Judul : Dunia Tanpa Rahasia
Tanggal : Jumat, 23 September 2022
Surat Kabar : Kompas
Halaman : 7

Dunia Tanpa Rahasia

Agus Sudibyo
Dosen Akademi Televisi Indonesia, Jakarta

"Facebook mengenali kita dengan sangat baik. Facebook melacak dengan siapa kita berbicara, apa yang kita bicarakan, apa yang kita sukai, sedang di mana kita berada, dan transaksi apa yang kita lakukan. Facebook menandai wajah Anda dalam foto orang lain, bahkan dalam foto kerumunan orang. Anda ditandai di begitu banyak foto, keren sekali, kan?"

Mike Matchett dalam artikel berjudul "Facebook and Data Mining: Is Anything Private?" menyampaikan pertanyaan ini.

Setelah semuanya terhimpun, diapakan data pribadi pengguna itu? Dikirimkan kepada mereka yang mampu membelinya, tanpa terkecuali pihak yang berniat jahat, seperti terjadi pada pemilihan presiden Amerika Serikat tahun 2016.

Meski hiperbolis, deskripsi Matchett mendekati kenyataan. Ia mengingatkan kita sejauh mana perusahaan platform digital mengawasi dan menembus privasi penggunanya. Perusahaan platform digital terus mencatatkan pertumbuhan skala ekonomi yang fantastis.

Kunci sukses mereka adalah data yang ditambang dari miliaran pengguna di seluruh dunia. Data tersebut menjadi fondasi dari praktik periklanan digital, propaganda komputasional, *machine learning*, dan rekayasa kecerdasan buatan.

Di saat yang sama, para pengguna internet umumnya tak sadar data pribadi mereka terus dikeruk dan dimanfaatkan. Hingga kemudian terjadi kebocoran data pribadi, *doxing*, *bullying*, penipuan daring, dan lain-lain, seperti ramai dibicarakan di Tanah Air belakangan.

Tidak ada layanan gratis

Facebook adalah platform media sosial terbesar di dunia. Di sana, miliaran pengguna beraktualisasi diri dan berinteraksi. Meskipun Facebook mengklaim layanannya bersifat gratis, nyatanya ada harga yang mesti dibayar oleh pengguna. Pengguna harus menyerahkan informasi pribadi saat mereka menyetujui syarat dan ketentuan penggunaan layanan Facebook.

Informasi pribadi itu mencakup: umur, jenis kelamin, riwayat pekerjaan, tingkat pendidikan, tanggal lahir, minat, informasi kontak, status hubungan, lokasi geografis, merek barang yang dikonsumsi, grup musik favorit, dan lain-lain. Sering kali pengguna menyetujui syarat dan ketentuan yang ditetapkan Facebook tanpa benar-benar memahami implikasinya.

Facebook kemudian merasa berhak menambang, mengelola, dan memonetisasi data pengguna tanpa merasa khawatir dituduh memanipulasi pengguna.

Seperti diuraikan Brian M Kwong dkk dalam "Facebook Data Mining the World's Largest Focus Group" (2012), memiliki miliaran pengguna aktif di seluruh dunia, sama artinya Facebook mengendalikan sebuah kelompok terfokus (*focus group*) terbesar di dunia. Interaksi yang terjadi di dalamnya memungkinkan Facebook membangun model perilaku pengguna berskala global.

Model perilaku pengguna ini ibaratnya harta karun bagi platform digital. Dari sana lahir bentuk periklanan yang sangat akurat dalam menargetkan sasaran individu, juga propaganda komputasional yang semakin populer belakangan ini, sekaligus semakin identik dengan kebocoran data pribadi pengguna internet.

Awal April 2018, Chief Executive Facebook Mark Zuckerberg hadir di Capitol Hill untuk memberikan penjelasan kepada Kongres AS tentang skandal kebocoran data pribadi 87 juta pengguna Facebook ke tangan perusahaan propaganda komputasional Cambridge Analytica. Dalam proses selanjutnya, terungkap bahwa Facebook tidak sanggup melindungi kerahasiaan data penggunanya.

