Policy Brief

KEAMANAN DATA KESEHATAN : TANTANGAN DAN REKOMENDASI ARAH PENGEMBANGAN

Lutfan Lazuardi, Bagas Suryo Bintoro, Zakiya Ammalia Farahdilla

RINGKASAN EKSEKUTIF

Digitalisasi data kesehatan semakin gencar dipraktikkan di masa depan dalam rangka memudahkan dan mempercepat pemberian pelayanan kesehatan. Disisi lain, tingkat keamanan data di Indonesia sangat lemah. Data kesehatan merupakan data pribadi yang bersifat spesifik, sensitif, dan rahasia yang harus dilindungi. Pemerintah Indonesia perlu segera merespon untuk meminimalisir risiko penyalahgunaan data, salah satunya dengan membuat pedoman dan payung hukum yang kuat untuk memerangi penyalahgunaan data.

PENDAHULUAN

Pada tahun 2009, Presiden Amerika Serikat, Barack Obama, mengeluarkan memorandum tentang transparansi dan pemerintahan terbuka. Keterbukaan memperkuat demokrasi, mendorong efisiensi, dan efektivitas pemerintahan. Sejak saat itu Pemerintah Amerika Serikat membuka data mereka dalam platform terbuka yaitu data.gov. Negara lain mengikuti hingga banyak situs data terbuka diluncurkan oleh pemerintah. Data terbuka berdampak pada keuntungan 3-5 triliun USD per tahun dalam bidang ekonomi global, menghemat 50-550 USD per tahun dalam pelayanan kesehatan di Amerika Serikat [1]. Data terbuka dapat mempercepat penyebaran pengetahuan, memicu kolaborasi, inovasi, dan mengurangi duplikasi [2]. Data terbuka menjadi dasar pengambilan keputusan dan kebijakan termasuk saat situasi darurat. Pandemi COVID-19 menuntut transparansi data agar penanganan dapat dilakukan dengan cepat. Hal ini menjadikan data kesehatan semakin terbuka dan berkembang pesat [3]. Sistem konsultasi kesehatan melalui aplikasi kesehatan (telemedicine) telah banyak dipraktikkan. Di saat yang sama juga dapat menimbulkan dampak atau ancaman baru terkait penyalahgunaan data pribadi sehingga dapat merugikan pemilik data. Hal ini menimbulkan banyak tantangan dalam pelaksanaannya [4]. Risalah kebijakan ini disusun untuk memberikan rekomendasi langkah Pemerintah Indonesia dalam memerangi penyalahgunaan data pribadi.

RUMUSAN MASALAH

Indonesia merupakan negara dengan pengguna internet peringkat ke-4 tertinggi di dunia setelah China, India, dan Amerika Serikat pada tahun 2021 [5]. Tingkat penetrasi internet di Indonesia mencapai 77,02% pada tahun 2021 [6]. Tingginya pengguna jasa internet menjadikan semakin pesatnya pertumbuhan layanan digital berbasis teknologi informasi. Telemedicine telah diterapkan oleh Kementerian Kesehatan untuk meningkatkan akses layanan kesehatan masyarakat di daerah rural sejak tahun 2012. Rekam medis banyak didokumentasikan dalam bentuk rekam medis elektronik.

Pandemi COVID-19 menuntut transparansi data agar penanganan dapat dilakukan dengan cepat. Pemanfaatan teknologi digital pada pelayanan kesehatan dapat memudahkan pasien maupun tenaga kesehatan. Meskipun demikian, sistem keamanan dan perlindungan data kesehatan pasien yang terekam secara digital di internet perlu dicermati. Data kesehatan pasien yang mengandung informasi pribadi berisiko diakses pihak tidak bertanggung jawab [7].
Telah banyak insiden kebocoran data kesehatan diantaranya kasus kebocoran data 279 pengguna BPJS Kesehatan pada Mei 2021. Baru-baru ini terjadi kebocoran 1,3 juta data pengguna aplikasi Electronic Health Alert (eHAC) milik Kemenkes RI pada Agustus 2021 dan bocornya sertifikat vaksin beserta Nomor Induk Kependudukan (NIK) milik Presiden Joko Widodo pada September 2021 [8].

