Jurist-Diction
Volume 4 No. 6 November 2021

Modus Operandi Tindak Pidana *Phising* Menurut UU ITE

Vikran Fasyadhiyaksa Putra Y
vikrannputra@gmail.com
Universitas Airlangga

How to cite:
Vikran Fasyadhiyaksa Putra Y. 'Modus Operandi Tindak Pidana Phising Menurut UU ITE' (2021) Vol. 4 No. 6 Jurist-Diction.

Histori artikel:
Submit 7 April 2021;
Diterima 15 Oktober 2021;
Diterbitkan 5 November 2021.

DOI:
10.20473/jd.v4i6.31857

p-ISSN: 2721-8392
e-ISSN: 2655-8297

Abstract

Phishing is an act to commit fraud by tricking the target with the intention of stealing the target's account, by spreading broadcasts which are often carried out through fake emails with fake information that directs the target to a fake page to trap the target so that the perpetrator gets access to the victim's account. Phishing still has some obscurity, especially in the modus operandi of the perpetrator. Therefore, this research aims to analyze and explain the modus operandi of the criminal act of phishing according to the ITE Law. This research is a normative legal research. Because the writing of this research in seeking the truth in order to answer legal issues raised by the author uses secondary data to find legal rules, legal principles, and legal doctrines, and tends to image law as a perspective discipline, which means that only see the law from the point of view of the norms only, which of course is prescriptive. This approach uses a statute approach, a conceptual approach and a case approach.

Keywords: *Phishing Crime; Cyber; Operandi Mode.*

Abstrak

Phising adalah suatu perbuatan untuk melakukan penipuan dengan mengelabui target dengan maksud untuk mencuri akun target, dengan cara menyebarkan broadcast yang seringkali dilakukan melalui email palsu dengan muatan informasi palsu yang mengarahkan target ke halaman palsu untuk menjebak target sehingga pelaku mendapatkan akses terhadap akun korban, Secara ringkas Perbuatan *phising* masih memiliki beberapa kekaburan terutama pada modus operandi pelaku. Oleh karena itulah penelitian ini bertujuan untuk menganalisis dan menjelaskan terkait modus operandi Tindak pidana *Phising* menurut UU ITE. Penelitian ini merupakan penelitian hukum normatif. Karena penelitian ini dalam mencari kebenaran guna menjawab isu hukum yang diangkat penulis menggunakan data sekunder untuk menemukan suatu aturan-aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum, dan cenderung mencitrakan hukum sebagai disiplin prespektif, yang berarti hanya melihat hukum dari sudut pandang norma-normanya saja, yang tentunya bersifat preskriptif. Pendekatan ini menggunakan pendekatan undang-undang (*statute approach*), pendekatan konseptual (*conceptual approach*) dan pendekatan kasus (*case approach*).

Kata Kunci: Tindak Pidana *Phising*; Siber; Modus Operandi.

Pendahuluan

Perkembangan berbagai jenis kejahatan saat ini bukan tanpa sebab, salah satunya akibat dari kompleksnya permasalahan yang dihadapi oleh manusia dalam berinteraksi, menjalin komunikasi dan saling menilai, sehingga tidak jarang timbul konflik atau pertikaian akibat tidak terpenuhinya harapan. Seiring berkembangnya zaman, akhirnya dikenal hal yang bernama Teknologi. Teknologi sendiri adalah sebuah sarana dan prasarana yang diciptakan untuk menyediakan sebuah barang maupun komponen yang dibutuhkan oleh manusia, teknologi sendiri bertujuan untuk memecahkan suatu permasalahan, membuka kreativitas, meningkatkan efektivitas dan efisiensi dalam aktivitas manusia, dengan begitu dapat dikatakan bahwa teknologi merupakan hal yang sangat bermanfaat bagi manusia dalam mengolah, memproses, menyusun, mengatur, dan mendapatkan data dan menghasilkan informasi yang akurat.[1] Walaupun terdapat banyak pengaruh positif dalam perkembangan teknologi, akan tetapi pengaruh negatif yang ditimbulkan dari perkembangan teknologi itu sendiri juga cukup banyak, seperti kegiatan bersosialisasi antara manusia menjadi berkurang, timbulnya rasa ketergantungan akan teknologi, tidak dapatnya menyaring berita-berita yang timbul di media internet, tidak menggunakan media informasi dengan baik contohnya membuka situs-situs yang seharusnya dilarang.[2]

