KEMENTERIAN HUKUM DAN HAM RI
BADAN PEMBINAAN HUKUM NASIONAL
Pusat Jaringan Dokumentasi dan Informasi Hukum Nasional
Jl.May.Jen. Sutoyo -Cililitan- Jakarta Timur

Sumber : KOMPAS	**Hari/Tgl :** Kamis, 27 Juni 2024	**Hlm/Kol :** 6/2-5
Subjek : UU - PERLINDUNGAN DATA PRIBADI		**Bidang :** HTN

Ujian Jelang Implementasi UU Pelindungan Data Pribadi

Cornel Juniarto
Data Governance Expert; Alumnus Lemhannas PPRA 53

Gangguan pada Pusat Data Nasional dalam beberapa hari ini bisa menjadi pisau bermata dua bagi Implementasi Undang-Undang Pelindungan Data Pribadi atau UU PDP, Oktober nanti. Keseriusan para pengambil keputusan untuk segera mengungkap dan mengatasi gangguan ini akan menjadi penentu utama kepercayaan publik terhadap keberhasilan implementasi UU PDP.

Dalam beberapa hari terakhir, pemberitaan nasional diramaikan dengan peristiwa gangguan terhadap Pusat Data Nasional atau PDN yang mengakibatkan *down*-nya sistem layanan publik yang terintegrasi dengan PDN, yakni layanan keimigrasian. Penyebab gangguan belum diungkap pemerintah, tetapi beberapa pakar menduga hal tersebut terkait dengan upaya peretasan data dan pemerasan (*ransomware*).

Menteri Komunikasi dan Informatika telah memberikan penjelasan kepada publik dan menyampaikan bahwa penyebab gangguan sistem bukan karena peretasan atau serangan siber.

Terlepas dari akar penyebabnya, gangguan yang terjadi menjelang implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi—yang akan diterapkan pada Oktober 2024—ini sedikit banyak pasti akan berpengaruh pada kepercayaan publik terhadap keandalan pemerintah dalam mewujudkan substansi pengaturan UU PDP. Khususnya kemampuan pemerintah dalam memitigasi risiko kegagalan pelindungan data pribadi di masa depan.

Kedaulatan data dan privasi data

Peran PDN sangat krusial bagi pemerintah. PDN tidak hanya membantu konsolidasi data secara nasional dan mempercepat pelayanan publik di seluruh sektor secara terintegrasi, tetapi juga kehadirannya akan menjamin kedaulatan data suatu negara (*data sovereignty*) dan hak privasi data warga negara (*data privacy*).

Mengacu pada standar *general data protection regulation* (GDPR), prinsip pelindungan data pribadi mengedepankan *data sovereignty* sebagai prioritas untuk mengamankan dan menjaga hak *data privacy* warga negara.

Kedaulatan data merupakan konsep di mana data pribadi seseorang yang disimpan di suatu lokasi atau suatu negara menjadi subyek dari hukum privasi data yang diterapkan di negara tersebut. Oleh karena itu, sudah sewajarnya pemerintah bertanggung jawab untuk semaksimal mungkin mengatur dan mengendalikan data di dalam batas wilayahnya.

Pada dasarnya kedaulatan data dan hak privasi data memiliki banyak kesamaan. Secara historis, konsep kedaulatan data adalah bagaimana suatu negara-bangsa mengklaim kekuasaan absolutnya atas suatu domain data atau bidang data tertentu.

Klaim yang sama terhadap domain data juga dimiliki individu sehingga kedaulatan negara dan privasi individu menjadi setara karena adanya kesamaan terhadap prinsip-prinsip umum tata kelola data yang dimiliki keduanya.

Seperti halnya negara yang mengklaim kedaulatannya di dalam wilayah yurisdiksinya dan non-interventif, individu juga menegaskan hak privasinya untuk dibiarkan berada di dalam wilayah mereka dalam kekuasaan yang sah atas pilihan mereka dan kendali yang efektif atas penggunaan data mereka sehingga mereka dapat "dibiarkan dalam damai."

Individu mempunyai kedaulatan dalam hal data pribadinya, sama seperti negara yang mempunyai kedaulatan atas data pribadinya di wilayah mereka (Polcak dan Svantesson, 2017 sebagaimana dikutip dari Cheung, 2023).

Risiko kegagalan pelindungan data pribadi

Meskipun belum terungkap penyebabnya, penjelasan pemerintah atas gangguan PDN patut diapresiasi karena hal tersebut merupakan bentuk penerapan kewajiban Pengendali Data Pribadi sesuai Pasal 46 UU PDP.

Berdasarkan UU PDP, salah satu kewajiban Pengendali Data Pribadi adalah memberitahukan terjadinya kegagalan pelindungan data pribadi.

Pasal 46 Ayat (1) dan (2) UU PDP mengatur bahwa dalam hal terjadi kegagalan pelindungan data pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 jam kepada: a) subyek data pribadi dan b) lembaga.

Pemberitahuan tersebut minimal memuat: data pribadi yang terungkap, kapan dan bagaimana data pribadi terungkap, serta upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh Pengendali Data Pribadi.

