editorial

# KRISIS KEAMANAN DATA PUBLIK DAN URGENSI KEDAULATAN DATA DI ERA GOVERNANSI DIGITAL

Transformasi digital yang terjadi secara masif di Indonesia telah membawa perubahan mendasar dalam tata kelola pemerintahan dan pelayanan publik. Digitalisasi memang menawarkan berbagai keuntungan seperti efisiensi, transparansi, serta akses yang lebih mudah bagi masyarakat terhadap layanan pemerintah. Namun, di balik kemajuan tersebut, terdapat tantangan besar yang belum terselesaikan, yaitu krisis keamanan data publik. Berbagai insiden kebocoran data yang terjadi sepanjang tahun 2024 menjadi peringatan serius bahwa sistem keamanan informasi di Indonesia masih sangat rentan. Krisis ini bukan hanya berdampak pada aspek teknis, tetapi juga berpotensi mengganggu stabilitas politik, sosial, dan kepercayaan publik terhadap negaraPerubahan dan pergeseran nilai yang cepat memerlukan pendekatan bijak melalui tindakan yang konsisten dan berkelanjutan dalam berbagai bidang pembangunan. Hal ini penting untuk membangun kepercayaan masyarakat demi mencapai tujuan pembangunan nasional. Oleh karena itu, untuk mewujudkan pelayanan publik yang semakin baik dan terintegrasi, transformasi digital adalah langkah penting yang harus dilakukan. Melalui transformasi digital, pemerintah memiliki banyak peluang untuk meningkatkan efisiensi, efektivitas, transparansi dan kualitas pelayanan publik.

Setidaknya terdapat tiga insiden besar yang menyoroti lemahnya perlindungan data di Indonesia. Pertama, kebocoran data 4,7 juta Aparatur Sipil Negara (ASN) dari sistem Badan Kepegawaian Negara (BKN), di mana data sensitif seperti Nomor Induk Kependudukan (NIK), alamat rumah, hingga riwayat pekerjaan bocor dan diperjualbelikan di forum gelap. Celah keamanan yang dimanfaatkan peretas diketahui berasal dari SQL injection, yang seharusnya dapat dicegah dengan sistem audit dan pengawasan yang ketat. Kedua, serangan ransomware LockBit 3.0 terhadap Pusat Data Nasional Sementara (PDNS) yang menyebabkan lumpuhnya sejumlah layanan vital seperti imigrasi dan bea cukai. Ketiadaan backup sistem di banyak instansi membuat dampak serangan ini semakin luas dan merugikan. Ketiga, dugaan kebocoran data Nomor Pokok Wajib Pajak (NPWP) yang melibatkan data jutaan wajib pajak termasuk pejabat tinggi negara, memperlihatkan kegagalan pemerintah dalam memberikan klarifikasi serta transparansi kepada publik.

Ketiga kasus tersebut mengindikasikan bahwa keamanan data belum menjadi prioritas nasional. Pengelolaan data di Indonesia masih bersifat sektoral, minim koordinasi, serta belum memiliki standar nasional yang kuat dan terintegrasi. Ketika terjadi serangan siber atau insiden kebocoran, respons dari pemerintah cenderung lamban, tidak terkoordinasi, dan kurang terbuka kepada publik. Kondisi ini semakin diperparah oleh rendahnya akuntabilitas lembaga-lembaga publik. Hampir tidak pernah terjadi evaluasi menyeluruh atau penjatuhan sanksi tegas terhadap pihak yang lalai. Biasanya, tanggung jawab hanya diakui secara simbolik tanpa disertai reformasi sistemik atau transparansi audit.

Undang-Undang Perlindungan Data Pribadi (UU PDP) yang telah disahkan pada tahun 2022 sejatinya merupakan langkah awal yang baik. UU ini mengamanatkan pembentukan Lembaga Perlindungan Data Pribadi (LPPDP) yang bersifat independen. Namun, hingga pertengahan 2025, lembaga tersebut belum operasional sepenuhnya dan masih berada di bawah kewenangan Kementerian Komunikasi dan Informatika (Kominfo), yang menimbulkan konflik kepentingan. Akibatnya, pengawasan terhadap pelanggaran data tidak berjalan efektif, dan masyarakat tidak memiliki mekanisme yang jelas untuk mengajukan keluhan, meminta penghapusan data, ataupun menuntut kompensasi atas pelanggaran haknya.

