

ABSTRAK

Penelitian ini menganalisis tentang pertanggungjawaban pelaku *cryptojacking* sebagai *cybercrime* dalam hukum pidana Indonesia. Topik ini penting untuk diteliti karena maraknya tindak kejahatan siber menimbulkan kekhawatiran serius di tengah masyarakat yang mengancam keamanan data, informasi pribadi, merugikan secara finansial, serta mengganggu ketertiban dan keamanan nasional. *Cryptojacking* adalah contoh kejahatan modern yang tidak dapat dijangkau oleh KUHP, sehingga lahirnya UU ITE dianggap mampu mengisi kekosongan hukum. Penelitian ini bertujuan untuk menganalisis pengaturan *Cryptojacking* sebagai tindak pidana di Indonesia dan memahami apakah konsep pertanggungjawaban dalam Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diterapkan terhadap pelaku tindak pidana *cryptojacking*.

Metode penelitian yang digunakan adalah penelitian normatif dengan pendekatan perundang-undangan dan konseptual. Teknik pengumpulan bahan hukum dilakukan dengan studi kepustakaan yang kemudian dianalisis menggunakan metode penelitian kualitatif.

Hasil penelitian menunjukkan bahwa praktik *cryptojacking* dapat dikenakan Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sepanjang dilakukan melalui akses tanpa hak terhadap sistem elektronik milik pihak lain. Namun, penerapannya memerlukan penafsiran hukum yang lebih luas, terutama mengenai unsur “tanpa hak” dan makna akses dalam konteks pemanfaatan sumber daya komputasi. Terhadap *cryptojacking* yang dilakukan tanpa peretasan, termasuk melalui website yang dikelola oleh pelaku sendiri, diperlukan penafsiran progresif. Keterbatasan norma tersebut menimbulkan ketidakpastian hukum dan menunjukkan perlunya pengaturan yang lebih eksplisit yang secara tegas mengatur serta mengkriminalisasi penyalahgunaan sumber daya komputasi dalam sistem hukum pidana Indonesia, tidak hanya terkait akses ilegal saja, melainkan juga aspek eksploitasi ekonomi dan pemanfaatan sumber daya digital secara melawan hukum.

Kata kunci: pertanggungjawaban pidana, *Cryptojacking*, hukum pidana.

ABSTRACT

This study analyzes the accountability of cryptojacking perpetrators as cybercriminals under Indonesian criminal law. This topic is important to research because the rise of cybercrime has caused serious concern among the public, threatening data security, personal information, causing financial losses, and disrupting national order and security. Cryptojacking is an example of a modern crime that cannot be covered by the Criminal Code, so the enactment of the ITE Law is considered to be able to fill the legal void. This study aims to analyze the regulation of cryptojacking as a criminal offense in Indonesia and to understand whether the concept of liability in Law No. 1 of 2024 concerning Electronic Information and Transactions can be applied to perpetrators of cryptojacking crimes.

The research method used is normative research with a legislative and conceptual approach. The technique for collecting legal materials is conducted through a literature study, which is then analyzed using qualitative research methods.

The results of this study indicate that cryptojacking practices may be subject to Article 30 of Law Number 11 of 2008 on Information and Electronic Transactions, insofar as they involve unauthorized access to electronic systems owned by other parties. However, its application requires broader legal interpretation, particularly concerning the element of “without authorization” and the meaning of access in the context of computational resource utilization. In cases where cryptojacking is conducted without hacking, including through websites managed by the perpetrators themselves, a progressive legal interpretation is required. The limitations of existing legal norms create legal uncertainty and highlight the need for more explicit regulations that clearly govern and criminalize the misuse of computational resources within the Indonesian criminal law system, not only in relation to illegal access but also concerning economic exploitation and unlawful use of digital resources.

Keywords: *criminal liability, Cryptojacking, criminal law.*