebut untuk mengidentifikasi dan menemukan orang-orang Yahudi. Di Belanda, catatan sensus termasuk agama warga, dan ini berkontribusi pada tingkat kematian tertinggi orang Yahudi di Eropa – 73 persen dibunuh. Namun di Prancis, undang-undang privasi melarang pengumpulan data keagamaan. Sehingga di sana, hanya 25 persen dari populasi Yahudi ditemukan dan dibunuh.

Privasi bukan tentang menyembunyikan kesalahan, ini tentang melindungi diri kita dari kesalahan orang lain. Selama data kita ada di luar sana, kita tidak pernah tahu siapa yang akan menganganya dan apa yang akan mereka lakukan dengannya.

Lebih lanjut, di dunia *offline*, jika seseorang mengikuti kita, kita akan menyebutnya *stalking*. Jika seseorang mengambil buku harian kita, disebut mengintip. Dan, jika pembawa surat kita membaca surat kita dengan cara yang sama seperti Google dan perusahaan lain membaca *email* kita, mereka akan menerima hukuman penjara.

Namun, ketika datang ke dunia *online*, perilaku ini ditoleransi dan bahkan dianggap penting untuk ekonomi internet. Mengapa hal ini menjadi standar ganda seperti itu? Alasannya adalah kekuatan Big Tech atas narasi. Faktanya adalah, perusahaan teknologi telah memenangkan perang ideologis melawan kita. Mereka meyakinkan kita bahwa privasi adalah nilai yang sudah ketinggalan zaman. Dan, mereka telah berhasil mendandani sistem pengawasan massal dengan dalih kemajuan.

Big Tech memiliki kepentingan pribadi pada orang-orang yang percaya bahwa teknologi yang dikembangkannya tidak dapat dihindari. Menolak perusahaan teknologi sama dengan menolak kemajuan itu sendiri. Logika semacam ini sangat menarik. Kita sering membayangkan bahwa teknologi berkembang pada lintasan linier dan semakin lama semakin baik. Namun cara berpikir ini mengabaikan peran sentimen publik dan regulasi pemerintah dalam mengarahkan perkembangan teknologi. Mungkin kita masih ingat Google Glass, kacamata virtual dengan kamera tersembunyi yang terpasang? Google pada dasarnya terpaksa menarik perangkat dari pasar karena fakta bahwa konsumen membencinya. Orang-orang merasa menyenamkan bahwa mereka dapat direkam tanpa sepengetahuan mereka.

Pelajaran yang dapat diambil adalah bahwa tidak ada teknologi yang tak terhindarkan. Kita memiliki kekuatan untuk menekan perusahaan agar mengembangkan teknologi yang lebih etis, dan kita juga memiliki kekuatan untuk mengatur bagaimana teknologi itu digunakan setelah dibuat. Tapi tetap saja, kita mungkin bertanya-tanya, bukankah kita perlu mengumpulkan data pribadi untuk mempromosikan inovasi teknologi etis?



Setiap jenis sistem sosial tergantung pada kerja sama orang-orang. Ketika mereka tidak lagi bekerja sama, sistem rusak. Kapitalisme pengawasan tidak berbeda. Jika kita semua mulai berperilaku seolah-olah privasi kita benar-benar penting, segalanya akan berubah.

Nah, ini adalah argumen lain dalam gudang retorika Big Tech. Menurut argumen itu, mengatur ekonomi data sama dengan menempatkan penghalang jalan di depan perkembangan teknologi. Meskipun benar bahwa perusahaan teknologi memerlukan beberapa data kita agar layanan mereka berfungsi, itu tidak berarti mereka perlu mengumpulkan segala sesuatu tentang kita dan menyimpan data itu tanpa batas. Misalnya, aplikasi yang menawarkan pembaruan *real-time* tentang lalu lintas memerlukan data lokasi kita untuk melakukannya. Tapi itu tidak berarti perlu mengumpulkan semua data di ponsel kita dan menjualnya ke pihak ketiga. Sebenarnya, privasi dan kemajuan teknologi tidak bertentangan satu sama lain. Dengan peraturan yang sesuai, perusahaan dapat menggunakan data pribadi untuk mengembangkan layanan mereka tanpa mengubah kita menjadi komoditas.

Kita perlu mengatur ekonomi data secara ketat.

