

ABSTRAK

TANGGUNG JAWAB NEGARA TERHADAP KEAMANAN DATA PESERTA BPJS KESEHATAN DALAM PERSPEKTIF HAK ASASI MANUSIA

Oleh

Beni Prawira Candra Jaya

Digitalisasi pelayanan kesehatan melalui program Jaminan Kesehatan Nasional (JKN) menempatkan BPJS Kesehatan sebagai pengelola data pribadi lebih dari 250 juta penduduk Indonesia. Data ini mencakup informasi sensitif seperti identitas peserta, riwayat penyakit, dan informasi medis lain yang secara hukum dikategorikan sebagai data pribadi yang dilindungi. Namun, kebocoran data 279 juta peserta BPJS Kesehatan pada tahun 2021 menunjukkan adanya kelemahan serius dalam tata kelola keamanan data dan memunculkan persoalan mengenai tanggung jawab negara dalam melindungi hak atas privasi sebagai bagian dari hak asasi manusia. Secara normatif, UUD 1945, UU HAM, UU BPJS, UU Kesehatan, UU ITE, dan UU Perlindungan Data Pribadi telah menetapkan kewajiban negara untuk menghormati, melindungi, dan memenuhi hak atas privasi, namun insiden kebocoran data menunjukkan adanya kesenjangan antara regulasi dan implementasi.

Penelitian ini bertujuan untuk menganalisis konsep tanggung jawab negara terhadap keamanan data peserta BPJS Kesehatan dalam perspektif hak asasi manusia dan mengevaluasi mekanisme pertanggungjawaban negara ketika terjadi kebocoran data peserta. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, pendekatan kasus, dan pendekatan perbandingan dengan *General Data Protection Regulation* (GDPR) Uni Eropa. Sumber data meliputi bahan hukum primer, sekunder, serta dokumen relevan terkait tata kelola data pribadi dan keamanan siber nasional.

Hasil penelitian menunjukkan bahwa negara berkewajiban menghormati, melindungi, dan memenuhi hak atas privasi melalui kerangka regulasi yang memadai, mekanisme pengawasan, dan tindakan preventif untuk mencegah terjadinya pelanggaran data. Namun dalam praktiknya, kebocoran data BPJS Kesehatan tahun 2021 mengindikasikan lemahnya penerapan prinsip *due diligence*, kurangnya ketahanan data, serta belum optimalnya koordinasi antar lembaga seperti BPJS Kesehatan, Kominfo, dan BSSN. Selain itu, belum adanya otoritas independen seperti Komisi Perlindungan Data Pribadi menyebabkan mekanisme pertanggungjawaban negara belum berjalan efektif. Dibandingkan dengan GDPR yang memiliki standar penegakan ketat, mekanisme notifikasi insiden cepat, dan kewajiban perlindungan data berbasis risiko, sistem nasional Indonesia masih bersifat reaktif dan fragmentaris.

Kesimpulannya, negara secara normatif memiliki tanggung jawab yang kuat untuk melindungi data peserta BPJS Kesehatan sebagai bagian dari hak atas privasi. Namun implementasi tanggung jawab tersebut belum optimal karena lemahnya infrastruktur hukum, pengawasan, dan ketahanan sistem elektronik. Penelitian ini merekomendasikan penguatan regulasi turunan UU PDP, pembentukan Komisi PDP yang independen, penerapan standar keamanan sekilas ISO 27001 bagi penyelenggara data kesehatan, peningkatan mekanisme pengawasan, serta optimalisasi penerapan SMKI berbasis siklus PDCA untuk memastikan perlindungan data yang lebih komprehensif dan berkelanjutan.

Kata Kunci: Tanggung Jawab Negara, Keamanan Data, BPJS Kesehatan, Hak Asasi Manusia

ABSTRACT

THE STATE'S RESPONSIBILITY FOR THE DATA SECURITY OF BPJS KESEHATAN PARTICIPANTS FROM A HUMAN RIGHTS PERSPECTIVE

By

Beni Prawira Candra Jaya

The digitalization of health services through the National Health Insurance (JKN) program positions BPJS Kesehatan as the controller of personal data belonging to more than 250 million Indonesians. This data includes sensitive information such as participant identities, medical histories, and other health-related details that are legally categorized as protected personal data. However, the 2021 data breach involving 279 million BPJS Kesehatan participants revealed significant weaknesses in data security governance and raised fundamental questions regarding the State's responsibility to safeguard the right to privacy as a component of human rights. Normatively, UUD 1945, UU HAM, UU BPJS, UU Kesehatan, UU ITE, and UU PDP impose obligations on the State to respect, protect, and fulfill the right to privacy, yet the breach indicates a considerable gap between regulation and implementation.

This study aims to analyze the concept of State responsibility for the security of BPJS Kesehatan participants' data within a human rights framework and to evaluate the mechanisms of State accountability when a data breach occurs. This research employs a normative juridical method through statutory, case, and comparative approaches, including comparison with the European Union's General Data Protection Regulation (GDPR). Data sources consist of primary and secondary legal materials as well as relevant documents on personal data governance and national cybersecurity frameworks.

The findings indicate that the State is obligated to respect, protect, and fulfill the right to privacy through adequate regulatory frameworks, supervisory mechanisms, and preventive measures to avoid data violations. In practice, however, the 2021 BPJS Kesehatan data breach demonstrates weak implementation of due diligence principles, insufficient data resilience, and suboptimal coordination among key institutions such as BPJS Kesehatan, the Ministry of Communication and Informatics, and the National Cyber and Crypto Agency. Furthermore, the absence of an independent authority such as the Personal Data Protection Commission has resulted in ineffective State accountability mechanisms. Compared to the GDPR, which provides stringent enforcement standards, rapid incident notification procedures, and risk-based data protection obligations, Indonesia's national system remains reactive and fragmented.

In conclusion, the State normatively holds a strong responsibility to protect BPJS Kesehatan participants' data as part of the right to privacy. However, the implementation of this responsibility remains suboptimal due to weaknesses in legal infrastructure, oversight, and electronic system resilience. This study recommends strengthening implementing regulations under the Personal Data Protection Law, establishing an independent Data Protection Commission, enforcing ISO 27001-level security standards for health data controllers, enhancing supervisory mechanisms, and optimizing the implementation of the Information Security Management System (SMKI) based on the PDCA cycle to ensure more comprehensive and sustainable data protection.

Keywords: State Responsibility, Data Security, BPJS Kesehatan, Human Rights