BAB V

KESIMPULAN

A. Kesimpulan

Hasil analisis pada Bab 4 menunjukkan bahwa kebocoran data Daftar Pemilih Tetap (DPT) tahun 2023 mencerminkan masih lemahnya pelaksanaan regulasi perlindungan data pribadi di Indonesia, meskipun telah ada payung hukum berupa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Permasalahan utama yang ditemukan adalah belum optimalnya penerapan prinsip kerahasiaan, integritas, dan ketersediaan data oleh Komisi Pemilihan Umum (KPU) sebagai pengendali data, serta minimnya pelaksanaan kewajiban notifikasi terhadap pemilik data yang terdampak insiden kebocoran.

Selain itu, ketiadaan pedoman teknis dan lembaga pengawas resmi mengakibatkan pelaksanaan UU PDP tidak berjalan secara efektif. Ketidakmampuan KPU dalam memberikan perlindungan menyeluruh terhadap data DPT mengindikasikan adanya kelalaian yang perlu segera diatasi melalui reformasi tata kelola data, penyusunan peraturan turunan yang mendukung, serta penguatan kapasitas teknis dan kelembagaan.

Dalam konteks pembanding, kasus serupa di Filipina menunjukkan penanganan yang lebih terstruktur, termasuk langkah transparansi dalam notifikasi publik, penegakan hukum terhadap pelaku kebocoran, dan perbaikan infrastruktur keamanan data. Hal ini menjadi pelajaran penting bagi Indonesia untuk segera meningkatkan efektivitas pengelolaan data pribadi melalui kolaborasi antara pemerintah, lembaga terkait, dan masyarakat.

Badan Siber dan Sandi Negara (BSSN) merekomendasikan sejumlah langkah strategis untuk memperkuat keamanan data di lingkungan Komisi Pemilihan Umum (KPU) guna memastikan pelaksanaan Pemilu yang aman dan andal. Rekomendasi ini meliputi tindakan preventif seperti pengaturan ulang kata sandi secara berkala,

pelaksanaan *Vulnerability Assessment* (VA) dan penetration test, serta penyusunan metadata untuk data sensitif. Selain itu, penerapan solusi teknologi canggih, seperti *Next-Generation Endpoint Protection* (EDR) *dan Multi-Factor Authentication* (MFA), menjadi prioritas untuk mencegah akses tidak sah.

BSSN juga menekankan pentingnya backup site dan enkripsi pada database server untuk menjaga kontinuitas operasional serta integritas data. Penyusunan rencana dan simulasi *Business Continuity Plan* (BCP) serta *Disaster Recovery Plan* (DRP) secara berkala juga dinilai krusial dalam menghadapi potensi insiden atau bencana.

Dari sisi regulasi, BSSN mendorong KPU untuk mengacu pada peraturan terkait, seperti Peraturan Presiden Nomor 82 Tahun 2022 dan sejumlah peraturan BSSN lainnya, termasuk yang mengatur pengamanan infrastruktur informasi vital dan pengelolaan Sistem Pemerintahan Berbasis Elektronik (SPBE). BSSN juga merekomendasikan peningkatan kapabilitas sumber daya manusia di bidang keamanan siber serta audit keamanan secara berkala untuk memastikan kepatuhan dan kematangan keamanan siber.

Keseluruhan langkah ini bertujuan untuk memperkokoh tata kelola keamanan data KPU, memastikan perlindungan data pemilih dari ancaman kebocoran, dan mendukung proses Pemilu yang transparan, andal, dan berkelanjutan.

B. Saran Praktis

Untuk pemerintah, terkhususnya lembaga Komisi Pemilihan Umum (KPU) sebagai yang bertanggung jawab sebagai pengendali data agar disarankan untuk lebih memperkuat sistem keamanan data mereka. Pengimplementasian enkripsi dan juga notifikasi bagi pemilih terdaftar juga sudah harus ditingkatkan penggunaanya. Hal tersebut dilakukan demi mencegah kembali terjadinya kasus kebocoran data.

Lalu untuk staff penyelenggara pemilu juga perlu dilakukan pelatihan secara berkala terkhususnya mengenai perlindungan data pribadi, agar mereka paham mengenai standar operasional prosedur dalam menangani data pemilih.

Dan untk masyarakat disarankan agar lebih berhati-hati dalam memberikan informasi pribadinya memalui platform online. Dan masyarakat juga harus lebih aktif dalam melaporkan ke pihak berwajib jika menemukan indikasi penyalahgunaan data.

C. Saran Teoritis

Disarankan untuk peneliti berikutnya agar dapat meneliti kasus ini lebih jauh. Terutama mengenai aspek legal terkait perlindungan data pribadi dengan membandingkannya ke nagara lain. Penelitian selanjutnya juga dianjurkan untuk memperdalam kajian lintas-disiplin dengan mengintegrasikan pendekatan teknis, dan hukum dalam menganalisis kebocoran data pribadi. Hal ini bertujuan merumuskan kerangka konseptual yang komprehensif sehingga tidak hanya memetakan celah keamanan teknologi, tetapi juga mengeksplorasi dinamika regulasi serta perilaku pengguna dalam konteks digital yang terus berkembang.