Facebook mengoperasikan berbagai perangkat pelacakan untuk menghimpun sebanyak mungkin data aktivitas pengguna. Namun, keamanan data tersebut ternyata rapuh dan dapat dibobol pihak lain.

Natasha Singer dalam "What You Don't Know About How Facebook Uses Your Data" (2018) mengingatkan yang terjadi sesungguhnya bukan sekadar kebocoran data pengguna. Dalam Pilpres AS 2016, Facebook juga terbukti menawarkan 1,5 juta profil pengguna yang diprediksi berorientasi politik liberal kepada kliennya.

Profil itu tak hanya menjelaskan usia, pekerjaan, lokasi, status hubungan, *likes*, tetapi juga minat, karakter, kebutuhan, jaringan, dan orientasi spiritual. "Berbekal teknologi kecerdasan buatan untuk menganalisis perilaku pengguna, Facebook dapat mempelajari hampir semua hal tentang Anda," kata Peter Eckersley, ilmuwan komputasi di Electronic Frontier Foundation, dikutip Singer.

Penambangan laten data

Apa yang dapat disimpulkan di sini? Semakin sulit bagi kita semua untuk menyembunyikan privasi. Bagi pengguna aktif internet, hampir tak ada tempat lagi untuk menjaga kerahasiaan. *Internet of everything* berarti internet tertanam dalam semua perangkat, dan semua perangkat itu adalah teropong bagi platform digital untuk memata-matai kita.

Facebook tak sendirian di sini. Semua platform digital melakukan apa yang dilakukan Facebook terhadap privasi pengguna. Dengan rentang layanan lebih luas dan beragam, Google bahkan menambang data berskala lebih besar.

Douglas C Schmidt dalam telaah berjudul "Google Data Collection" (2018) menjelaskan bagaimana Google mengumpulkan data pengguna. Sebagai perusahaan platform terbesar, Google mengoperasikan *web browser*, sistem operasi seluler, platform video, layanan *e-mail*, aplikasi peta, dan mesin pencari nomor satu di dunia.

Melalui berbagai layanan ini, Google memiliki kemampuan luar biasa dalam menghimpun informasi terperinci mengenai perilaku daring ataupun realitas hidup sehari-hari penggunanya. Menguasai data psikografis miliaran orang di seluruh dunia adalah kunci keberhasilan Google dalam menguasai surplus ekonomi digital.

Menurut Schmidt, Google pertama-tama melakukan pengumpulan data secara aktif di mana pengguna secara sadar menyerahkan informasi pribadinya. Google memiliki lusinan produk dan layanan. Layanan utama, seperti Youtube, Google Search, Gmail, dan Google Maps, telah menjadi episentrum kegiatan sehari-hari penggunanya di seluruh dunia.

Untuk mengakses berbagai layanan itu, pengguna umumnya disyaratkan untuk membuat akun Google. Pembukaan akun ini merupakan gerbang pertama Google untuk mengumpulkan informasi pribadi, seperti nama, alamat *e-mail*, nomor telepon, nomor kartu kredit, kode pos, dan tanggal lahir.

Cara yang kedua adalah proses pengumpulan data secara pasif yang tanpa disadari pengguna. Pada berbagai layanan Google sesungguhnya terdapat perangkat deteksi aktivitas pengguna yang bekerja secara otomatis dan laten.

Perangkat ini tertanam dalam sistem Android dan Chrome, aplikasi Google Search, Youtube, Maps, Gmail, dan perangkat penunjang untuk penerbit, seperti Google Analytics, AdSense, AdMob, dan AdWords. Mereka secara keseluruhan menggerakkan proses penambangan data yang terstruktur dan terintegrasi dalam ekosistem data Google.

Sistem Android dan Chrome merupakan sarana utama Google dalam melakukan pengumpulan data pengguna secara aktif ataupun pasif. Hingga akhir 2021, OS Android menguasai 71 persen dari pasar sistem operasi seluler global, tertanam dalam lebih dari dua miliar ponsel di seluruh dunia.

