ANCAMAN NYATA ERA DIGITAL

Oleh : Tim Riset Stabilitas LPPI

Era digital ibarat mata uang yang memiliki dua sisi. Satu sisi mendorong beragam kemudahan dalam kehidupan sehari-hari, di sisi lain rentan akan pencurian data-data pribadi. Sisi terakhir memasuki ke ranah privat seseorang yang bisa menimbulkan beragam dampak negatif. Oleh karena itu sangat penting bagi pemangku kepentingan mengupayakan segala daya dan upaya untuk mewujudkan perlindungan data pribadi dari kejahatan siber. Daya dan upaya yang bisa dilakukan oleh pemerintah adalah dengan meningkatkan literasi digital dan pengesahan RUU Perlindungan Data Pribadi.

Praktik digitalisasi di semua lini kehidupan dan di segala kebutuhan membuat ancaman baru pada data pribadi menyeruak. Dibutuhkan aturan untuk melindungi data pribadi sekaligus mengatur praktik digital

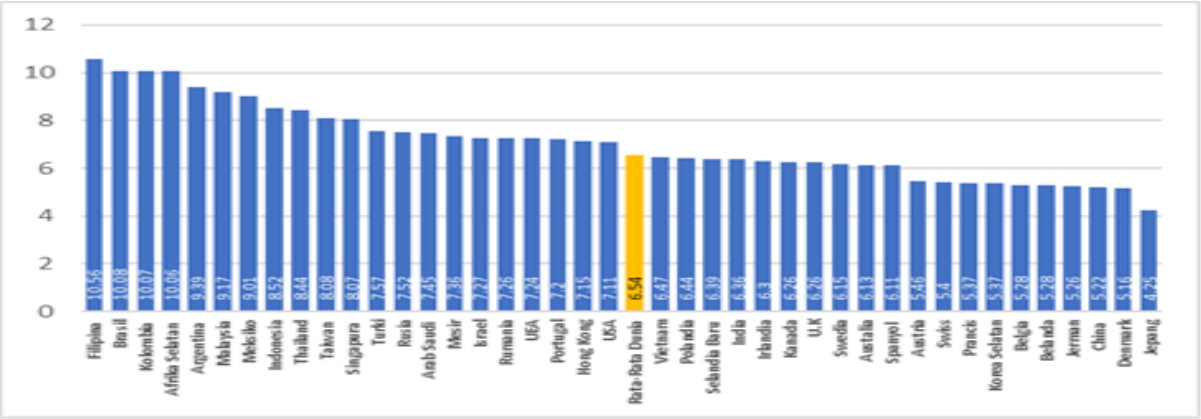
EKONOMI DIGITAL

Sejak teknologi internet merambah ke hampir seluruh pojok-pojok dunia, nyaris semua orang di bumi ini mulai terhubung dan semakin hari hubungan tersebut semakin dekat. Terlebih dengan semakin pesatnya level koneksi internat mulai dari 2G hingga sekarang 5G. Bahkan beberapa negara tengah mempersiapkan dirinya untuk masuk ke jaringan atau koneksi yang semakin cepat dengan platform 6G seperti China. Sejalan dengan hal tersebut, interaksi masyarakat semakin tidak intim dengan internet. Bahkan, internet sudah menjadi kebutuhan hidup yang mendasar bagi Sebagian kalangan dimana apabila tidak ada koneksi internet, aktivitas sosial ekonomi akan terhenti.

Ekonomi digital di Indonesia sangat menjanjikan. Sejak tahun 2015 hingga tahun 2020, nilai total transaksi (Gross Merchandise Value - GMV) sektor ekonomi digital di Indonesia tumbuh sekira 40% per tahunnya. Angka tersebut diperkirakan akan mencapai 130 miliar dollar AS pada tahun 2025 (CIPS, 2021). Data dan proyeksi data tersebut menjadikan Indonesia menjadi pasar digital yang paling menjanjikan di antara negara-negara di Kawasan. Menurut riset JP Morgan (2019), nilai ekonomi digital Indonesia senilai 100 miliar dollar AS, terbesar senilai di antara negara ASEAN.

Sejalan dengan itu, pengguna internet di Indonesia meningkat pesat, terlebih di tengah pandemi Covid-19. Keberadaan pandemi memaksa masyarakat memiliki akses internet guna bekerja dari rumah. Perusahaan media asal Inggris, We Are Social, dalam laporannya bertajuk Digital 2021: The Latest Insights Into The State of Digital, mengungkapkan jumlah pengguna internet di Indonesia mencapai 202,6 juta dengan tingkat penetrasi 73,7 persen.

