PUSAT KAJIAN AKUNTABILITAS KEUANGAN NEGARA
BADAN KEAHLIAN DPR RI
www.puskajiakn.dpr.go.id

Accountability Brief

Tim Penulis:
Helmizar
Achmad Yugo Pidhegso
Mochammad Ramadhan

2022

Komisi I

Urgensi Pengesahan RUU Perlindungan Data Pribadi

1. Isu Strategis

Salah satu tujuan negara Republik Indonesia yang tercantum dalam pembukaan UUD 1945 adalah melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia. Dalam Pasal 28G ayat (1) UUD 1945 juga disebutkan bahwa warga negara Indonesia berhak atas perlindungan diri pribadi. Dimensi perlindungan terhadap warga Indonesia tentunya sangat luas, termasuk perlindungan terhadap keamanan data pribadi seluruh warga Indonesia. Data pribadi merupakan hak privasi setiap warga negara Indonesia. Terkait dengan hak privasi, dalam *International Covenant on Civil and Political Rights* (ICCPR) *Article* 17 Nomor 1 disebutkan bahwa tidak ada satu orang-pun yang pantas untuk diperlakukan sewenang-wenang dan melanggar hukum dalam hal privasi, keluarga ataupun martabat dan reputasinya. Dapat dilihat bahwa perlindungan data pribadi sudah merupakan suatu kewajiban negara dan hak warga negara serta diakui dan disadari secara internasional.

Kondisi saat ini Indonesia belum memiliki Undang-Undang yang secara spesifik mengatur tentang perlindungan data pribadi warga negara Indonesia. Dengan kondisi ini terdapat beberapa kasus kebocoran data di Indonesia yaitu:

1. Kebocoran 279 juta data BPJS Kesehatan pada Mei 2021 dengan kondisi 20 juta diantaranya memiliki foto diri. Data tersebut dijual di RaidForums dengan harga 0,15 Bitcoin.
2. Kebocoran 2,9 juta data pengguna Cermati.com yang sebagian besar merupakan data kegiatan finansial. Data ini juga diperjualbelikan di RaidForums.
3. Kebocoran 1,1 juta data pengguna Lazada.
4. Kebocoran 463.000 dokumen berupa foto E-KTP, nomor rekening, NPWP, Akta Kelahiran nasabah BRI Life yang dijual dengan harga USD 7.000 di Juli 2021.
5. Kebocoran 91 juta data pengguna Tokopedia Mei 2020 yang dijual seharga USD 5.000.
6. Kebocoran 2,3 juta data warga negara Indonesia di Komisi Pemilihan Umum pada Mei 2021. Data ini berupa Nama, Alamat, Nomor KK, dan NIK.
7. Kebocoran 1,3 juta data Electronic Health Alert Card (E-HAC) pada Juli 2021.
8. Kebocoran 28.000 data akun dan data pribadi Polri pada November 2021.
9. Sertifikat Vaksinasi Covid-19 Presiden Indonesia Joko Widodo beredar di Internet.
10. Kebocoran 6 juta data rekam medis pasien Covid-19 milik Kementerian Kesehatan pada Januari 2022. Data ini diperjualbelikan di RaidForums.

Dari beberapa contoh kasus yang telah disebutkan, tidak ada konsekuensi hukum yang harus dijalani oleh pihak pengendali data dalam hal ini perusahaan atau instansi yang menyimpan data pribadi warga negara Indonesia. Sebenarnya UU ITE mengatur tentang larangan akses *computer*/sistem elektronik milik orang lain pada Pasal 30 dan hukuman atas hal ini diatur pada Pasal 46. Namun hukuman yang dikenakan pada aturan ini adalah bagi orang yang mengakses data tersebut secara ilegal, bukan terhadap perusahaan atau instansi pengendali data. Berikut beberapa implikasi dari lemahnya perlindungan data pribadi di Indonesia:

2. Risiko Kerugian Materiil Warga Negara Indonesia

Menyandingkan data dengan materi bukan merupakan hal baru, Presiden Joko Widodo mengatakan pada pidato tanggal 24 Januari 2020 bahwa data merupakan jenis kekayaan baru dan data merupakan "*new oil*" atau bahkan lebih berharga dari minyak serta menjadi salah satu kunci keberhasilan pembangunan.

Data pribadi warga negara Indonesia yang bocor menjadikan warga Indonesia memiliki risiko untuk mengalami kerugian materiil. Hal ini disebutkan oleh Pratama Persadha Pakar Keamanan *Communication & Information System Security Research Center* (CISSReC) yaitu data pribadi yang bocor dapat digunakan oleh orang untuk mengambil dompet digital yang dimiliki orang pemilik data tersebut. Hal ini dimungkinkan karena data pribadi yang bocor tentunya akan memudahkan pihak yang berniat jahat untuk melakukan verifikasi data saat proses mengambil dompet digital pemilik data.