Tanpa disadari pengguna, Android membantu Google mengumpulkan informasi pribadi pengguna ponsel (nama, nomor ponsel, tanggal lahir, kode pos, nomor kartu kredit, dan lain-lain), aktivitas digital pengguna melalui ponsel (aplikasi yang digunakan, *website* yang dikunjungi, transaksi elektronik yang dilakukan), dan koordinat lokasi pengguna.

Di sisi lain, *browser* Chrome yang terpasang di lebih dari 2,65 miliar perangkat seluler ataupun *desktop* hingga akhir 2021 juga membantu Google mengumpulkan data pengguna. Chrome mengumpulkan informasi pribadi sejak saat pengguna mengisi Chrome juga mengirimkan informasi tentang riwayat penelusuran *web* dan aktivitas aplikasi seluler pengguna kepada *server* Google.

Perlu ditegaskan di sini, eksperimen Schmidt menunjukkan baik Android maupun Chrome mengirimkan data pengguna ke *server* Google meski pengguna tak sedang mengaktifkan ponsel atau komputernya.

Persoalan terbesar di sini adalah pengguna umumnya tak memahami kompleksitas penambangan data oleh platform digital. *Internet of everything* ternyata juga bermakna *we don't know everything about internet*. Begitu banyak layanan digital yang kita gunakan, begitu banyak aplikasi yang tertanam dalam gawai kita, begitu sedikit pemahaman kita tentang konsekuensinya.

Kita sangat gembira jika ada Wi-Fi di tempat kita *nongkrong*. Namun, kita tak paham ketersediaan Wi-Fi di manamana telah membuat pelacakan lokasi dan aktivitas kita menjadi sangat intensif. Google Maps adalah dewa penolong bagi para pemilik kendaraan bermotor dan pejalan kaki. Namun, aplikasi ini juga sarana bagi Google untuk memetakan mobilitas, budaya berkendara, kebutuhan, pula konsumsi pengguna.

Bicara tentang rahasia pribadi, lebih absurd lagi dalam konteks layanan Gmail. Gmail ibaratnya pusat penyimpanan surat bagi begitu banyak orang. Gmail menyimpan semua pesan yang dikirim atau diterima penggunanya. Bukan sekadar menyimpan, Google diam-diam juga telah mempelajari isi pesan pengguna Gmail untuk melacak aktivitas bisnis dan sosial mereka, serta memetakan masalah dan rencana-rencana mereka.

Ini dilakukan untuk meningkatkan akurasi penargetan iklan dan hasil penelusuran, menyaring *spam* dan untuk tujuan lain. Dengan demikian, semestinya Google tak lagi mengklaim bahwa mereka menambang data pengguna secara anonim. Menurut Schmidt, tak ada lagi anonimitas dalam konteks ini!

Keamanan digital

Kompleksitas masalah di atas mesti menjadi titik tolak pembahasan Undang-Undang Perlindungan Data Pribadi (UU PDP). Platform digital secara eksesif menambang data pengguna, tetapi sering gagal menjamin keamanannya. Kebocoran dan penyalahgunaan data pribadi pun semakin lazim terjadi di saat kita semakin bergantung pada berbagai layanan digital asing.

Jika Google dan Facebook saja tak mampu menjamin keamanan data pengguna, demikian pula dengan para vendor teknologi yang sering digunakan pemerintah. Masalahnya, kalangan pemerintah dan swasta nasional jelas belum mampu membangun sistem data sendiri dan masih bergantung pada jasa perusahaan asing.

Seperti halnya Google dan Facebook, mereka mampu menyajikan layanan teknologi informasi, tetapi gagap dalam menjinakkan residu-residu yang tak terkendali.

UU PDP penting agar kita tak semakin tertinggal dalam membangun sistem pelindungan data. Namun, sama pentingnya adalah terus menyadarkan masyarakat betapa rentannya kita dari praktik pengawasan digital dan penambangan data dengan semua konsekuensinya. *Digital safety* mesti menjadi paradigma yang diarusutamakan.

Jika tidak, UU PDP akan berfungsi layaknya pemadam kebakaran yang tak berhenti memadamkan api yang terus menjalar di padang yang gersang: dunia digital yang tanpa rahasia untuk para penggunanya.