

Abstrak

Tindak pidana siber memanfaatkan perkembangan teknologi informasi untuk melakukan kejahatan, termasuk penyebaran informasi berunsur SARA yang dapat menimbulkan konflik sosial dan gangguan stabilitas masyarakat. Penelitian ini mengidentifikasi kesenjangan hukum dalam pertanggungjawaban pidana pelaku siber serta tantangan dalam pengumpulan bukti digital. Kurangnya batasan hukum yang jelas dan berbagai kendala dalam penegakan hukum di ranah digital menjadi fokus utama. Melalui metode yuridis normatif, penelitian ini mengkaji hukum sebagai norma yang berlaku dalam masyarakat berdasarkan hierarki perundang-undangan dan hubungan harmoni perundang-undangan. Contoh kasus yang dibahas adalah kejahatan phishing oleh Rizki Fahmi, terdakwa penyebaran kebencian berunsur SARA. Penegakan hukum yang tegas dan konsisten diperlukan untuk mengatasi kejahatan siber dan dampaknya yang signifikan terhadap korban serta masyarakat luas.

Kata Kunci: Tindak pidana siber, penyebaran SARA, kesenjangan hukum, phishing, penegakan hukum

Abstract

Cybercrime utilizes the development of information technology to commit crimes, including the dissemination of racially charged information that can lead to social conflict and disruption of community stability. This research identifies legal gaps in the criminal liability of cyber offenders as well as challenges in collecting digital evidence. The lack of clear legal boundaries and various obstacles in law enforcement in the digital realm are the main focus. Through the normative juridical method, this research examines the law as a norm that applies in society based on the hierarchy of legislation and the harmony of legislation. The case example discussed is the phishing crime by Rizki Fahmi, the defendant of spreading SARA hatred. Firm and consistent law enforcement is needed to overcome cybercrime and its significant impact on victims and the wider community.

Keywords: Cybercrime, spreading SARA, legal gap, phishing, law enforcement