Dari adanya pengaruh negatif yang dibawa oleh teknologi diiringi dengan timbulnya Tindak Pidana dalam bidang Teknologi sendiri, hal ini merupakan hal yang dapat dikatakan masih baru dibandingkan dengan tindak pidana pada umumnya. Pada dasarnya Teknologi sendiri diciptakan bukan diperuntukan sebagai alat kejahatan, teknologi sendiri diciptakan dengan sifat yang netral, akan tetapi seiring berjalannya waktu dengan keluasan fungsi dan kecanggihan teknologi informasi yang terkandung didalamnya semakin merebaknya globalisasi dalam

[1] Nudirman Munir, *Pengantar Hukum Siber Indonesia (*Rajawali Pers 2017).[10].

[2] BPMPK KEMDIKBUD, 'Dampak IPTEK Terhadap Perubahan Tata Nilai Pada Diri Individu' (m-edukasi, 2016) <https://m-edukasi.kemdikbud.go.id/medukasi/produk-files/kontenkm/km2016/KM2016 37/materi1.html> diakses pada 13 Juni 2020.

kehidupan mendorong para pelaku kejahatan untuk menggunakan internet sebagai sarananya.[3] Penggunaan media internet pada zaman ini juga cukup menjadi sebuah sarana yang memudahkan manusia dalam mendapatkan informasi maupun hal lainnya. Semua hal menjadi lebih praktis dalam dunia internet, akan tetapi diiringi dengan kepraktisan yang dibawanya, internet juga membawa dampak negatif berupa keamanan yang belum bisa terjamin. Keamanan dalam dunia siber masih sangat rentan dikarenakan adanya unsur mudahnya dalam mengakses teknologi itu sendiri menyebabkan banyak peretas yang dapat dengan mudah menjangkau sebuah sistem keamanan yang dibuat sedemikian rupa, dalam dunia internet akan selalu ada celah apabila berbicara mengenai sistem keamanan. Hal tersebut dalam dunia internet dikenal sebagai sebuah *bug,* atau dapat diartikan sebagai kecacatan dalam sebuah perangkat yang dibangun. Kecacatan atau *bug* yang paling bahaya adalah *bug* yang menyebabkan celah pada sistem keamanan, dapat dikatakan berbahaya karena dengan menggunakan metode tertentu para peretas dapat masuk dan menguasai sistem yang diretas tersebut.[4]

Terdapat istilah *Hacker* atau dalam bahasa Indonesia biasa disebut sebagai Peretas. Peretas sendiri diartikan sebagai seseorang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer ataupun jaringan komputer milik orang lain yang dapat merugikan orang tersebut ataupun diasari oleh sebuah tantangan dari dirinya sendiri.[5] Hacker sendiri dibagi menjadi dua tipe, yaitu *White Hat Hackers* dan *Black Hat Hackers,* dalam pengertian mengenai *White Hat Hackers* sendiri merupakan peretas sebenarnya, mereka memiliki kemampuan dalam bidang komputer maupun jaringan komputer yang mampu membuat suatu program komputer yang lebih baik daripada yang dirancang.[6]

---

[3] Ronal, 'Tinjauan Yuridis Terhadap Cyber Crime' (Media Neliti, 2015) <https://media.neliti.com/media/publications/149003-ID-none.pdf>, diakses pada 13 Juni 2020.

[4] William Stark, 'Apa yang dimaksud dengan bug? serta apa penyebab bug dalam suatu program?' (Dictio, 2017) <https://www.dictio.id/t/apa-yang-dimaksud-dengan-bug-serta-apa-penyebab-bug-dalam-suatu-program/12466>, diakses pada 05 September 2020.