Dalam konteks ini, konsep data sovereignty atau kedaulatan data menjadi sangat relevan. Data sovereignty menekankan pentingnya negara memiliki kontrol penuh atas data warganya termasuk lokasi penyimpanan fisik, yurisdiksi hukum yang mengaturnya, serta mekanisme perlindungan dan akses data tersebut. Sayangnya, konsep ini belum menjadi fondasi utama dalam kebijakan digital Indonesia. Masih banyak data strategis pemerintah yang disimpan di layanan cloud milik perusahaan asing seperti AWS, Google Cloud, atau Microsoft Azure. Hal ini membuka celah risiko besar, karena data tersebut berada di bawah yurisdiksi hukum negara asal penyedia layanan, seperti CLOUD Act di Amerika Serikat, yang memungkinkan akses oleh otoritas asing.

Penerapan prinsip data localization, yakni kewajiban menyimpan seluruh data strategis di server fisik dalam negeri dengan standar keamanan tinggi, menjadi solusi mendesak. Namun, hal ini tidak cukup dilakukan secara administratif saja, melainkan harus disertai dengan audit keamanan rutin oleh lembaga independen, sistem backup harian, prosedur pemulihan bencana (disaster recovery), serta penggunaan teknologi enkripsi end-to-end. Transparansi dalam penanganan insiden juga mutlak diperlukan. Pemerintah wajib mengumumkan insiden kebocoran, hasil investigasi, serta langkah mitigasi secara terbuka kepada publik. Selain itu, pelibatan masyarakat sipil, akademisi, dan sektor swasta dalam penyusunan kebijakan keamanan data sangat diperlukan untuk membangun kepercayaan dan legitimasi publik.

Krisis ini membawa dampak serius dalam berbagai aspek. Di bidang politik, data yang bocor dapat dimanfaatkan untuk kampanye hitam, pemerasan, atau manipulasi opini publik. Dalam ranah sosial, penyebaran informasi sensitif yang tidak terkendali dapat memicu hoaks dan memperdalam polarisasi di masyarakat. Dampak ekonomi pun tidak kalah besar: perusahaan atau instansi yang menjadi korban serangan siber harus menanggung biaya pemulihan yang tinggi, serta kehilangan kepercayaan dari mitra maupun investor. Lebih jauh, jika masyarakat merasa data pribadinya tidak aman, maka mereka akan enggan berpartisipasi dalam program digital pemerintah seperti layanan e-government, smart city, maupun pemilu elektronik, yang pada akhirnya menghambat kemajuan transformasi digital nasional.

Oleh karena itu, reformasi tata kelola digital yang berlandaskan pada kedaulatan data menjadi sangat mendesak. Langkah pertama adalah mempercepat pembentukan LPPDP yang benar-benar independen, dengan kewenangan penuh untuk menginvestigasi, mengaudit, dan memberi sanksi kepada pelanggar, termasuk lembaga pemerintah. Kedua, penerapan kebijakan data localization harus dilakukan secara konsisten, dengan memastikan seluruh data warga disimpan di server nasional yang memenuhi standar keamanan internasional. Ketiga, sistem digital pemerintah perlu diaudit secara berkala oleh pihak ketiga yang kompeten dan independen, dengan mengadopsi arsitektur zero trust, otentikasi multi-faktor, dan sistem pemantauan real-time.

Pemerintah juga harus meningkatkan literasi digital masyarakat agar mereka memahami hak-hak perlindungan data pribadi dan bisa melapor apabila terjadi pelanggaran. Selain itu, saluran pengaduan harus dibuat sederhana dan aman, serta memberikan perlindungan terhadap pelapor. Transparansi menjadi kunci dalam membangun kepercayaan: setiap kebocoran data harus diumumkan secara terbuka, disertai dengan langkah mitigasi yang jelas dan akuntabel. Publik juga harus dilibatkan dalam proses perumusan kebijakan data, agar kebijakan yang dihasilkan tidak hanya top-down, tetapi juga responsif terhadap kebutuhan nyata masyarakat.