Grafik 1
Rata-Rata Lama Waktu Menghabiskan Internet Dalam Satu Hari (Jam-Menit)

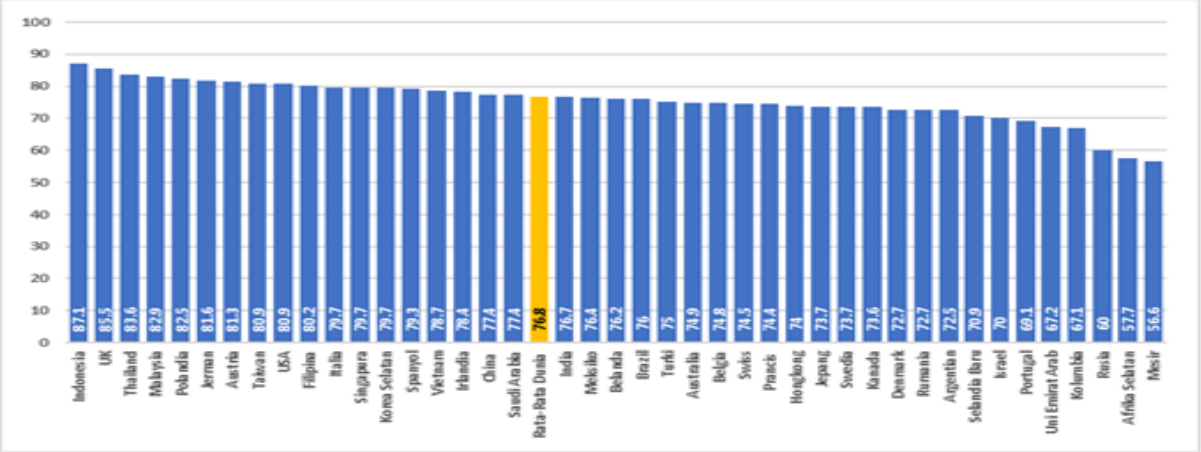


Sumber : www.wearesocial.com - 2021

Pengguna internet di Indonesia menghabiskan waktu di atas rata-rata pengguna dunia. Orang Indonesia mengakses internet per hari rata-rata sebanyak 8 jam 52 menit. Sedangkan di rata-rata dunia hanya menghabiskan 6 jam 54 menit. Masih menurut laporan yang sama, 96,4 persen dari total 202,6 juta pengguna, menggunakan ponsel pintar untuk mengakses internet. Angka ini meningkat pesat jika dibandingkan dengan jumlah pengguna internet pada tahun 2020. Terdapat kenaikan 15,5 persen atau lebih dari 27 juta orang dalam jangka waktu 1 tahun.

Kenaikan pengguna internet tersebut didorong oleh makin besarnya pasar e-commerce di Indonesia. Data per Januari 2021 mengungkapkan, pengguna internet Indonesia usia 16-64 tahun, sebanyak 87 persen nya membeli produk dalam satu bulan. Angka tersebut merupakan angka tertinggi di dunia. Pada level global, hanya 77 persen pengguna internet yang membeli barang secara online dalam satu bulan terakhir.

Grafik 2
Persentase Pengguna Internet Usia 16-64 Tahun yang Membeli Barang Secara Online dalam 1 Bulan Terakhir



Sumber : www.wearesocial.com - 2021

SISI GELAP

Pesatnya perkembangan sektor digital di Indonesia memiliki sisi gelap, kebocoran data pribadi. Hingga saat ini kasus kebocoran data pribadi masyarakat yang menyedot perhatian publik. Pertama, kebocoran data BPJS Kesehatan. Pada bulan Mei 2021, terungkap sejumlah praktik penjualan data sejumlah peserta Badan Penyelenggara Jaminan Sosial (BPJS) di sebuah forum daring. Meski diklaim bukan dari BPJS Kesehatan yang membocorkan data tersebut, namun data-data yang diperjualbelikan tersebut mirip dengan milik badan penyelenggara pelayanan Kesehatan tersebut.

Terbaru, kebocoran data pengguna e-HAC (Electronic Health Alert) yang menggemparkan jagad maya nasional. Diduga, kebocoran data tersebut berasal dari mitra. Langkah tindak lanjut yang diambil pemerintah adalah meminta kepada masyarakat untuk menghapus e-HAC lama dari ponsel yang digunakan. Selain dua kasus kebocoran data tersebut di atas, masih banyak ditemukan kasus kebocoran data dari entitas bisnis lain yang bisa ditemukan di internet dan media sosial. Lebih lanjut, kejahatan siber tidak terkotak dalam jual beli data pribadi saja, namun lebih luas dari itu semisal penggelapan rekening nasabah serta penipuan lain dengan menggunakan data pribadi milik orang lain.

Kejahatan siber seperti pencurian data menimbulkan kerugian ekonomi yang tidak sedikit. Berdasarkan data Indonesia Cyber Security Independent Resilience Team (CSIRT.ID), kebocoran 279 juta penduduk Indonesia, bisa menyebabkan kerugian material mencapai Rp600 triliun. Perhitungan angka kerugian ini berdasarkan kerugian masyarakat Indonesia akibat penyalahgunaan data yang bocor.

Terkait dengan kebocoran data e-HAC, Communication & Information System Security Research Center (CISSReC) menyebutkan terdapat potensi kerugian dari kebocoran Rp2,8 triliun. Kerugian ini muncul dari bocornya 1,3 juta pengguna aplikasi kesehatan tersebut. Masih menurut CISSReC, jenis data yang bocor antara lain data nama, nama rumah sakit, alamat, hasil tes PCR, dan akun e-HAC.