[5] Fadjar Efendy Rasjid, '*Hacker* Dan Cracker' (Ubaya, 2014) <https://www.ubaya.ac.id/2018/content/articles_detail/148/*Hacker*-dan-Cracker.html>, diakses pada 03 September 2020.

[6] Cepi Prayoga, '10 *Hacker* Berbahaya di Dunia' (CodePolitan, 2017) <https://www.codepolitan.com/10-*hacker*-paling-berbahaya-didunia-5a361efbceca9>, diakses pada 03 September 2020.

Sedangkan yang menjadi pelaku kejahatan teknologi merupakan bagian dari *Black Hat Hackers,* karena mereka merupakan peretas yang menimbulkan kerugian kepada individu lainnya dengan mencari celah keamanan yang belum maksimal dalam suatu perangkat lunak untuk menyusup serta merusak sistem perangkat lunak tersebut.[7] *Black Hat Hackers* menjadi salah satu kategori peretas yang menjalankan aktivitas *Phising.*

Salah satu contoh kasus mengenai aktivitas *Phising* di Indonesia yaitu kasus dengan nomor putusan 30/Pid.Sus/2019/PN.Skg, secara singkat terdakwa dengan nama Suparman dalam kasus ini diduga telah turut serta melakukan aktivitas *Phising,* Suparman pada awalnya membuat alamat *e-mail* untuk diserahkan kepada rekannya yaitu Nursyam alias Ikhsan, Suparman disini meminta Ikhsan untuk dibuatkan sebuah situs yang sama ataupun serupa dengan situs *internet banking* milik Bank BRI.

Setelah situs tersebut selesai dibuat, selanjutnya baik Suparman maupun Ikhsan langsung menyebarkan situs tersebut melalui SMS caster. Situs tersebut berisi muatan yang menuntun korban untuk mengisi data pribadi korban untuk mengajukan kredit atau pinjaman secara online. Korban yang dituju antara lain korban yang memiliki rekening BRI yang terdaftar dalam *internet banking*. Setelah korban selesai memasukkan data pribadi mulai dari *username, password* dan juga *PIN* rekening mereka, terdakwa langsung dapat mengakses rekening korban tersebut lalu mentransferkan isi rekening korban ke rekening milik terdakwa untuk dicairkan.

Suparman dalam kasus ini dapat dikatakan sebagai aktivitas *Phising* dikarenakan terdakwa dalam hal ini melakukan aktivitas yang memancing korban untuk memasukan data pribadi mereka dengan menggunakan situs palsu yang dengan sengaja dibuat oleh terdakwa.

Dalam contoh kasus tersebut terdakwa dikenakan sanksi pidana dalam Pasal 35 Jo. Pasal 51 ayat (1) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi

[7] *ibid.*

Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843, untuk selanjutnya disingkat sebagai UU ITE) Jo. Pasal 55 ayat (1) ke-1 Undang-Undang Nomor 1 Tahun 1946 Republik Indonesia tentang Peraturan Hukum Pidana Untuk Seluruh Wilayah Republik Indonesia dan Mengubah Kitab Undang-Undang Hukum Pidana (*Wetboek van Strafrecht*) Staatsblad Nomor 732 Tahun 1915 (Lembaran Negara Republik Indonesia Tahun 1958 Nomor 127, Tambahan Lembaran Negara Republik Indonesia Nomor 1660 yang selanjutnya disingkat sebagai KUHP) , Pasal-Pasal tersebut dijadikan acuan oleh penuntut umum dalam merumuskan dakwaannya karena terdakwa memenuhi semua unsur yang terdapat dalam Pasal-Pasal tersebut, sedangkan konsep aktivitas *Phising* sendiri belum dikenal dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE), dalam Undang-Undang ITE Pasal 35 sendiri hanya menyebutkan mengenai:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik".

