ANALISIS YURIDIS TERHADAP TINDAK PIDANA SIBER *RANSOMWARE* DALAM HUKUM POSITIF INDONESIA

Oleh:
Muhammad Rizki Kurniarullah
NIM. 2205040077

ABSTRAK

Penelitian ini bertujuan untuk menganalisis secara mendalam problematika yuridis terkait tindak pidana siber *ransomware* dalam kerangka hukum positif Indonesia serta mengidentifikasi kompleksitas modus operandi sistematis yang melatarbelakangi kejahatan tersebut. Metode penelitian yang diterapkan dalam skripsi ini adalah penelitian hukum normatif dengan menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*) untuk membedah sinkronisasi aturan yang berlaku. Hasil penelitian menunjukkan bahwa secara yuridis, upaya penanggulangan *ransomware* di Indonesia saat ini masih bertumpu pada instrumen hukum positif seperti Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Pelindungan Data Pribadi (UU PDP). Namun, keseluruhan regulasi tersebut dinilai masih bersifat parsial, fragmentaris, dan reaktif, karena cenderung menitikberatkan pada aspek vandalisme digital seperti akses ilegal atau perusakan data secara terpisah, sehingga gagal menjangkau hakikat *ransomware* sebagai kejahatan hibrida yang menyatukan sabotase teknis dengan motif pemerasan ekonomi yang sangat kompleks. Dalam aspek operasional, penelitian ini menemukan bahwa modus operandi *ransomware* dijalankan melalui tahapan yang sangat terorganisir, diawali dengan teknik *phishing* dan rekayasa sosial sebagai pintu masuk utama penetrasi sistem. Pelaku kemudian memanipulasi fitur internal sistem sehingga serangan sulit terdeteksi, yang diikuti dengan enkripsi data massal serta pelumpuhan sistem cadangan (*backup*) secara permanen. Fenomena ini semakin diperparah dengan munculnya strategi *double extortion* dan model bisnis *Ransomware-as-a-Service* (RaaS) yang memanfaatkan anonimitas aset kripto untuk mengaburkan jejak transaksi finansial. Kesimpulannya, adanya ketidakjelasan konsep dan fragmentasi hukum saat ini yang memicu adanya fenomena kekaburan norma sehingga menciptakan celah penegakan hukum yang signifikan, sehingga diperlukan langkah mendesak berupa harmonisasi regulasi melalui formulasi kebijakan hukum pidana yang lebih komprehensif guna memperkuat ketahanan siber nasional dan menjamin kepastian hukum yang utuh di ruang digital Indonesia.

Kata Kunci: *Ransomware*, Hukum Positif Indonesia

ANALISIS YURIDIS TERHADAP TINDAK PIDANA SIBER *RANSOMWARE* DALAM HUKUM POSITIF INDONESIA

By:
Muhammad Rizki Kurniarullah
NIM. 2205040077

ABSTRACT

This research aims to analyze in depth the legal problematics concerning ransomware cybercrime within the framework of Indonesian positive law and to identify the complexities of the systematic modus operandi underlying such crimes. The research methodology employed in this study is normative legal research, utilizing a statute approach and a conceptual approach to examine the synchronization of existing regulations. The findings indicate that, from a legal perspective, ransomware countermeasures in Indonesia currently rely on positive law instruments such as the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the Personal Data Protection Law (UU PDP). However, these regulations are deemed partial, fragmentary, and reactive, as they tend to focus on aspects of digital vandalism such as illegal access or data destruction separately. Consequently, they fail to encompass the essence of ransomware as a hybrid crime that integrates technical sabotage with highly complex economic extortion motives. Operationally, this study reveals that the ransomware modus operandi is executed through highly organized stages, initiated by phishing techniques and social engineering as the primary entry points for system penetration. Perpetrators subsequently manipulate internal system features, rendering attacks difficult to detect, followed by mass data encryption and the permanent disabling of backup systems. This phenomenon is further exacerbated by the emergence of double extortion strategies and the Ransomware-as-a-Service (RaaS) business model, which leverages the anonymity of crypto assets to obscure financial audit trails. In conclusion, the current conceptual ambiguity and legal fragmentation trigger a vagueness of norms, creating significant gaps in law enforcement. Therefore, urgent measures are required through regulatory harmonization and the formulation of more comprehensive criminal law policies to bolster national cyber resilience and ensure absolute legal certainty within Indonesia's digital domain.

Keywords*: Ransomware, Indonesian Positive Law*