Ekonomi pengawasan membuat kita lengah. Industri teknologi berkembang lebih cepat daripada yang dapat diatur oleh pemerintah. Sesuai dengan mantra Lembah Silikon, perusahaan teknologi bergerak cepat dan menghancurkan banyak hal-hal seperti kehidupan dan demokrasi.

Tetapi sekuat apa pun raksasa teknologi itu, mereka lebih rapuh daripada yang terlihat. Sebagian besar kekuatan mereka berasal dari data kita. Kita hanya perlu mengesahkan beberapa undang-undang sederhana yang melindungi hak kita atas privasi *online*, dan raksasa teknologi akan jatuh seperti susunan rumah kartu. Itulah mengapa mereka menghabiskan banyak uang untuk melobi – bukan hanya karena mereka bisa, tetapi karena mereka akan kehilangan banyak hal. Google, misalnya, membelanjakan setiap perusahaan lain yang berusaha memengaruhi Washington. Tetapi perusahaan teknologi tidak boleh diizinkan untuk membeli demokrasi kita. Kita bisa dan kita harus mengatur ekonomi data. Sudah saatnya kita berdiri dan menuntut hak kita.

Dalam hal perlindungan data pribadi, dikenal dua metode untuk melindungi suatu data pribadi, yaitu yang pertama adalah pengamanan terhadap fisik data pribadi itu sendiri dan yang kedua adalah pengaturan melalui regulasi yang menjamin privasi atas penggunaan data pribadi tersebut (Djafar Wahyudi, Sumigar Bernhard Ruben Fritz, 2016). Dalam tataran regulasi, saat ini setidaknya 107 negara telah memiliki undang-undang perlindungan data pribadi (UNCTAD, 2019), Uni Eropa sendiri memiliki General Data Protection (GDPR) yang menjalankan aturan perlindungan data pribadi, sementara Indonesia baru merancang undang-undang perlindungan data pribadi.

Menurut penulis, hal pertama yang harus kita larang adalah iklan bertarget.

Janji di balik iklan bertarget adalah bahwa pengiklan hanya perlu membayar untuk iklan yang efektif dan konsumen hanya perlu melihat iklan yang mereka minati. Secara teori, ini adalah *win-win solution*. Namun kenyataannya, iklan bertarget telah menormalkan pengawasan massal, memutarbalikkan demokrasi, dan mempolarisasi masyarakat kita dengan penyebaran berita palsu. Ironi pahitnya adalah bahwa iklan bertarget bahkan mungkin tidak berfungsi. Penelitian menunjukkan bahwa perolehan pendapatan yang diterima pengiklan dari iklan bertarget versus iklan konvensional adalah marjinal. Karena biaya lebih banyak untuk menargetkan iklan, perusahaan membuang-buang uang mereka. Yang berarti kita semua mungkin kehilangan privasi tanpa alasan sama sekali.

Hal kedua yang penulis minta adalah bahwa kita harus menuntut pemerintah kita untuk melarang perdagangan data pribadi. Kehidupan pribadi orang tidak boleh menjadi komoditas yang dapat dibagikan, dijual, dan dieksploitasi oleh perusahaan ataupun pemerintah untuk mendapatkan keuntungan. Saat ini kita hidup di dunia di mana legal bagi perusahaan untuk mengambil untung dari pengetahuan bahwa seseorang mengonsumsi obat tertentu, atau bahwa mereka adalah korban pelecehan seksual sehingga mem-

butuhkan iklan rekomendasi obat tertentu. Hal ini seharusnya tidak kita lakukan dan pemerintah harus hadir melindungi warga negaranya.

Di luar praktik bisnis yang tercela, perdagangan data adalah risiko keamanan pribadi. Memori Amy Boyer, 20 tahun dibunuh oleh penguntitnya, harus menjadi peringatan. Pembunuhnya telah membeli alamatnya dari broker data. Kita harus menuntut hak untuk mengontrol data kita. Kita harus diminta dengan jelas untuk persetujuan kita sebelum data dikumpulkan. Kita harus dapat melihat data kita dan menentangnya jika tidak akurat. Dan, harus memiliki hak untuk menghapusnya jika kita mau.

Langkah sederhana yang dapat kita ambil untuk melindungi privasi online kita.