Dalam kutipan Pasal *aquo* tidak menjelaskan secara jelas mengenai konsep dari *Phising* itu sendiri, sehingga belum dapat disimpulkan apakah aktivitas *Phising* dapat dikategorikan sebagai suatu tindak pidana dalam Undang-Undang ITE, karena suatu kegiatan dapat dikatakan sebagai sebuah aktivitas *Phising* apabila pelaku dengan sengaja bertujuan memancing atau menjebak korban untuk memasukan informasi pribadi miliknya sehingga pelaku dapat mengambil alih akses terhadap akun korban, sedangkan dalam Pasal *aquo* hanya menjelaskan bahwa tujuan dari pelaku adalah membuat dokumen palsu maupun informasi palsu agar terlihat seperti dokumen atau informasi elektronik yang otentik.

Adapula tambahan berupa pendapat ahli dalam bidang Informasi dan Teknologi Elektronik yaitu Ronny, dalam memberikan keterangan dalam kasus tersebut beliau mengatakan bahwa tidak semua rekayasa melanggar Pasal 35 UU ITE tergantung motif dan kerugian yang ditimbulkan dan juga bahwa perbuatan

terdakwa dengan cara mengirimkan sms caster kepada para korban tidak dapat dikatakan memenuhi unsur yang ada dalam Pasal 35 UU ITE, namun apabila sms caster tersebut yang bermuatan berita bohong atau yang bersifat menyesatkan maka akan lebih tepat jika dikenakan Pasal 28 ayat (1) UU ITE.[8]

Berkaitan dengan contoh kasus sebagaimana yang telah disebutkan dalam paragraf sebelumnya, maka terdapat suatu permasalahan yang akan dikaji dan dibahas lebih lanjut dalam skripsi ini, yaitu mengenai aktivitas Tindak Pidana *Phising* dalam Undang-Undang ITE.

Perkembangan Aktivitas *Phising*

Seiringnya berjalannya waktu kemajuan teknologi semakin pesat hal ini dikarenakan tujuan dari teknologi itu sendiri adalah untuk memudahkan manusia dalam melakukan aktivitasnya sehari-hari, baik itu dalam melakukan pekerjaan maupun cara berkomunikasi. Dari berbagai kalangan usia saat ini telah menikmati dan menggunakan teknologi yang menjadi bagian penting dalam kesehariannya, mulai dari anak-anak hingga orang tua. Akan tetapi seringkali penggunaan inovasi baru ini tidak diseimbangi dengan adanya edukasi mengenai dampak yang akan ditimbulkan. Dalam penggunaan teknologi khususnya internet beserta berbagai alat elektronik pendukung lainnya, memang memudahkan kita dalam melakukan pekerjaan terlebih bagi mereka yang diharuskan untuk bekerja dengan rekan kerja yang terpaut jauh lokasinya sehingga tidak mudah dijangkau. Sebuah terobosan yang sangat membantu pekerja dalam hal ini adalah alat komunikasi elektronik berupa email karena dengan itu mereka dapat bertukar pesan dan juga mengirim hasil pekerjaan kepada klien.

Namun kemudahan tersebut tentunya selain membawa dampak positif juga membawa dampak negatif yang seharusnya perlu kita ketahui juga sebagai langkah preventif untuk penggunaan jangka panjang. Karena terlena dengan kemudahan yang disediakan oleh teknologi masa kini, kita tidak mengetahui bahaya yang bisa

[8] Pengadilan Negeri Sengkang, "Putusan Nomor 30/Pid.sus/2019/PN.Skg".[25]

saja terjadi di dunia siber karena yang mengakses bukan hanya orang awam saja melainkan juga orang yang sangar mahir di bidang IT juga tentunya menggunakan hal serupa. Bahaya tersebut tidak lain ada cybercrime, yang mana merupakan dampak negatif dari penggunaan teknologi dan internet yang tidak diiringi pengetahuan yang cukup untuk berhati-hati. Berbicara mengenai tindak pidana dalam ruang lingkup siber yang terus mengalami perkembangan baik dalam segi modus operandi maupun jenis kejahatan yang dilakukan, perkembangan kejahatan dalam dunia siber ini dipicu oleh perkembangan teknologi yang sangat cepat.[9]

