

RINGKASAN

Zuraini **Aspek Hukum Kejahatan Siber Terhadap**
200510268 **Tindak Pidana Phishing (Penipuan Informasi) di**
 Indonesia
 (Dr. Yusrizal, S.H., M.H dan Eko Gani Pg, S.H.,
 M.H)

Kemajuan teknologi internet telah memberikan dampak positif sekaligus memunculkan tantangan baru, salah satunya kejahatan siber berupa *phishing*. Kasus *phishing* di Indonesia meningkat tajam dari 19.919 kasus pada 2021 menjadi 64.989 kasus pada 2023, menunjukkan lemahnya literasi digital dan pengawasan keamanan siber. Meskipun Indonesia memiliki Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi, penegakan hukum terhadap *phishing* belum efektif karena keterbatasan pengetahuan aparat dan sumber daya hingga kompleksitas hukum *cyber* yang masih berkembang.

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis konsep kejahatan *phishing* dalam perspektif hukum pidana di Indonesia, serta mengkaji secara mendalam mekanisme perlindungan hukum yang tersedia bagi korban kejahatan *phishing* di Indonesia.

Metode penelitian yang digunakan adalah yuridis normatif, dengan pendekatan undang-undang dan analisis kasus. Penelitian ini bersifat deskriptif, dan menggunakan sumber bahan hukum primer, sekunder, dan tersier, dan analisis data secara kualitatif.

Phishing adalah bentuk kejahatan siber yang memanfaatkan manipulasi psikologis untuk mencuri data pribadi dan informasi sensitif. Meskipun Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi menyediakan dasar hukum di Indonesia, implementasi masih menghadapi tantangan terutama dalam hal teknis dan koordinasi antar lembaga. Pendekatan terintegrasi melalui edukasi, penguatan regulasi, dan pemanfaatan teknologi diperlukan untuk menangani ancaman *phishing* secara komprehensif. Perlindungan hukum bagi korban phishing harus dilakukan melalui mekanisme yang jelas dan terstruktur untuk memastikan pemulihan hak dan penegakan keadilan. Pemerintah perlu meningkatkan pelatihan literasi digital serta memperkuat Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi untuk memastikan perlindungan hukum yang lebih efektif. Selain itu, kerja sama yang lebih erat antara lembaga penegak hukum dan penyedia layanan digital diperlukan untuk mempermudah pelaporan dan penyelesaian kasus.

Kata Kunci: *Phishing, Cyber Law*

SUMMARY

**Zuraini The Legal Aspects of Cybercrime Regarding
200510268 Phishing (Information Fraud) in Indonesia
 (Dr. Yusrizal, S.H., M.H and Eko Gani Pg, S.H.,
 M.H)**

The advancement of internet technology has brought positive impacts while simultaneously presenting new challenges, one of which is cybercrime in the form of phishing. Phishing cases in Indonesia have surged dramatically from 19,919 cases in 2021 to 64,989 cases in 2023, indicating weak digital literacy and insufficient cybersecurity oversight. Although Indonesia has enacted the Information and Electronic Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), law enforcement against phishing remains ineffective due to limited knowledge of law enforcement officers, resource constraints, and the evolving complexity of cyber law.

This study aims to identify and analyze the concept of phishing crimes from the perspective of criminal law in Indonesia, as well as to examine in depth the legal protection mechanisms available for victims of phishing crimes in Indonesia.

The research employs a normative juridical method, utilizing statutory and case analysis approaches. This study is descriptive in nature and uses primary, secondary, and tertiary legal materials, with qualitative data analysis.

Phishing is a form of cybercrime that exploits psychological manipulation to steal personal data and sensitive information. Although the UU ITE and UU PDP provide a legal foundation in Indonesia, their implementation faces technical challenges and inter-agency coordination issues. A comprehensive and systematic approach through education, regulatory strengthening, and technology utilization is essential to effectively counter phishing threats. Legal protection for phishing victims should be carried out through clear and structured mechanisms to ensure the recovery of rights and the enforcement of justice.

The government should enhance digital literacy training and strengthen the UU ITE and UU PDP to ensure more effective legal protection. Furthermore, closer cooperation between law enforcement agencies and digital service providers is needed to facilitate case reporting and resolution.

Keywords: *Phishing, Cyber Law.*