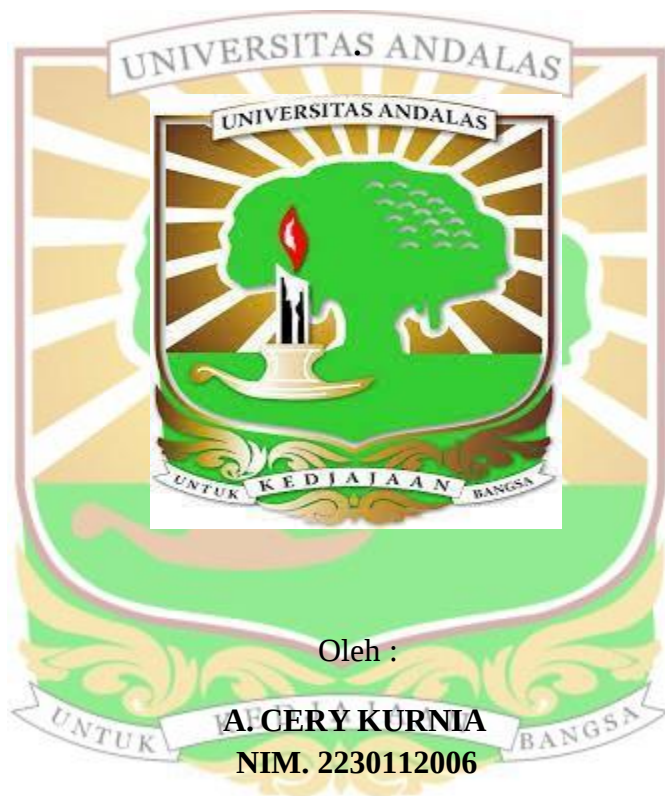


**PENGATURAN PENGELOLAAN BIG DATA DALAM
ANCAMAN TERHADAP KEAMANAN SIBER: SUATU KAJIAN
PENEGAKAN KEDAULATAN DIGITAL DI INDONESIA**

Disertasi

Diajukan untuk memenuhi persyaratan
dalam rangka memperoleh gelar Doktor Hukum



Oleh :

A. CERY KURNIA
NIM. 2230112006

**PROGRAM STUDI DOKTOR HUKUM
FAKULTAS HUKUM
UNIVERSITAS ANDALAS
PADANG
2026**

ABSTRAK

PENGATURAN PENGELOLAAN BIG DATA DALAM ANCAMAN TERHADAP KEAMANAN SIBER; SUATU KAJIAN KEDAULATAN DIGITAL DI INDONESIA

(A. Cery Kurnia, 2230112006, Program Studi Doktor Hukum Fakultas Hukum
Universitas Andalas, Halaman 456, 2026)

