ABSTRAK

KAJIAN KRIMINOLOGI TERHADAP PELAKU KEJAHATAN PENGELABUAN UNTUK MENDAPATKAN DATA PRIBADI (PHISING) MENGGUNAKAN TAUTAN YANG DIKIRIM MELALUI MEDIA SOSIAL

Oleh

DIANA

Teknologi informasi yang mengalami kemajuan dapat menimbulkan dampak negatif berupa munculnya berbagai jenis-jenis kejahatan baru dengan berbasis internet yang biasa disebut dengan kejahatan dunia maya atau *cybercrime*, salah satunya seperti kejahatan pengelabuan untuk mendapatkan data pribadi (phising) menggunakan tautan yang dikirim melalui media sosial. Dalam penulisan ini dibahas beberapa permasalahan, yakni: apakah faktor-faktor penyebab terjadinya kejahatan pengelabuan untuk mendapatkan data pribadi (phising) menggunakan tautan, dan bagaimanakah upaya menanggulangi kejahatan pengelabuan untuk mendapatkan data pribadi (phising) menggunakan tautan.

Metode penelitian yang digunakan penulis dalam skripsi ini adalah pendekatan yuridis normatif dan empiris. Adapun data yang digunakan dalam penelitian adalah data primer dan data sekunder dengan proses pengumpulan data melalui studi lapangan dan studi kepustakaan. Narasumber dalam penelitian ini adalah enyidik Unit *Cybercrime* Polda Lampung, Akademisi Fakultas Lampung Bagian Hukum Pidana dan Akademisi Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung.

Berdasarkan hasil penelitian dan pembahasan maka dapat disimpulkan bahwa terdapat dua faktor penyebab terjadinya kejahatan pengelabuan untuk mendapatkan data pribadi (phising) menggunakan tautan yang dikirim melalui media sosial, yaitu faktor internal yang terdiri dari faktor kurangnya pengetahuan dan faktor kebocoran data pengguna. Terdapat juga faktor eksternal yang terdiri dari faktor ekonomi, faktor kurangnya kesadaran hukum, dan faktor kurangnya sistem keamanan serta kurangnya penegakan hukum. Upaya menanggulangi kejahatan pengelabuan untuk mendapatkan data pribadi (phising) menggunakan tautan dapat dilakukan dengan menggunakan upaya penal dan upaya non penal. Upaya penal yaitu dengan menggunakan sanksi pidana sesuai dengan yang diatur dalam Pasal 28 ayat (1) jo

Pasal 45A ayat (1) dan Pasal 35 jo Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, sanksi pidana ini juga digunakan untuk menjatuhkan sanksi pidana dalam Putusan Nomor : 155/Pid.Sus/2018/PN-Cbn, dimana pelaku dijatuhi hukuman penjara selama 8 (delapan) bulan. Sedangkan, upaya nonpenal yang dapat dilakukan yaitu dengan mensosialisikan pengetahuan terkait kejahatan phising, lebih berhati-hati dalam membuka suatu pesan yang berisikan tautan, tidak meng-klik secara sembarangan suatu tautan, melakukan update software secara rutin untuk memaksimalkan sistem keamanan pada platform sosial media dan mengaktifkan data encryption untuk melindungi data-data penting.

Saran yang diajukan sebagai hasil dari penelitian ini adalah sebaiknya masyarakat lebih berhati-hati dalam menggunakan sosial media khususnya jika menerima suatu tautan harus memeriksa terlebih dahulu sumber ke akuratan suatu tautan dan aparat penegak hukum diharapkan lebih memperhatikan masyarakat khususnya para pengguna media sosial agar dapat memberikan pengawasan kepada masyarakat sehingga masyarakat dapat merasakan perlindungan keamanan serta memberikan edukasi terkait kejahatan phising agar kedepannya masyarakat dapat lebih berhati-hati lagi dalam menggunakan media sosial dan mengakses suatu tuatan sehingga dapat meminimalisir terjadinya kejahatan phising.

Kata Kunci : Kriminologi, Pelaku Kejahatan, Pengelabuan Data Pribadi(*Phising*).

ABSTRACT

CRIMINOLOGICAL STUDY ON PERPETRATORS OF FRAUD CRIMES DECEPTION TO OBTAIN PERSONAL DATA (PHISHING) USING LINKS THAT SENT THROUGH SOCIAL MEDIA

By

DIANA

Advancements in information technology can have an impact negative in the form of the emergence of various new types of crimes based on the internet commonly referred to as cybercrime, one of one of them is phishing to obtain personal data using links sent through social media.In this writing discussed several issues, namely: what are the factors causing the occurrence fraud to obtain personal data (phishing) using link, and what are the efforts to combat phishing crimes to obtaining personal data (phishing) using links.

The research method used by the author in this thesis is an approach juridical normative and empirical.The data used in the research are primary data and secondary data with the data collection process through field studies field studies and library research.The resource person in this research is an investigator Cybercrime Unit of Polda Lampung, Academics from the Faculty of Law at Lampung University Criminal Law and Academics from the Faculty of Social and Political Sciences, University of Lampung.

Based on the results of the research and discussion, it can be concluded that there are two factors l causing the crime of deception to obtain personal data (phishing) using links sent through social media, namely internal factors consisting of the lack of knowledge factor and the data leakage factor user data.There are also external factors that consist of economic factors, factors such as lack of legal awareness, and factors such as lack of security systems and lack of law enforcement.Efforts to combat phishing crimes to obtaining personal data (phishing) using links can be done with using penal and non-penal efforts.Penal efforts are those that using criminal sanctions in accordance with the provisions of Article 28 paragraph (1) jo article 45A paragraph (1) and Article 35 in conjunction with Article 51 paragraph

(1) of Law Number 19 Year 2016 Regarding Amendments to Law Number 11 of 2008 Regarding Information and Electronic Transactions, this criminal sanction is also used to impose criminal sanctions in Decision Number: 155/Pid.Sus/2018/PN Cbn, where the perpetrator was sentenced to 8 (eight) months in prison. Meanwhile, non-penal efforts that can be undertaken include socializing knowledge related to phishing crimes, be more cautious when opening a messages containing links, not clicking on links indiscriminately, regularly updating software to maximize security systems on social media platforms and enabling data encryption to protect important data.

The recommendation put forward as a result of this research is that the public should be more careful in using social media, especially when receiving a links must first check the source for the accuracy of a link and the authorities law enforcement is expected to pay more attention to the community, especially the social media users so they can provide oversight to the community so that the community can feel secure protection and provide education related to phishing crimes so that in the future the community can be more cautious be more careful when using social media and accessing certain content so that can minimize the occurrence of phishing crimes.

***Keywords**: Criminology, Criminal Offenders, Personal Data Deception (Phishing).*