Di kantor pusat Microsoft di Redmond, Washington, ada ruangan khusus yang didedikasikan untuk pengelolaan sistem komputasi awannya, Azure. Di dalam ruangan ini, ada dua layar besar. Satu menampilkan status sistem, dan yang lainnya menampilkan sentimen publik terhadap sistem, seperti yang diungkapkan di media sosial.

Mengapa Microsoft menampilkan sentimen publik terhadap sistem *cloud*-nya di ruangan yang sama di mana ia mengelola fungsinya? Karena kerjasama dari masyarakat sangat penting agar teknologi dapat berfungsi.

Setiap jenis sistem sosial tergantung pada kerja sama orang-orang. Ketika mereka tidak lagi bekerja sama, sistem rusak. Kapitalisme pengawasan tidak berbeda. Jika kita semua mulai berperilaku seolah-olah privasi kita benar-benar penting, segalanya akan berubah.

Untuk itu, berikut adalah beberapa tindakan nyata yang dapat kita ambil untuk melindungi privasi Kita dan menekan institusi untuk mengubah praktik mereka.

Pertama-tama, pikirkan dua kali sebelum memposting sesuatu secara *online*. Tanyakan pada diri sendiri: Apakah saya benar-benar membutuhkan ini di internet? dan, Bagaimana ini bisa digunakan untuk melawan saya? Konten yang kita posting secara *online* dan di media sosial akan tetap ada dalam catatan perusahaan ini secara permanen. Sayangnya, kita tidak dapat mengetahui bagaimana informasi tersebut akan digunakan di masa mendatang. Sebagai aturan umum, semakin sedikit kita memposting *online*, semakin baik.

Selanjutnya, coba temukan alternatif ramah privasi untuk aplikasi dan layanan yang kita gunakan. Aplikasi pemesanan yang solid dan ramah

privasi, akun *email*, *browser*, dan mesin pencari sudah ada yang berfungsi sama seperti yang dimiliki oleh Google dan Facebook. Ini tidak hanya melindungi data kita, tetapi juga mendukung pengembangan teknologi ramah privasi.

Kebiasaan baik lainnya untuk dilakukan adalah melakukan sedikit pembersihan digital dari waktu ke waktu. Itu berarti, misalnya, menghapus aplikasi di ponsel yang tidak kita gunakan lagi, menghapus dokumen dari perangkat kita yang tidak lagi relevan, dan mengubah pengaturan di akun *online* kita ke opsi paling pribadi. Semakin sedikit aplikasi yang kita miliki dan semakin sedikit data yang kita miliki, semakin tidak rentan kita jika perangkat kita pernah disusupi.

Jaga privasi kita dengan serius. Praktik privasi yang kita jalani hari ini akan berdampak pada keselamatan, kesejahteraan, dan peluang kita di masa mendatang.

Saatnya untuk berpikir hati-hati tentang masa depan seperti apa yang ingin kita jalani. Ada dua jalur yang bisa kita ikuti, yang pertama mengarah ke masyarakat pengawasan yang lebih ekstrem daripada yang kita jalani saat ini. Saat ini adalah dunia di mana setiap kata yang kita ucapkan dan setiap tindakan yang kita lakukan direkam, dianalisis, dan dibagikan kepada siapa pun yang bersedia membayarnya. Tetapi ada juga jalur lain, yang mengarah ke dunia di mana perangkat kita tidak memantau kita, di mana hanya kita yang memiliki akses ke informasi paling pribadi kita, di mana perusahaan melayani warga daripada mengeksploitasi dan mengambil keuntungan dari mereka. Pilihannya jelas. Pengawasan massal tidak sesuai dengan kebebasan, kesetaraan, dan demokrasi. Kapitalisme pengawasan harus pergi. ●

Redaksi Majalah *Warta Pemeriksa* mengharapkan kontribusi dari rekan-rekan pembaca untuk mengirimkan tulisan dengan tema pemeriksaan maupun keuangan negara/daerah.

Tulisan format doc minimal 7.000 karakter dapat dikirimkan melalui email **wartapemeriksa@bpk.go.id** dengan subjek 'Rubrik Kolom'.

Cantumkan nama lengkap, instansi/unit kerja dan nomor yang bisa dihubungi. Bagi artikel terpilih untuk dimuat akan diberikan apresiasi berupa fee menulis sebesar Rp750.000.