Perusahaan digital seperti E-commerce biasanya mengumpulkan data seperti nama, NIK, alamat, alamat email, nomor telepon, sebagian foto anggota tubuh atau biometric data, dan akses sebagian data pada telepon genggam seseorang baik itu riwayat lokasi, foto, maupun kontak. NIK rentan diretas karena Pemerintah Indonesia banyak menggunakan NIK sebagai kode unik yang diintegrasikan ke berbagai data pribadi lainnya. Dampak kebocoran data pribadi tidak hanya kerugian secara materi, namun juga psikis korban, misalnya, potensi perlakukan diskriminatif pada pasien penyakit tertentu yang memiliki stigma buruk.

Kasus-kasus kebocoran data pribadi di Indonesia seringkali berakhir tanpa penyelesaian yang tuntas. Pihak terkait seakan cukup mengeluarkan pernyataan dan klarifikasi terkait kebenaran berita kebocoran data tersebut, kemudian dilakukan pemutusan akses atau penonaktifan aplikasi sementara. Hal tersebut menandakan keamanan data di Indonesia sangat lemah [9]. Banyak masyarakat dalam hal ini pemilik data tidak menyadari bahwa ia dirugikan atas kasus kebocoran data miliknya. Hal ini menjadikan para pelaku pencurian data pribadi leluasa melakukan tindakan tersebut dan menjadikan jual beli data pribadi sebagai mata pencahariannya [10].

PENYEBAB

Indonesia merupakan salah satu negara di ASEAN yang belum memiliki kebijakan atau regulasi khusus terkait perlindungan data pribadi. Belum ada aturan yang komprehensif mengatur tindak lanjut penyalahgunaan data pribadi. Aturan tersebar dalam beberapa peraturan yang sifatnya umum. Hal ini menjadikan penyalahgunaan data pribadi ditindaklanjuti dengan hukum yang kurang tepat. Belum ada lembaga khusus yang ditunjuk untuk menangani perlindungan data pribadi. Kementerian Komunikasi dan Informatika (Kominfo) menindaklanjuti kasus kebocoran mengacu pada tiga aturan berikut, yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika No 21 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Kominfo telah menindaklanjuti beberapa kasus kebocoran data pribadi dengan memberikan sanksi berupa teguran tertulis dan rekomendasi perbaikan sistem[11].

Berdasarkan peraturan perundang-undangan, kasus kebocoran data kesehatan melanggar UU No 26 Tahun 2009 tentang Kesehatan. Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.

Pengendali adalah orang atau badan hukum, otoritas publik, swasta atau badan lain yang menentukan tujuan dan sarana pengolahan data, misalnya Rumah Sakit (RS). Pemroses data adalah orang atau badan hukum, otoritas publik, swasta, atau badan lain yang memproses data pribadi atas nama pengendali, misalnya Rumah Sakit menunjuk Divisi Pengelolaan Data atau pihak ketiga. Keberadaan pemroses tergantung pengendali yang memproses data dalam organisasinya. GDPR dan UU di Indonesia tidak mengatur secara eksplisit perbedaan tanggung jawab hukum antara pengendali dan pemroses data, maka upaya hukum perlu mengetahui isi perjanjian pengelolaan data yang disepakati kedua belah pihak. Hal ini menjadikan pihak yang lalai yang dimintai pertanggung-jawaban [7].

Kurangnya kesadaran dari orang-orang yang bersinggungan dengan data pribadi baik pemilik, pemroses, dan pengendali data mengenai pentingnya keamanan data pribadi turut andil menjadi penyebab kebocoran data. Pemilik data dalam hal ini misal pasien perlu diberikan peningkatan pengetahuan melalui literasi. Pemroses memerlukan orang yang ahli dalam bidang IT dan mau terus belajar berkejaran dengan pengetahuan terkait perlindungan data pribadi di tengah pesatnya perkembangan digital.