Kebocoran data tidak melulu berasal dari aplikasi yang digunakan oleh konsumen. Namun juga bisa berasal dari scamming melalui pesan WA dan juga SMS. Contohnya jika seseorang mengeklik tautan di dalam pesan WA atau SMS untuk mengetahui iming-iming yang diberikan semisal uang tunai, maka besar kemungkinan data atau ponsel tersebut telah dikloning. Alhasil, pelaku kejahatan bisa dengan leluasa menggunakan ponsel tersebut untuk kegiatan mengatasnamakan pemilik ponsel.

Kasus pengkloningan data melalui ponsel menimbulkan kerugian non-material dan material. Kerugian non material antara lain mencakup opportunity waktu yang diperlukan untuk membereskan persoalan kebocoran data. Pelaporan kepada provider data, pelaporan kepada pihak bank untuk memblokir rekening keuangan, serta woro-woro kepada keluarga, teman dan kolega. Setidaknya waktu setengah hari diperlukan untuk melakukan semua itu. Kerugian material dari kejahatan skimming handphone tidak bisa dielakkan. Biaya-biaya akan dikeluarkan untuk menyelesaikan persoalan yang muncul akibat kebocoran data pribadi kita.

JALAN KELUAR

Salah satu sebab masih maraknya data kebocoran data pribadi dan kejahatan siber lainnya adalah rendahnya literasi digital masyarakat Indonesia. Literasi digital tidak hanya mencakup persoalan berapa persen penduduk yang telah mengakses internet, tapi juga seberapa jauh pemahaman masyarakat terhadap aspek dunia digital. Bagaimana pemahaman masyarakat tentang risiko serta hak dan kewajiban dalam pengelolaan data konsumen/masyarakat yang telah disetorkan.

Kementerian Komunikasi dan Informatika menyebutkan setidaknya ada lima alasan utama pentingnya menjaga data pribadi yakni, pertama menghindari intimidasi online terkait gender. Privasi data tentang gender penting untuk menghindari kasus pelecehan seksual atau perundungan (bullying) secara online. Selain itu, perlindungan terhadap data penting dilakukan agar menghindari ancaman kejahatan dunia maya termasuk Kekerasan Berbasis Gender Online (KBGO).

Kedua, mencegah penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab. Ketiga, menjauhi potensi penipuan, keempat menghindari potensi pencemaran nama baik. Kelima hak kendali atas data pribadi. Hak kendali ini sejalan dengan Deklarasi Universal tentang Hak Asasi Manusia 1948 pasal 12 dan Konvensi Internasional tentang Hak Sipil dan Politik (ICCPR) 1966 pasal 1

Di sisi lain, pengamanan data pribadi di Indonesia masih menghadapi tantangan. Berdasarkan Badan Siber dan Sandi Negara (BSSN), pengamanan data pribadi di Indonesia menghadapi setidaknya lima tantangan. Pertama, banyaknya jumlah data yang ditampung aplikasi harus diimbangi dengan upaya jauh lebih kuat dalam pengamanannya. Kedua, data pribadi yang dapat diserahkan kepada pihak lain menimbulkan risiko kebocoran data pribadi. Ketiga, pengelolaan data pribadi harus disertai dengan manajemen yang baik. Keempat, penggunaan ragam platform seperti mobile phone dan website juga menjadi tantangan tersendiri dalam pengamanan data pribadi. Kelima, penggunaan komputasi awan menimbulkan risiko yang harus dimitigasi pelaku usaha

Saat ini, standar perlindungan data pribadi sudah termaktub dalam SNI 27001. Melalui SNI ini, pelaku usaha yang memanfaatkan atau mengumpulkan data pribadi konsumen atau masyarakat diwajibkan mendaftarkan sistem keamanannya sesuai standar tersebut sebelum melayani masyarakat. Hal ini ditujukan untuk memberi perlindungan data pribadi yang telah dikumpulkan pelaku usaha tersebut. Satu hal yang harus digarisbawahi adalah, SNI 27001 memberi kepercayaan masyarakat pada perusahaan tersebut.

Usaha meningkatkan literasi digital harus dibarengi usaha paripurna pengesahan RUU Perlindungan Data Pribadi. Hal ini penting meskipun sebuah masyarakat sudah sangat paham literasi digital baik tekstual dan kontekstual, pencurian data pribadi masih tetap dimungkinkan ada. Ketiadaan perlindungan data pribadi akan memperparah kejahatan pencurian data. Oleh karena itu, diharapkan per 2021, RUU Perlindungan Data Pribadi harus segera disahkan.

File ini dapat diunduh melalui : http://lppi.or.id/produk/riset/
Untuk korespondensi dan informasi lebih lanjut, hubungi :
Divisi Corporate Secretary
Telp: (021) 71790919 ext. 393 | Email: dcsc@lppi.or.id
Website : www.lppi.or.id