

ABSTRAK

Penelitian ini bertujuan untuk mengkaji kepemimpinan keamanan siber KPU RI dalam upaya perlindungan data pribadi pemilih pemilu pada Sistem Informasi Daftar Pemilih (SIDALIH). Penerapan teknologi informasi dalam pemilu menimbulkan adanya ancaman serangan siber terhadap sistem informasi yang digunakan, salah satunya SIDALIH. Pengalaman serangan siber terhadap pelaksanaan Pemilu di Indonesia menjadikan isu keamanan siber menjadi penting, terkhusus berkaitan dengan perlindungan data pribadi pemilih. Kompleksitas serangan siber yang terus meningkat mempertegas bahwa organisasi hari ini penting untuk memiliki peran aktor kepemimpinan yang baik dan tata kelola komunikasi kepemimpinan yang tanggap dan fokus terhadap keamanan siber. Berdasarkan fenomena tersebut, pertanyaan penelitian ini adalah bagaimana kepemimpinan keamanan siber KPU menjaga keamanan data pemilih dalam menerapkan SIDALIH (Sistem Informasi Daftar Pemilih) di Pemilu 2024. Peneliti menggunakan konseptual teori kepemimpinan keamanan siber yang dicetuskan oleh Ozkaya yang terdiri dari lima pilar. Metodologi yang digunakan adalah paradigma interpretif dengan jenis penelitian deskriptif kualitatif, serta dengan menggunakan metode studi kasus tunggal. Temuan penelitian yang didasarkan pada lima pilar kepemimpinan keamanan siber menunjukkan bahwa untuk meningkatkan keamanan data pemilih, diperlukan perhatian yang lebih baik terhadap aspek kepemimpinan dan tata kelola komunikasi, transparansi dan pemahaman publik, integrasi regulasi, strategi yang baik, kolaborasi antar lembaga, dan alokasi sumber daya yang memadai.

Kata Kunci: Kepemimpinan keamanan siber, Data Pemilih, SIDALIH, Teknologi Pemilu.

ABSTRACT

This research aims to examine the cybersecurity leadership of the General Election Commission of Indonesia (KPU RI) in protecting the personal data of voters in the Voter Registration Information System (SIDALIH). The implementation of information technology in elections has led to the emergence of cyber threats to the information systems used, including SIDALIH. The experience of cyber attacks during the implementation of elections in Indonesia has made cybersecurity a crucial issue, especially regarding the protection of voters' personal data. The increasing complexity of cyber attacks emphasizes the importance for organizations today to have responsive and focused leadership and communication governance, particularly through the implementation of cybersecurity leadership. Based on this phenomenon, the research question is how KPU's cybersecurity leadership ensures the security of voter data in implementing SIDALIH in the 2024 elections. The researcher utilizes the conceptual theory of Cybersecurity Leadership proposed by Ozkaya, consisting of five pillars. The methodology employed is an interpretive paradigm with a qualitative descriptive research design, using a single case study method. The research findings based on the five pillars of cybersecurity leadership indicate that to enhance the security of voter data, greater attention is needed towards leadership and communication governance aspects, transparency and public understanding, regulatory integration, sound strategies, interagency collaboration, and adequate resource allocation.

Keywords: *Cybersecurity Leadership*, SIDALIH, Election Technology, Voters Data.