Terdapat beberapa karakteristik kejahatan dalam dunia siber diantaranya, *Cyberpiracy* yang merupakan perbuatan dimana pelaku mencetak ulang sebuah software atau bisa juga sebuah informasi yang nantinya akan didistribusikan melalui teknologi komputer, lalu ada *Cybertrespass* dimana bertujuan untuk meningkatkan sebuah sistem keamanan dalam akses sebuah komputer pada suatu organisasi atau individu, dan *Cybervandalism* menggunakan teknologi untuk membuat program yang bertujuan mengganggu proses transmisi elektronik dan menghancurkan data pada komputer.[10] Dalam contoh kehidupan sehari-hari semakin banyak pula orang-orang yang berlomba memperbanyak akun jejaring sosial seperti halnya Instagram, Facebook, Snapchat, Twitter, dan sosial media lainnya. Dengan tujuan untuk mencari berbagai informasi maupun artikel dari dalam atau luar negeri, mengetahui kabar seseorang, hingga berjualan secara daring *(online shop)* semua bisa diakses melalui media sosial, seiring dengan hal tersebut membuat semakin banyak penjahat-penjahat dalam dunia siber yang mencari celah dalam setiap akun tersebut.[11]

Salah satu kesulitan dalam menjaring berbagai kejahatan teknologi adalah ketentuan pidana yang berlaku yang mengatur tentang kejahatan tersebut masih dirasa belum lengkap, Di Indonesia terdapat berbagai macam jenis kejahatan siber

[9] Maskun, *Kejahatan Siber (Cyber Crime) : Suatu Pengantar* (Kencana 2013).[50].
[10] Nudirman Munir, *Op.Cit*.[202].
[11] Mia Haryati Wibowo, *Op.Cit*.[1].

yang marak terjadi dalam masyarakat diantaranya:[12]

a. Pembajakan situs web, hal ini dikenal dengan istilah *deface* dimana peretas merubah halaman web dengan cara mengeksploitasi celah yang terdapat pada keamanan web tersebut;
b. *Denial of Service (DoS) attack,* merupakan serangan yang ditujukan kepada sebuah server maupun jaringan komputer yang bertujuan melumpuhkan target tersebut sehingga menyebabkan terjadinya *hang* atau *crash;*
c. *Cybersquatting,* kejahatan yang berhubungan dengan nama domain atau situs, dengan kata lain pelaku membuat sebuah web yang mirip atau identik dengan web milik suatu perusahaan yang bertujuan untuk menarik keuntungan.

Dari berbagai macam jenis kejahatan yang telah diuraikan diatas, yang menjadi poin dalam penulisan skripsi ini adalah jenis kejahatan *cybersquatting* yang mana secara spesifik yaitu *Phising, Phising* sendiri merupakan suatu metode untuk melakukan penipuan dengan cara mengelabui target menggunakan alamat situs palsu dengan maksud untuk mencuri data privasi milik target. Kata *Phising* sendiri berasal dari istilah dalam bahasa inggris yaitu *Fishing* yang memilliki arti "memancing", istilah "memancing" disini digunakan untuk menjebak korban agar memasukan informasi pribadi milik korban dengan maksud tertentu, *Phising* sendiri sering disebarkan para pelaku melalui *e-mail* korban, *e-mail* disini digunakan pelaku untuk menyebarkan situs palsu dengan maksud menjebak korban yang dituju oleh pelaku.[13]

Menurut Dendy Eka Puspawadi, sebagai salah satu ahli dalam bidang informasi dan teknologi elektronik menyatakan bahwa aktivitas *Phising* adalah suatu perbuatan untuk melakukan penipuan dengan mengelabui target dengan maksud untuk mencuri akun target, dengan cara menyebarkan *broadcast* yang seringkali dilakukan melalui email palsu dengan muatan informasi palsu yang mengarahkan

[12] Nudirman Munir, *Op.Cit.*[204-205].