Tentu saja, implementasi dari seluruh langkah tersebut tidak mudah. Tantangan utama datang dari tumpang tindih kewenangan antarinstansi seperti BSSN, Kominfo, dan lembaga teknis lain, yang belum memiliki mekanisme koordinasi yang efektif. Keterbatasan anggaran dan infrastruktur juga menjadi kendala besar, karena pengembangan server nasional, pelatihan SDM, dan audit independen memerlukan investasi jangka panjang. Budaya birokrasi yang masih defensif terhadap audit dan kritik publik turut menghambat proses reformasi. Belum lagi, ketergantungan pada vendor teknologi asing membuat proses migrasi ke sistem dalam negeri menjadi mahal dan rumit secara teknis.

Meskipun begitu, tantangan ini tidak boleh dijadikan alasan untuk menunda perubahan. Justru, krisis kebocoran data yang berulang kali terjadi harus dimanfaatkan sebagai momentum untuk mempercepat reformasi sistemik di bidang keamanan digital. Tanpa pembenahan menyeluruh, Indonesia akan terus berada dalam situasi rentan yang membahayakan masa depan demokrasinya.

Sebagai penutup, krisis keamanan data publik merupakan pengingat bahwa transformasi digital tidak cukup hanya dengan membangun infrastruktur dan platform digital. Tanpa fondasi keamanan dan kedaulatan data yang kokoh, digitalisasi justru bisa menjadi ancaman baru yang lebih besar. Oleh karena itu, pemerintah harus menjadikan perlindungan data sebagai agenda prioritas nasional, bukan sekadar isu teknis sektoral. Kedaulatan data adalah hak warga negara dan sekaligus tanggung jawab negara untuk menjaganya.

**Cindy Sabrina**[1]

[1] Mahasiswi Fakultas Ilmu Sosial dan Ilmu Pemerintahan, UIN Ar-Raniry Banda Aceh

**Referensi**


Antaranews. (2024, September 23). DJP bantah adanya kebocoran data NPWP. https://www.antaranews.com/berita/4347351/djp-bantah-adanya-kebocoran-data-npwp

Artikel Pajakku. (2024, September 19). 6 juta data NPWP diduga bocor, ini respons DJP. https://artikel.pajakku.com/6-juta-data-npwp-diduga-bocor-ini-respon-djp/

CISSReC. (2024, Agustus 22). Analisis insiden kebocoran data ASN dari BKN. https://www.cissrec.org/insiden-bkn/

Detik.com. (2024, Agustus 21). 4,7 juta data ASN diduga bocor, BKN imbau segera ganti password. https://www.detik.com/sumbagsel/berita/d-7485273/4-7-juta-data-asn-diduga-bocor-bkn-imbau-segera-ganti-password

IDN Times. (2024, Agustus 22). Benarkah data pribadi ASN bocor hingga dijual?. https://www.idntimes.com/news/indonesia/cek-fakta-benarkah-data-pribadi-asn-bocor-hingga-dijual

Kominfo Lhokseumawe. (2024, Juli 5). BSSN identifikasi PDNS diserang ransomware LockBit 3.0. https://kominfo.lhokseumawekota.go.id/berita/read/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware-20240705172015016 5

Pointstar Indonesia. (2024, Juli 1). Apa itu ransomware LockBit dan bagaimana mencegahnya? https://www.pointstar.co.id/data-security/lockbit-ransomware/

Reuters. (2024, Juni 28). Bulk Indonesia data hit by cyberattack, not backed up, officials say. https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28

Tempo.co. (2024, September 20). 6 juta data NPWP bocor, diduga milik pejabat tinggi negara. https://www.tempo.co/ekonomi/6-juta-data-npwp-bocor-diduga-milik-jokowi-sri-mulyani-dan-zulhas-diperjualbelikan-seharga-rp-152-juta

Zettagrid Indonesia. (2024, Juli 5). Belajar dari serangan ransomware LockBit 3.0 ke PDN: Pentingnya backup. https://www.zettagrid.id/blog/2025/06/05/belajar-dari-serangan-ransomware-lockbit-3-0-ke-pdn-pentingnya-solusi-veeam-cloud-connect-backup