

ABSTRAK

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa perubahan besar dalam kehidupan masyarakat, termasuk munculnya bentuk kejahatan baru yang dikenal sebagai penipuan online (*online fraud*). Penipuan online merupakan salah satu jenis kejahatan siber (*cybercrime*) yang dilakukan melalui media elektronik dengan tujuan memperoleh keuntungan secara melawan hukum, dan terus mengalami peningkatan signifikan dari tahun ke tahun di Indonesia. Penelitian ini bertujuan untuk mengkaji dan menganalisis dua permasalahan pokok, yaitu: (1) pertanggungjawaban pidana terhadap pelaku tindak pidana penipuan online berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE); dan (2) upaya penegakan hukum terhadap tindak pidana penipuan online di Indonesia.

Penelitian ini menggunakan metode penelitian hukum normatif yang bersifat deskriptif analitis, dengan sumber bahan hukum yang terdiri dari bahan hukum primer berupa peraturan perundang-undangan seperti Kitab Undang-Undang Hukum Pidana (KUHP) dan UU ITE beserta perubahannya, bahan hukum sekunder berupa literatur dan doktrin hukum, serta bahan hukum tersier. Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dan analisis data dilakukan secara kualitatif dengan menggunakan penalaran hukum yang logis dan sistematis.

Hasil penelitian menunjukkan bahwa pertanggungjawaban pidana pelaku penipuan online dapat dikenakan apabila terpenuhi unsur-unsur: adanya perbuatan melawan hukum, adanya kesalahan, kemampuan bertanggung jawab, serta tidak adanya alasan pembeda maupun pemaaf. Secara yuridis, penipuan online diatur dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE sebagai *lex specialis* terhadap Pasal 378 KUHP, dengan ancaman pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Adapun upaya penegakan hukum terhadap penipuan online dilakukan secara

preventif dan represif oleh aparat penegak hukum, khususnya Kepolisian melalui Direktorat Tindak Pidana Siber (Dittipidsiber), Kejaksaan, Pengadilan, serta Badan Siber dan Sandi Negara (BSSN). Namun, penegakan hukum masih menghadapi berbagai kendala, antara lain sulitnya melacak identitas pelaku yang menggunakan akun anonim, keterbatasan kapasitas forensik digital aparat penegak hukum, rendahnya literasi digital masyarakat, serta sifat lintas yurisdiksi dari kejahatan siber. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas sumber daya manusia di bidang forensik digital, serta kerjasama internasional yang lebih intensif guna mewujudkan penegakan hukum yang efektif terhadap tindak pidana penipuan online.

Kata Kunci: Penipuan Online, Pertanggungjawaban Pidana, Penegakan Hukum, Undang-Undang Informasi dan Transaksi Elektronik, Kejahatan Siber.

ABSTRACT

The rapid development of information and communication technology has brought significant changes to society, including the emergence of new forms of crime known as online fraud. Online fraud constitutes a type of cybercrime conducted through electronic media with the intent to obtain unlawful financial gain, and has continued to increase significantly in Indonesia. This study aims to examine and analyze two main issues: (1) criminal liability of perpetrators of online fraud offenses under the Electronic Information and Transactions Law (UU ITE); and (2) law enforcement efforts against online fraud offenses in Indonesia.

This research employs a normative legal research method with a descriptive-analytical approach, utilizing primary legal materials including statutory regulations such as the Criminal Code (KUHP) and the UU ITE and its amendments, secondary legal materials comprising legal literature and doctrines, and tertiary legal materials. Data collection was conducted through library research, and data analysis was carried out qualitatively using logical and systematic legal reasoning.

The findings indicate that criminal liability for online fraud may be imposed when the following elements are fulfilled: the existence of an unlawful act, the presence of fault, criminal capacity, and the absence of justification or excuse. Juridically, online fraud is regulated under Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the UU ITE as *lex specialis* to Article 378 of the Criminal Code, carrying a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000 (one billion

rupiah). Law enforcement against online fraud is carried out through both preventive and repressive measures by law enforcement agencies, particularly the National Police's Directorate of Cybercrime (Dittipidsiber), the Prosecutor's Office, Courts, and the National Cyber and Crypto Agency (BSSN). However, law enforcement continues to face several obstacles, including difficulty in tracing perpetrators who use anonymous accounts, limited digital forensic capacity among law enforcement personnel, low digital literacy in society, and the cross-jurisdictional nature of cybercrime. Therefore, regulatory strengthening, enhancement of digital forensic human resource capacity, and more intensive international cooperation are needed to achieve effective law enforcement against online fraud.

Keywords: Online Fraud, Criminal Liability, Law Enforcement, Electronic Information and Transactions Law, Cybercrime.