Penjelasan Pasal 46 Ayat (1) UU PDP menjelaskan bahwa yang dimaksud dengan "kegagalan pelindungan data pribadi" adalah kegagalan melindungi data pribadi seseorang dalam hal kerahasiaan, integritas, dan ketersediaan data pribadi, termasuk pelanggaran keamanan, baik yang disengaja maupun tidak disengaja, yang mengarah pada perusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah ter-

Sambungan

Sumber : KOMPAS | Hari/Tgl : Kamis, 27 Juni 2024 | Hlm/Kol : 6/2-5

hadap data pribadi yang dikirim, disimpan, atau diproses.

Lebih lanjut, Pasal 46 Ayat (3) UU PDP mengatur bahwa dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan pelindungan data pribadi.

Penjelasan Pasal 46 Ayat (3) menjelaskan bahwa yang dimaksud "dalam hal tertentu", antara lain, jika kegagalan pelindungan data pribadi mengganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat.

Kejadian gangguan PDN baru-baru ini telah mengganggu pelayanan publik dan berdampak pada kepentingan masyarakat secara luas. Dalam hal ini, pemerintah melalui Menkominfo telah memberikan penjelasan kepada masyarakat atas terjadinya gangguan tersebut. Namun, belum dapat diketahui apakah gangguan tersebut telah memenuhi aspek "kegagalan pelindungan data pribadi" atau tidak.

Terlepas dari ada atau tidaknya risiko kegagalan dalam pelindungan data pribadi pada kejadian gangguan tersebut, efektivitas pemerintah dalam penanganan kejadian gangguan harus menjadi catatan penting bagi para pengambil keputusan dan menjadi masukan berharga dalam pembahasan rancangan peraturan pemerintah (RPP) sebagai peraturan pelaksana dari UU PDP yang masih berlangsung saat ini.

Peran strategis PDN

Perlu diketahui bahwa PDN yang tersedia saat ini merupakan layanan pusat data sementara berbasis Cloud yang digunakan untuk membantu konsolidasi data pemerintah secara nasional sekaligus mendukung percepatan berbagai layanan publik sambil menunggu selesainya pembangunan PDN di empat lokasi di Indonesia (Cikarang, Batam, IKN, dan Labuan Bajo).

Dalam beberapa tahun terakhir, PDN sementara itu telah digunakan oleh sekurang-kurangnya 56 kementerian/lembaga (K/L) pusat, 13 pemerintah provinsi, 105 pemerintah kabupaten, dan 31 pemerintah kota (laman Kemenkominfo, data pengguna PDN 2020-2021).

PDN itu dimanfaatkan sebagai media penempatan, penyimpanan dan pengolahan data, serta pemulihan data setiap instansi pemerintah, di mana di dalamnya mencakup data pribadi warga negara Indonesia.

Dalam konteks UU PDP, keberadaan PDN yang dikelola Kemkominfo akan menjadi jantung utama dalam pengendalian dan pemrosesan data pribadi warga negara yang diselenggarakan pemerintah. Dengan demikian, keberhasilan implementasi UU PDP sendiri akan sangat bergantung dari keandalan PDN dalam melindungi kedaulatan data warga negara yang dikelolanya.

Berdasarkan data Badan Siber dan Sandi Negara (BSSN), sepanjang 2023 telah terjadi 279,84 juta serangan siber di Indonesia. Angka ini sebenarnya lebih baik dari tahun sebelumnya yang mencapai 700 juta serangan. Banyaknya kejadian serangan siber itu menggambarkan besarnya potensi ancaman terhadap PDN dan tingginya ancaman risiko kegagalan dalam pelindungan data pribadi. Ini akan menjadi tantangan tersendiri bagi pemerintah dalam mengimplementasikan UU PDP dan melindungi PDN sebagai salah satu alat utama dalam pelindungan data pribadi.

PDN saat ini lazim digunakan sejumlah negara sebagai bagian dari upaya menciptakan *data sovereignty* (kedaulatan data nasional) negara tersebut. Perspektif ini jelas penting dalam konteks ketahanan nasional.

Namun, di sisi lain, PDN juga berperan penting sebagai penjaga atau pelindung data pribadi (*data privacy*). Kedua perspektif penting ini harus dijaga dan dikelola dengan baik oleh pengelola PDN dalam mengimplementasikan hak privasi warga negara.

Kejadian gangguan PDN ini bisa menjadi pisau bermata dua bagi implementasi UU PDP pada Oktober nanti. Di satu sisi, peristiwa gangguan ini akan menjadi momentum untuk menunjukkan urgensi mengapa UU PDP harus segera diimplementasikan. Namun, di sisi lain, peristiwa ini juga bisa menimbulkan keraguan publik terhadap kapasitas pemerintah dalam mewujudkan *data privacy* bagi warga negara.

Keraguan ini harus segera dijawab agar tak berdampak luas terhadap kepercayaan masyarakat kepada pemberi layanan lain, tidak hanya pemerintah, tetapi juga korporasi/swasta yang juga dituntut menjaga keamanan data pribadi seluruh konsumennya.

Dalam hal ini, keseriusan para pengambil keputusan untuk segera mengungkap dan mengatasi gangguan PDN akan menjadi penentu utama kepercayaan publik terhadap keberhasilan implementasi UU PDP pada Oktober nanti.

Di sisi lain, keandalan dalam mengelola PDN juga akan menjadi bukti konkret sejauh mana negara mengedepankan *data privacy* sebagai bagian dari upaya mewujudkan hak warga negara sekaligus mewujudkan kedaulatan data sebagai bagian dari ketahanan nasional.