ABSTRAK

Penggunaan AI dalam sistem operasional perusahaan telah merubah pola pemrosesan data menjadi lebih kompleks yang berimplikasi pada meningkatnya risiko kebocoran data. Kondisi ini menimbulkan ketidaksesuaian antara karakter AI dengan kerangka hukum perlindungan data. Hal inilah yang kemudian memunculkan permasalahan mengenai mekanisme pengaturan perlindungan data pribadi yang dikelola oleh sistem perusahaan berbasis AI serta konsep perlindungan hukum bagi konsumen atas kebocoran data pribadi yang disebabkan oleh sistem perusahaan tersebut.

Metode penelitian yang digunakan adalah metode penelitian hukum doktrinal guna mengkaji konsistensi norma serta merumuskan konstruksi pertanggungjawaban hukum yang relevan terhadap perkembangan teknologi.

Hasil penelitian menunjukkan bahwa pengaturan perlindungan data pribadi dalam sistem perusahaan berbasis AI telah diakomodasi melalui kebijakan perusahaan yang bernama *AI Guardrails,* namun tetap implementasinya masih menghadapi berbagai kendala salah satunya adalah keterbatasan infrastruktur atau teknologi. Selanjutnya mekanisme perlindungan hukum atas kebocoran data pribadi telah diatur melalui mekanisme preventif dan represif melalui undang-undang, namun konsep pertanggungjawaban hukum yang masih berorientasi pada kesalahan manusia belum mampu menjangkau tindakan otonom AI. Kesimpulan penelitian ini adalah, penggunaan AI dalam sistem perusahaan menimbulkan ketidakpastian hukum dalam atribusi tanggung jawab sehingga diperlukan penguatan regulasi yang adaptif serta guna menjamin perlindungan data pribadi secara komprehensif.

Kata Kunci: Perlindungan Data Pribadi, Kecerdasan Buatan.

ABSTRACT

The use of AI in corporate operational systems has transformed data processing patterns into more complex ones, leading to an increased risk of data breaches. This situation creates a mismatch between the nature of AI and the legal framework for data protection. This has led to issues regarding the regulatory mechanisms for protecting personal data managed by AI-based corporate systems and the concept of legal protection for consumers in the event of personal data breaches caused by these systems.

The research method used is doctrinal legal research to examine the consistency of norms and formulate a legal accountability framework relevant to technological developments.

The results show that the regulation of personal data protection in AI-based corporate systems has been accommodated through company policies called AI Guardrails. However, its implementation still faces various obstacles, including limited infrastructure and technology. Furthermore, legal protection mechanisms for personal data breaches have been regulated through preventive and repressive mechanisms within the law. However, the concept of legal accountability, which is still oriented towards human error, has not yet been able to address the autonomous actions of AI. The conclusion of this study is that the use of AI in corporate systems creates legal uncertainty in the attribution of responsibility, necessitating the strengthening of adaptive regulations to ensure comprehensive personal data protection.

Keywords: *Personal Data Protection, Artificial Intelligence.*