REKOMENDASI

Saat ini terdapat keadaan darurat perlindungan data pribadi di tengah pesatnya perkembangan teknologi. RUU Perlindungan Data Pribadi harus segera disahkan dan diundangkan guna menjaga kerahasiaan data pribadi warga negara Indonesia dan bersaing dengan bisnis global. Selanjutnya melakukan evaluasi untuk menciptakan suatu politik hukum yang komprehensif disertai kajian-kajian yang masif untuk mengeluarkan produk hukum berkualitas. Mencakup standar dan prosedur pengelolaan data pribadi sebagai langkah preventif dan tindak lanjut jika terjadi penyalahgunaan data pribadi. Penunjukan lembaga khusus perlu dilakukan sebagai pengawas pelaksanaan perlindungan data pribadi. Perlindungan data pribadi membutuhkan infrastruktur dan sumber daya manusia yang memadai, oleh karena itu pemerintah perlu mengalokasikan dana untuk hal tersebut. Serta peningkatan kesadaran dari orang yang bersinggungan dengan data baik pemilik, pemroses, dan pengendali data.

SASARAN PEMANGKU KEBIJAKAN

- Kementerian Kesehatan
- Kementerian Komunikasi dan Informatika

REFERENSI
[1] Kobayashi S, Kane TB, Paton C. The Privacy and Security Implications of Open Data in Healthcare. Yearb Med Inform. 2018 Aug;27(1):41-47. doi: 10.1055/s-0038-1641201. Epub 2018 Apr 22. PMID: 29681042; PMCID: PMC6115211.
[2] Rockhold F, Bromley C, Wagner EK, Buyse M. Open science: The open clinical trials data journey. Clin Trials. 2019 Oct;16(5):539-546. doi: 10.1177/1740774519865512. Epub 2019 Jul 26. PMID: 31347390.
[3] Tanwar AS, Evangelatos N, Venne J, Ogilvie LA, Satyamoorthy K, Brand A. Global Open Health Data Cooperatives Cloud in an Era of COVID-19 and Planetary Health. OMICS. 2021 Mar;25(3):169-175. doi: 10.1089/omi.2020.0134. Epub 2020 Oct 13. PMID: 33719569.
[4] Setiawan, H. B., Najicha, F. U., Perlindungan Data Pribadi Warga Negara Indonesia terkait dengan Kebocoran Data, 2022, 6(1): 976-982
[5] https://www.internetworldstats.com/top20.htm diakses pada tanggal 20 Agustus 2022.
[6] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2022, Profil Internet Indonesia 2022. Jakarta
[7] Sukmadilaga, A., Rosadi, S. D., Upaya Hukum terhadap Pelanggaran Implementasi Internet of Things (IoT) di Bidang Pelayanan Kesehatan menurut Ketentuan Perlindungan Data Pribadi, Suara Keadilan, 2020, 21(2): 205-221.
[8] https://katadata.co.id/muchamadnafi/indepth/613239a9d3cfa/mengapa-data-kesehatan-di-indonesia-mudah-bocor diakses pada tanggal 21 Agustus 2022.
[9] Djafar, W., 2019, Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan, Makalah disampaikan sebagai materi dalam kuliah umum "Tantangan Hukum dalam Era Analisis Big Data". Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada.
[10] https://theconversation.com/tokopedia-dan-bukalapak-memang-bisa-digugat-tapi-tidak-lantas-masalah-kebocoran-data-tuntas-140193 diakses 22 Agustus 2022
[11] https://katadata.co.id/desysetyowati/digital/61cd8cf0e5173/kominfo-tangani-43-kebocoran-data-tahun-ini-bpjs-kesehatan-belum diakses 22 Agustus 2022