URGENSI PERLINDUNGAN DATA INFORMASI PEMERINTAH DI ERA DIGITAL

Kamis, 14 Agustus 2025 - kalsel

Belakangan ini, masyarakat Indonesia dihebohkan dengan kasus pembobolan data informasi pemerintah. Peristiwa tersebut menambah panjang daftar kasus serupa dalam beberapa tahun terakhir. Kebocoran data ini bukan hanya mencoreng wajah pemerintah, tetapi juga menimbulkan kekhawatiran serius mengenai keamanan dan privasi data warga negara.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), yang disahkan pada 17 Oktober 2022, hadir sebagai wujud komitmen negara menjaga hak privasi dan keamanan informasi individu. Namun, pertanyaan besar muncul di tengah masyarakat: bagaimana sistem pemerintah yang digadang canggih bisa ditembus oleh peretasan ilegal hingga berujung pemerasan sebesar 8 juta USD?

Merujuk Pasal 1 ayat 2 UU PDP, perlindungan data pribadi mencakup segala upaya melindungi individu dalam pemrosesan atau pengelolaan data untuk menjamin hak konstitusional Subjek Data Pribadi. Artinya, pemerintah dituntut mampu menyelesaikan persoalan ini secara tuntas agar kerugian tidak semakin meluas. Situasi ini wajar membuat masyarakat semakin cemas terhadap keamanan data pribadinya.

Pembobolan data pemerintah memiliki implikasi serius. Informasi yang dicuri bisa disalahgunakan untuk pencurian identitas, penipuan finansial, penyalahgunaan informasi pribadi, hingga ancaman terhadap keamanan nasional. Data pribadi yang mencakup nomor identitas, alamat, dan informasi sensitif lainnya dapat dimanfaatkan pihak tidak bertanggung jawab untuk tindakan kriminal.

Bagi individu, kebocoran data bisa berarti kerugian finansial, hilangnya privasi, hingga beban psikologis yang berat. Rasa tidak aman dalam bertransaksi digital akan menghantui korban. Sementara bagi pemerintah, kejadian ini menimbulkan pertanyaan mengenai kompetensi dalam mengelola data sensitif. Kepercayaan publik terhadap kemampuan pemerintah menjadi taruhannya. Jika terus terguncang, dampaknya bisa merembet pada aspek lain pemerintahan dan hubungan pemerintah dengan masyarakat.

Salah satu penyebab utama pembobolan data adalah lemahnya sistem keamanan siber. Di era digital yang berkembang pesat, teknologi yang digunakan pemerintah sering tertinggal dari metode serangan yang semakin canggih. Peretas selalu mencari celah dan memanfaatkan kelemahan sistem untuk mencuri data. Hal ini menegaskan pentingnya investasi dalam teknologi keamanan mutakhir. Sistem harus diperbarui dan disesuaikan dengan ancaman yang berkembang. Enkripsi data, *firewall* , dan sistem deteksi intrusi harus diimplementasikan secara berkelanjutan, disertai audit keamanan rutin untuk menemukan dan menutup celah yang ada.

Namun, teknologi saja tidak cukup. Sumber daya manusia yang mengelola sistem juga harus memiliki kompetensi dan kesadaran tinggi terhadap ancaman siber. Pelatihan serta peningkatan kapasitas pegawai pemerintah di bidang teknologi informasi perlu menjadi prioritas. Setiap individu harus memahami potensi serangan, mulai dari *phishing*, *malware*, hingga social engineering, serta mengetahui langkah yang harus dilakukan jika terjadi insiden.

Selain teknologi dan SDM, regulasi dan kebijakan yang tegas juga diperlukan. Pemerintah harus menetapkan standar keamanan data yang tinggi dan memastikan kepatuhan terhadapnya. Pengawasan dan penegakan hukum yang ketat wajib diterapkan terhadap pelanggaran, baik oleh pihak internal maupun eksternal. UU PDP harus mampu memberikan perlindungan memadai bagi warga negara, disertai sanksi berat bagi pelanggarnya. Transparansi pemerintah dalam menangani insiden kebocoran data juga sangat penting untuk membangun kembali kepercayaan publik.

Regulasi tersebut harus mencakup penyimpanan data, pembatasan akses hanya untuk pihak berwenang, serta prosedur

respons insiden yang jelas agar kebocoran dapat ditangani cepat dan efektif.

Masyarakat pun memiliki peran penting dalam menjaga keamanan data. Edukasi mengenai pentingnya kerahasiaan data pribadi harus ditingkatkan. Warga perlu memahami cara membuat kata sandi yang kuat, mengenali email atau pesan mencurigakan, serta langkah yang harus diambil jika data pribadi bocor. Penggunaan autentikasi dua faktor dan enkripsi data juga perlu digalakkan. Kesadaran ini harus terus didorong melalui kampanye edukasi dan sosialisasi.

Selain itu, kerja sama internasional juga sangat penting. Ancaman siber bersifat lintas negara, sehingga pemerintah perlu menjalin kemitraan dengan negara lain dan organisasi internasional dalam berbagi informasi maupun teknologi keamanan. Dukungan terhadap inisiatif global dalam pengembangan standar keamanan siber juga diperlukan agar perlindungan data dapat diterapkan secara universal.

Kasus pembobolan data pemerintah yang mencuat belakangan ini seharusnya menjadi momentum bagi pemerintah dan masyarakat untuk berbenah. Keamanan siber bukanlah tanggung jawab satu pihak, melainkan tanggung jawab bersama.

Dengan meningkatkan teknologi, memperkuat kapasitas sumber daya manusia, mempertegas regulasi, serta menumbuhkan kesadaran masyarakat, lingkungan digital yang aman dan terpercaya dapat terwujud. Pemerintah juga harus bergerak cepat memulihkan kepercayaan publik dan memastikan kasus serupa tidak terulang. Langkah-langkah itu mencakup investasi dalam sistem keamanan mutakhir, pelatihan berkelanjutan, penerapan regulasi yang ketat, edukasi publik, serta peningkatan kerja sama internasional.

Dengan upaya tersebut, sistem perlindungan data informasi pemerintah dan data pribadi warga negara akan lebih kokoh. Kepercayaan publik pun dapat dipulihkan dan dijaga. Hanya dengan kerja sama erat antara pemerintah dan masyarakat, tantangan keamanan siber di era digital dapat dihadapi dengan lebih efektif.

Oleh: Viviana Melinda

Insan Ombudsman Kalsel