Perkembangan teknologi, informasi dan komunikasi selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Interaksi dan komunikasi data secara global berakibat tidak hanya pada perkembangan teknologi, akan tetapi berdampak juga pada penyalahgunaan data, pencurian data pribadi, penjualan data pribadi, penipuan dan lain-lain. Maraknya kasus-kasus kebocoran data di ruang siber tidak lepas dari transformasi data dari konvensional ke digital. Transformasi digital telah menempatkan big data sebagai aset strategis nasional yang memerlukan pengelolaan dan perlindungan hukum secara komprehensif dari ancaman-ancaman keamanan siber. Kajian penegakan kedaulatan digital di Indonesia masih belum terkoordinasi dengan baik ketika dihadapkan dengan kasus-kasus terkait big data. Penelitian ini mengkaji tentang bagaimana pengaturan hukum pengelolaan big data dalam menghadapi ancaman keamanan siber, bagaimana kajian penegakan kedaulatan digital, bagaimana model pengaturan hukum yang ideal untuk melindungi big data guna menegakkan kedaulatan digital di Indonesia. Penelitian ini bersifat normatif dengan pendekatan perundang-undangan, komparatif dan konseptual, berlandaskan teori kedaulatan negara, kepastian hukum, dan hak atas privasi. Hasil penelitian menunjukkan bahwa pengaturan hukum pengelolaan big data di Indonesia masih bersifat fragmentatif dan belum terintegrasi secara koheren. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebagai *lex generalis* belum optimal karena ketiadaan Peraturan Pemerintah pelaksana dan belum terbentuknya Lembaga Pelindungan Data Pribadi sebagai otoritas pengawas independen. Pengaturan masih bersifat reaktif-represif belum mengadopsi proaktif-preventif berbasis risiko. Ketiadaan undang-undang keamanan dan ketahanan siber menempatkan Indonesia dalam kondisi *vacuum of norm*. Penegakan kedaulatan digital menghadapi tantangan multidimensional mencakup aspek kelembagaan, infrastruktur, dan transfer data lintas batas. Model pengaturan hukum yang diusulkan bersifat integratif-komprehensif dengan pendekatan proaktif-transformatif-progresif berbasis risiko, mencakup arsitektur regulasi tiga tingkatan, pembentukan Lembaga Pelindungan Data Pribadi yang independen, penguatan BSSN, pembentukan Tim Tanggap Insiden Siber berjenjang, serta model penegakan hukum berlapis dengan sanksi proporsional. Implementasi dilakukan bertahap melalui kolaborasi antara pemerintah, akademisi, pelaku usaha, dan komunitas.

Kata Kunci: Big Data, Keamanan Siber, Kedaulatan Digital, Pelindungan Data Pribadi, Penegakan Hukum

ABSTRACT

REGULATION OF THE MANAGEMENT OF BIG DATA IN MITIGATING THREAD OF CYBERSECURITY THREATS; A STUDY ON DIGITAL SOVEREIGNTY IN INDONESIA

**(A. Cery Kurnia, 2230112006, Doctoral of Law Program, Faculty of Law,
Andalas University, Pages 456, 2026)**

*The development of information, communication, and technology not only contributes to improving human welfare, progress, and civilization, but also serves as an effective means of combating illegal acts. Global data interaction and communication have resulted not only in technological advancement but also in data misuse, personal data theft, the sale of personal data, fraud, and other issues. The rise in data leaks in cyberspace is inextricably linked to the transformation of data from conventional to digital. Digital transformation has positioned big data as a strategic national asset that requires comprehensive legal management and protection from cybersecurity threats. Studies on the enforcement of digital sovereignty in Indonesia are still not well coordinated when faced with cases related to big data. This research examines how the legal regulations for big data management are regulated in the face of cybersecurity threats, how the study of digital sovereignty enforcement is carried out, and what the ideal legal regulation model is for protecting big data in order to uphold digital sovereignty in Indonesia. This research is normative in nature, using statutes, comparative, and conceptual approaches, grounded in the theories of state sovereignty, legal certainty, and the right to privacy. This results found that the legal regulations for big data management in Indonesia remain fragmented and not yet coherently integrated. Law Number 27 of 2022 concerning Personal Data Protection, as a *lex generalis*, is not yet optimal due to the absence of implementing Government Regulations and the lack of a Personal Data Protection Agency as an independent supervisory authority. Regulations remain reactive-repressive, yet have not adopted a risk-based proactive-preventive approach. The absence of cybersecurity and resilience legislation places Indonesia in a norm vacuum. Enforcing digital sovereignty faces multidimensional challenges encompassing institutional aspects, infrastructure, and cross-border data transfer. The proposed legal regulatory model is integrative and comprehensive, with a proactive, transformative, and progressive, risk-based approach. It encompasses a three-tier regulatory architecture, the establishment of an independent Personal Data Protection Agency (BSSN), the strengthening of a tiered Cyber Incident Response Team, and a multi-layered law enforcement model with proportional sanctions. Implementation will be carried out in stages through a collaboration between the government, academics, business actors, and the community.*

Keywords: Big Data, Cybersecurity, Digital Sovereignty, Personal Data Protection, Law Enforcement