
PENEGAKAN HUKUM TINDAK PIDANA *CYBER CRIME* DALAM BENTUK *PHISING* DI INDONESIA

Triyanto

Fakultas Hukum Universitas Islam Batik Surakarta

Email : mastriy@yahoo.co.id

ABSTRAK

The development of information technology has changed the times, bringing more modern human progress. This development has an impact on the digitalization era in various fields. This has an impact on the birth of phishing crimes. Advances in information technology have provided many opportunities for cyber crime in the form of phishing. This article aims to write about law enforcement for cybercrime in the form of phishing. Considering that the crime of phishing is a crime that has only recently emerged due to the development of information technology. There is a need for efforts by the state to control phishing crimes so that they do not harm society. Moreover, phishing perpetrators are increasingly sophisticated in this era. This research method is normative juridical.

ARTICLE INFO

Article History:

Accepted 10 Nov 2023

Available online 24 Des 2023

Kata kunci: ***cyber crime, phishing***

I. PENDAHULUAN

Dalam era digital saat ini, perkembangan teknologi telah membawa dampak positif dan negatif dalam berbagai aspek kehidupan. Salah satu dampak negatif yang muncul adalah meningkatnya tindak pidana cybercrime, di antaranya adalah phishing atau pencurian data secara online. Phishing merupakan tindakan memperoleh informasi pribadi, seperti kata sandi, informasi kartu kredit, dan data identitas lainnya, dengan menyamar sebagai entitas tepercaya melalui komunikasi elektronik. Indonesia, sebagai salah satu negara berkembang dengan penetrasi internet yang semakin luas, tidak luput dari ancaman phishing. Semakin meningkatnya pengguna internet di Indonesia juga diiringi dengan peningkatan kasus phishing yang dilaporkan, yang mencakup serangan terhadap individu, perusahaan, bahkan pemerintah.

Meskipun telah ada upaya untuk memerangi kejahatan ini, penegakan hukum terhadap tindak pidana cybercrime, khususnya dalam bentuk phishing, masih menghadapi berbagai tantangan. Tantangan tersebut meliputi kecanggihan teknologi yang digunakan oleh para pelaku, kurangnya kesadaran masyarakat akan risiko keamanan cyber, serta keterbatasan sumber daya dan kapasitas instansi penegak hukum dalam menangani kasus-kasus ini.

Kemajuan teknologi informasi saat ini memberikan kemudahan bagi masyarakat untuk mengakses informasi darimanapun. Perkembangan teknologi informasi juga menuntut masyarakat untuk dapat mengikuti perkembangannya. Perkembangan teknologi informasi menjadikan masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial. Disamping banyaknya manfaat yang ditimbulkan dari perkembangan tersebut juga lahirlah dampak negatif dalam

penyalahgunaan teknologi. Dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.¹

Kejahatan sebagai akibat dari penyalahgunaan internet atau yang dilakukan di dunia maya disebut dengan *cybercrime*. Salah satu bentuk *cybercrime* adalah *phishing*. *Phishing* dikategorikan sebagai jenis serangan *cyber* di mana penyerang berusaha memperoleh informasi pribadi atau rahasia secara tidak sah dari individu atau entitas dengan menyamar sebagai bisnis yang dapat dipercaya. Pelaku biasanya menggunakan strategi yang menipu, seperti membuat komunikasi elektronik, pesan teks, atau situs web palsu yang sangat mirip dengan platform sah, untuk menyesatkan individu yang tidak menaruh curiga agar mengungkapkan informasi sensitif, seperti kata sandi, rincian kartu kredit, atau data keuangan penting lainnya. *Phishing* adalah praktik umum yang bertujuan melakukan pencurian identitas, melakukan tindakan penipuan terkait informasi keuangan, atau secara tidak sah memperoleh akses tidak sah ke akun dan data korban.²

Cybercrime dalam bentuk *phishing* terus meningkat seiring berjalannya waktu. Ini dikarenakan kurangnya pemahaman masyarakat terhadap teknologi yang semakin berkembang. Kejahatan *phishing* biasa dilakukan dengan memanfaatkan media-media sosial yang terhubung dengan jaringan internet. Media yang sering digunakan untuk *phishing* adalah e-mail, sms, atau web.

