

ABSTRAK

PENEGAKAN HUKUM PIDANA TERHADAP TINDAKAN *PHISING* PENCURIAN DATA MELALUI MEDIA SOSIAL (Studi Kasus di Polda Sumsel)

**Oleh
Igo Rollis Joosevelt**

Perkembangan teknologi informasi dan komunikasi membawa Indonesia ke era digital, di mana internet menjadi krusial dalam mendukung berbagai aktivitas. Seiring berkembangnya teknologi informasi mampu memberikan dampak positif bagi banyak orang namun hal ini juga menyebabkan munculnya kejahatan-kejahatan baru yang selanjutnya dikenal dengan istilah *cybercrime*. Salah satu bentuk kejahatan yang marak terjadi adalah *phising*, yaitu upaya penipuan untuk mencuri data pribadi melalui media sosial dengan cara mengelabui korban. Kejahatan ini berpotensi menimbulkan kerugian besar bagi individu maupun lembaga. Oleh karena itu, penegakan hukum terhadap tindak pidana *phising* menjadi suatu hal yang krusial untuk memberikan perlindungan hukum bagi masyarakat. Permasalahan penelitian ini : (1). Bagaimana penegakan hukum pidana terhadap tindakan *phising* pencurian data melalui media sosial (2). Apakah faktor-faktor yang mempengaruhi penegakan hukum pidana terhadap tindakan *phising* pencurian data melalui media sosial

Penelitian ini menggunakan pendekatan yuridis normatif dan yuridis empiris. Jenis data terdiri dari data primer dan data sekunder. Narasumber pada penelitian ini terdiri dari Penyidik Ditreskrimsus Siber Kepolisian Daerah Sumatera Selatan, Akademisi Fakultas MIPA Universitas Lampung, dan Akademisi Fakultas Hukum Universitas Lampung. Pengumpulan data dengan studi lapangan dan studi pustaka. Analisis data dilakukan secara kualitatif.

Hasil penelitian ini menunjukkan bahwa penegakan hukum pidana terhadap tindakan *phising* pencurian data melalui media sosial telah berjalan baik dan telah sesuai dengan tahap formulasi dan tahap aplikasi. Pada tahap formulasi, hal ini tercermin dalam pengaturan hukum melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pada tahap aplikasi, terhadap tindakan *phising* pencurian data melalui media sosial juga telah dilaksanakan melalui langkah-langkah yang sistematis dan berpedoman pada peraturan perundang-undangan yang berlaku, sedangkan pada faktor yang mempengaruhi penegakan hukum pidana terhadap tindakan *phising* pencurian data melalui media sosial terdapat tiga faktor

dominan yaitu faktor penegak hukum, sarana dan fasilitas, serta masyarakat. Faktor penegak hukum dipengaruhi oleh keterbatasan kemampuan penyidik siber, terutama dalam aspek teknologi informasi. Hal ini juga berkaitan dengan faktor sarana dan fasilitas, di mana keterbatasan anggaran menghambat pengadaan perangkat forensik dan infrastruktur teknologi yang memadai. Sementara itu, faktor masyarakat turut berperan dalam maraknya kasus *phising* di media sosial akibat rendahnya pemahaman teknologi, kurangnya kewaspadaan, serta mudahnya masyarakat tergiur oleh modus penipuan yang menjanjikan hadiah atau uang. Selain itu, banyak korban *phising* yang merasa malu atau enggan melaporkan kasus yang dialaminya karena cenderung menyalahkan diri sendiri atas kelalaian mereka atau khawatir dengan stigma negatif dari lingkungan sekitar dan juga sering menganggap proses pelaporan kejahatan sebagai sesuatu yang sulit, rumit, dan memakan waktu, sehingga menghambat penyidik untuk mempercepat pengungkapan dan penanganan kasus *phising*.

Adapun saran dari penelitian ini adalah perlunya pelatihan dan peningkatan kapasitas bagi penyidik, khususnya personel di bidang siber, agar lebih menguasai teknologi informasi yang terus berkembang. Selain itu, pemerintah dan institusi terkait perlu mengalokasikan anggaran yang memadai untuk pengadaan perangkat keras dan perangkat lunak forensik guna mendukung efektivitas penyidikan. Partisipasi aktif masyarakat juga sangat diperlukan dalam upaya penegakan hukum, masyarakat diharapkan lebih berani untuk melapor, menggunakan teknologi secara bijak, serta memahami aspek hukum dan modus kejahatan yang berkembang.

Kata Kunci : Penegakan Hukum Pidana, Tindakan *Phising*, Pencurian Data, Media Sosial

ABSTRACT

CRIMINAL LAW ENFORCEMENT AGAINST PHISING DATA THEFT THROUGH SOCIAL MEDIA (Case Study at South Sumatra Regional Police)

**By
Igo Rollis Joosevelt**

The development of information and communication technology has brought Indonesia into the digital era, where the internet plays a crucial role in supporting various activities. While technological advancements have had a positive impact on many aspects of life, they have also led to the emergence of new crimes, commonly referred to as cybercrime. One of the most prevalent forms of cybercrime is phishing, a fraudulent attempt to steal personal data through social media by deceiving victims. This crime has the potential to cause significant losses for individuals and institutions alike. Therefore, criminal law enforcement against phishing crimes is crucial to providing legal protection to society. This research addresses the following issues: (1) How is criminal law enforcement carried out against phishing data theft through social media? (2) What factors influence the enforcement of criminal law against phishing data theft through social media?

This study employs a normative juridical and empirical juridical approach. The data consists of primary and secondary data. The research respondents include investigators from the Cyber Crime Unit of the South Sumatra Regional Police, an academic from the Faculty of Mathematics and Natural Sciences at the University of Lampung, and an academic from the Faculty of Law at the University of Lampung. Data collection methods include field studies and literature studies, while data analysis is conducted qualitatively.

The findings of this study indicate that criminal law enforcement against phishing data theft through social media has been effectively implemented, aligning with both the formulation and application stages. In the formulation stage, this is reflected in legal regulations such as Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, as well as Law Number 27 of 2022 on Personal Data Protection. In the application stage, law enforcement against phishing data theft through social media has been carried out through systematic measures based on applicable legal provisions. However, three dominant factors influence the enforcement of criminal law against phishing crimes: law enforcement officers, facilities and infrastructure, and the public. The effectiveness of law enforcement is hindered by the limited capabilities of cybercrime investigators, particularly in information technology.

This issue is also linked to infrastructure and facilities, where budget constraints hinder the procurement of forensic tools and adequate technological infrastructure. Meanwhile, public factors also contribute to the prevalence of phishing cases on social media due to low technological literacy, lack of vigilance, and susceptibility to fraudulent schemes promising rewards or money. Additionally, many phishing victims feel ashamed or reluctant to report their cases, either because they blame themselves for their negligence or fear social stigma. The perception that reporting cybercrimes is complicated and time-consuming further hampers investigators in resolving phishing cases efficiently.

This study suggests the need for training and capacity-building programs for investigators, especially those in the cybercrime unit, to enhance their expertise in evolving information technology. Furthermore, the government and relevant institutions should allocate sufficient budgets for procuring forensic hardware and software to support effective investigations. Active public participation is also essential in law enforcement efforts. Society is encouraged to be more proactive in reporting cases, using technology wisely, and understanding both legal aspects and emerging cybercrime tactics.

Keywords : Criminal Law Enforcement, Phishing, Data Theft, Social Media