Direktur Sistem dan Sumber Daya Informasi Universitas Gadjah Mada (UGM) Widyawan, ST., M.Sc., Ph.D. menyampaikan bahwa pencurian identitas ini akan mengakibatkan pemilik data terekspos dalam risiko menjadi sasaran marketing ilegal dan penipuan *online*. Dijelaskan lebih lanjut bahwa tindak kriminal terkait transaksi elektronik muncul dengan adanya kebocoran data pribadi.

Tidak hanya itu, Indonesia *Cyber Security Independent Resilience Team* (CSIRT) melansir bahwa dengan peristiwa bocornya data BPJS Kesehatan, Indonesia dimungkinkan merugi sebesar Rp600 Triliun. Hitungan fantastis ini didapat dari perhitungan kebocoran data yang dimiliki oleh lembaga riset Ponemon-IBM.

3. Risiko Hilangnya Kepercayaan Masyarakat Terhadap Keamanan Data di Indonesia

Pakar dari Universitas Gadjah Mada (UGM) Widyawan, ST., M.Sc., Ph.D. mengungkapkan bahwa kebocoran data jika tidak segera dituntaskan akan mengakibatkan runtuhnya reputasi perusahaan atau instansi. Kepercayaan publik terhadap kemampuan perusahaan atau instansi mengamankan data akan turun drastis.

CEO Indonesia Digital Identity (VIDA) Sati Rasuanto menyampaikan bahwa kepercayaan digital merupakan hal yang paling penting dalam pertumbuhan *industry digital*. Dalam hal ini data menjadi sumber kehidupan *industry digital*. Maraknya peristiwa kebocoran data di Indonesia tentunya akan sangat berpengaruh terhadap kepercayaan masyarakat dalam keamanan data digital.

Tidak hanya untuk perusahaan atau instansi saja, pelindungan data pribadi juga akan mempengaruhi kepercayaan investor terhadap pasar di Indonesia. Peristiwa kebocoran data pada perusahaan dan instansi publik di Indonesia ini dapat menimbulkan "*distrust*" dari negara lain. Hal ini diungkapkan oleh Staf Ahli Kementerian Komunikasi dan Informatika Henri Subiakto. Hal ini perlu mendapatkan perhatian karena rendahnya kepercayaan investor terhadap pasar di Indonesia ini tentunya akan berpengaruh negatif terhadap nilai tukar Rupiah.

4. Saran Perhatian

Kondisi yang telah dijabarkan diatas menunjukkan perlunya ada payung hukum pelindungan data pribadi yang dapat menjadi acuan pelaksanaan pelindungan data pribadi di perusahaan

maupun instansi pemerintahan. Maka dari itu, diharapkan Komisi I DPR RI melalui Panja RUU PDP dapat mendorong Kementerian Komunikasi dan Informatika untuk mempercepat pembahasan dan pengesahan RUU PDP. Disamping itu, diharapkan Komisi I DPR RI untuk dapat mendorong Badan Siber dan Sandi Negara untuk meningkatkan keamanan siber di Indonesia dan memberikan laporan berkala terkait serangan siber yang terjadi di Indonesia.

5. Referensi

Cnnindonesia.com. 2021. Perlindungan Data Pribadi Jadi Kunci Pertumbuhan Digitalisasi RI. Perlindungan Data Pribadi Jadi Kunci Pertumbuhan Digitalisasi RI – 7 Maret 2022.

Csirt.id. 2021. *Indonesia Rugi Dari 600 Triliun Rupiah Akibat Kebocoran 279 Juta Data Penduduk*. Diakses dari Indonesia Rugi Dari 600 Triliun Rupiah Akibat Kebocoran 279 Juta Data Penduduk – csirt.id 9 Maret 2022.

Kompas.com. 2021. *28.000 Data Polri Disebut Bocor, Ini Analisis Pengamat.* 28.000 Data Polri Disebut Bogor, Ini analisis Pengamat – 10 Maret 2022.

Merdeka.com. 2020. *Pencurian Data Pribadi Dikhawatirkan Ancam Kepercayaan Investor*. Pencurian Data Pribadi Dikhawatirkan Ancam Kepercayaan Investor – 9 Maret 2022.

Nugroho, Agung. 2021. Pentingnya Ratifikasi RUU Perlindungan Data Pribadi. Universitas Gadjah Mada. Yogyakarta.

Republik Indonesia. 1999. Undang-Undang Dasar Republik Indonesia 1945

Republik Indonesia. 2008. Undang-Undang Nomor 11 Tahun 2008. Tentang Informasi dan Transaksi Elektronik.

Riyadi. Gliddheo Algifariyano. 2021. Data Privacy in the Indonesian Personal Data Protection Legislation. Center for Indonesian Policy Study. Jakarta.

Tempo.co. 2021. *6 Kasus Kebocoran Data Pribadi di Indonesia.* Diakses dari 6 Kasus Kebocoran Data Pribadi di Indonesia – nasional.tempo.co 8 Maret 2022.