Indonesia sendiri telah memanfaatkan banyak jaringan internet guna mengikuti perkembangan global mulai dari penggunaan media sosial hingga transaksi perbankan menggunakan media elektronik. Hal tersebut

mengundang pelaku *cybercrime* untuk melakukan kejahatan *phising*. Salah satu contoh yang sering terjadi yaitu penggunaan *internet banking* dimana pelaku memanfaatkan untuk mengambil keuntungan secara melawan hukum.

Oleh sebab itu, perlu adanya penegakan hukum bagi pelaku kejahatan *phising* yang berkeliaran di dunia maya untuk diberikan sanksi berupa pertanggungjawaban pidana atas perbuatannya.

II. METODE PENELITIAN

Penelitian hukum normatif atau penelitian kepustakaan atau studi dokumen adalah metode penelitian yang digunakan penulis. Bahan hukum primer yang digunakan berupa peraturan perundang-undangan, antara lain UUD RI 194, KUHP, Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Bahan hukum sekunder yang digunakan seperti buku, jurnal, dan literasi yang berkaitan dengan penulisan

III. HASIL PENELITIAN DAN PEMBAHASAN

1. Pengaturan Tindak Pidana Bagi Pelaku Kejahatan *Phising*

Sebelum UU ITE dibuat, penegakan hukum terhadap pelaku *cyber crime* menggunakan ketentuan dalam KUHP dengan menerapkan pasal yang memiliki kesesuaian unsur. Dalam KUHP ketentuan pidana *cyber crime* yang berbentuk *phising* dapat menggunakan ketentuan pasal 378 tentang penipuan. Hal ini karena *phising* secara umum juga merupakan bentuk tindakan penipuan. Pasal 378 dirumukan "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu

¹ Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik*, Studi Kasus Prita Mulyasari, PT. Rineka Cipta, Jakarta, 2009

² Irma Yurita, *Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime*. Fakultas Hukum : Universitas Muhammadiyah Kotabumi, Jurnal Hukum Legalita Vol.5, No 2, 2023

kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun”.

Penggunaan pasal 378 dalam pemidaan kasus *cybercrime* dilakukan berdasar penafsiran. Terdapat perbedaan jenis tindak pidana antara tindak pidana *cybercrime* dengan tindak pidana konvensional. Meskipun kejahatan *phising* dan penipuan dalam KUHP terdapat kesamaan unsur perbuatan tetapi terdapat perbedaan bentuk tindak pidana dalam penentuan *locus delicti* dan *tempus delictinya*. Oleh sebab itu diperlukan undang-undang khusus untuk tindak pidana *cyber crime* ini. Karena apabila hanya menggunakan penafsiran saja dapat berakibat terbenturnya tatanan hukum yang berakibat kurang maksimalnya penegakan hukum.

Penegakan hukum terhadap perbuatan tindak pidana *cybercrime* di Indonesia ditandai dengan pembentukan undang-undang khusus yaitu Undang-Undang Nomor 19 Tahun 2016 tentang ITE. Baha berdasarkan asas “*Lex Specialis Derogat Legi General*” yang berarti bahwa undang-undang yang bersifat khusus dapat mengesampingkan undang-undang yang bersifat umum. Sehingga yang berlaku saat ini adalah UU ITE dalam menangani kasus tindak pidana *cyber crime*. UU ITE yang dikenakan kepada pelaku *phising*, jenisnya adalah tindak pidana penjara dan tindak pidana denda, tidak adanya ancaman sanksi pidana tambahan. Jadi sistem pidana yang dipakai tidak ada inovasi jenis sanksi pidana yang khas untuk tindak pidana di bidang informasi dan transaksi elektronik.³

Saat ini *cyber crime* dalam bentuk *phising* dimungkinkan dapat dikenakan Pasal 35 UU ITE karena *phising* merupakan kejahatan siber yang membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu. Cyber crime

dalam bentuk *phising* ini juga dapat dikenakan Pasal 28 UU ITE karena *phising* juga melakukan kebohongan untuk menyesatkan orang lain dimana mengarahkan orang yang dibohongi untuk mengakses sebuah link yang dimana link tersebut ditujukan ke situs palsu dan memberikan suatu perintah untuk memperbarui informasi pribadinya yang rahasia ke dalam situs palsu yang telah dibuat oleh pelaku *phising*, sehingga informasi pribadinya yang rahasia tersebut diketahui oleh pelaku *phising* dan menyebabkan orang tersebut mengalami kerugian.

Namun dalam Pasal 35 dan Pasal 28 UU ITE tersebut tidak memuat unsur manipulasi, penciptaan, dan perubahan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, maksudnya tidak memuat unsur seseorang membuat situs yang seolah-olah mirip situs asli resminya. Sehingga dapat disimpulkan bahwa dalam UU ITE belum mengatur secara jelas mengenai penegakan hukum tindak pidana *phising*.

2. Kebijakan Hukum Terhadap Cyber Crime dalam Bentuk Phising

Upaya yang dilakukan pemerintah dalam mencegah dan meminimalisir tindak kejahatan dunia maya adalah dengan memberlakukan UU ITE. Adanya undang-undang tersebut telah membantu penegak hukum dalam menangani perkara kejahatan yang terjadi karena penyalahgunaan teknologi informasi. Dalam pemberantasan kejahatan dunia maya pada dasarnya saling berhubungan dengan domain kebijakan pencegahan kejahatan, yang biasa dikenal dengan strategi kejahatan.

Adapun upaya pemerintah dalam menangani tindak pidana *phising*:

a. Penegakan protokol dan pedoman

³ Supanto, Perkembangan Kejahatan Teknologi Informasi(Cyber Crime) dan Antisipasinya dengan Penal Policy, Yustisia Jurnal Hukum , No 1, 2016

mengenai keamanan siber dan *phising* merupakan elemen penting dalam perlindungan sistem digital dan mitigasi bahaya online.

- b. Lembaga penegak hukum memainkan peran penting dalam mengidentifikasi dan mengadili mereka yang terlibat dalam aktivitas *phising*, sehingga berfungsi sebagai pencegahan terhadap pelaku kejahatan dunia maya. Hal ini sejalan dengan peraturan yang tercantum dalam pasal 46 ayat (3) Undang-undang Informasi dan Teknologi Elektronik.

IV. KESIMPULAN

Penegakan hukum tindak pidana *cybercrime* dalam bentuk *phising* sebenarnya telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang ITE. Namun dalam Pasal 35 dan Pasal 28 tidak memuat unsur manipulasi, penciptaan, perubahan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik. Mengingat kejahatan *phising* ini merupakan tindakan bahwa seolah-olah seseorang membuat situs yang sama dengan aslinya untuk mengelabui korban. Dengan begitu kurang tegasnya Undang-Undang ITE dalam mengatur penegakan hukum tindak pidana *phising*. Sehingga telah terjadi kekosongan hukum dalam pengaturan tindak pidana *cyber* berupa *phising*.

V. SARAN

Pemerintah perlu melakukan perbaikan dalam Undang-Undang ITE agar mempertegas pengaturan tindak pidana *cyber* berupa *phising* agar kejahatan tersebut tidak terus terjadi dan merugikan banyak masyarakat. Perlunya memberikan kepastian hukum agar tidak terjadi kekaburan hukum. Pemerintah juga perlu meningkatkan pengetahuan masyarakat terkait tindak pidana *phising*. Masyarakat dalam hal ini juga perlu meningkatkan kewaspadaan dalam menerima

informasi melalui media sosial terlebih bagi masyarakat yang masih awam terkait kejahatan *phising*.

DAFTAR PUSTAKA

- Sunarso, Siswanto. 2009. Hukum Informassi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari. Jakarta : Rineka Cipta
- Supanto. 2016. Perkembangan Kejahatan Teknologi Informasi (*Cyber Crime*) dan Antisipasinya dengan Penal Policy, Yustisia Jurnal Hukum 5 , No 1
- Yurita, Irma. 2023. Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana *Cybercrime*. Fakultas Hukum : Universitas Muhammadiyah Kotabumi. Jurnal Hukum Legalita Vol.5, No 2
- Depri Liber Sonata. (2014). Metode Penelitian Hukum Normatif dan Empiris : Karakteristik Khas Dari Metode Meneliti Hukum". *Fiat Justicia Jurnal Ilmu Hukum Volume 8 No 1*.
- Dedi Harianto. (2016). "Asas Kebebasan Berkontrak : Problema Penerapannya Dalam Kontrak Baku Antara Konsumen Dengan Pelaku Usaha". *Jurnal Hukum Samudera Keadilan*.
- Lina Jamilah. (2012). "Asas Kebebasan Berkontrak Dalam Perjanjian Standar Baku". *Jurnal Ilmu Hukum FH Unisba Vol XIII No 1 Maret – Agustus 2012*.