[13] PT Cloud Hosting Indonesia, 'Mengenal Apa itu Phising, Penyebab, dan Mengatasinya' (Id Cloudhost, 2016) <https://idcloudhost.com/mengenal-apa-itu-phising-penyebab-dan-mengatasinya/>, diakses pada 15 September 2020.

target ke halaman palsu untuk menjebak target sehingga pelaku mendapatkan akses terhadap akun korban tersebut.[14]

Teknik *Phising* sendiri pertama kali dikenalkan pada tahun 1987 oleh sebuah perusahaan teknologi di Amerika yaitu Hewlett Packard (HP) Group Interex, sedangkan sebutan *Phising* sendiri baru bermula pada tahun 1990-an dimana seorang hacker bernama Khan C. Smith menggunakan teknik *phising* untuk mendapatkan data akun bank pengguna American Online (AOL), yang bertujuan mendapatkan *username* maupun *password* dari pengguna akun tersebut.[15]

Phising juga dikenal sebagai "*Brand Spoofing"* atau *"Carding"* yang mana berarti *Phising* merupakan sebuah bentuk layanan yang menipu seseorang dengan menjanjikan sebuah keabsahan dan keamanan dari transfer data yang dilakukan orang tersebut. menurut Felten et al spoofing (1997), *phising* didefinisikan sebagai teknik yang digunakan hacker untuk dapat mengakses sebuah komputer secara tidak sah yang mana menimbulkan sebuah ancaman. Adapula aspek-aspek ancaman sebuah web terkena virus yang dilakukan oleh pelaku *Phising* diantaranya:[16]

a. Manipulasi Link, dimana pelaku *Phising* membuat sebuah link yang mirip dengan aslinya tetapi dengan ejaan sehingga terlihat seperti situs yang asli.
b. *Filter Evasion*, mengecoh pengguna dengan menggunakan email dengan tautan sebuah link yang dihubungkan dengan alamat web yang sah padahal web tersebut merupakan web buatan pelaku *phising* sehingga pengguna atau korban *phiser* memasukan informasi pribadi miliknya.
c. *Website Forgery*, teknik ini memanfaatkan celah pada keamanan sebuah website lalu menggunakannya untuk memasang link pada file multimedia, pada beberapa kasus celah yang digunakan pelaku adalah *cross site scripting* (xss), yang mana pelaku menanamkan sebuah link yang tidak sah kedalam sebuah website yang sah.

[14] Pengadilan Negeri Jember, "Putusan Nomor 650/Pid.sus/2019/PN.Jmr".[10].
[15] Dian Rachmawati, 'Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber' (2014) 13 Jurnal SAINTIKOM.[211].
[16] *ibid.*[212].

Phising di dunia mulai marak pada tahun 2000 dengan merebaknya sebuah sistem pembayaran elektronik, dimana membuat para hacker mendapatkan celah lebih banyak dalam melakukan aksinya, seperti pada kasus 2003-2004 pengguna e-gold sebanyak 1,2 juta komputer berhasil diretas menggunakan *phising*, dan total kerugian yang ditimbulkan mencapai 2 milyar USD. Hingga tahun 2008 sangat banyak akun yang diretas dengan cara *phising* dimana pada tahun tersebut muncul *cryptocurrency* seperti bitcoin membuat semakin mudahnya peretas melakukan praktik *phising*.[17]

Di Indonesia sendiri Kasus *Phising* yang paling terkenal adalah kasus dari Internet banking milik bank BCA pada tahun 2001, saat itu terdapat seseorang berinisial Steven Haryanto yang membeli beberapa domain yang mirip dengan domain milik bca yaitu klikbca.com, Steven Haryanto sendiri melakukan aksinya dengan membuat domain serupa dengan mengubah ejaan dari website asli seperti clickbca.com, klickbca.com, klikbac.com. Steven Haryanto juga mendesain website tersebut sedemikian rupa sehingga mirip dengan website asli milik bca sehingga banyak orang yang tertipu.[18] Namun Steven Haryanto melakukan hal tersebut bukan untuk mencuri data dari nasabah, melainkan Steven Haryanto bertujuan untuk menguji tingkat keamanan dari situs milik bank BCA tersebut, akan tetapi perbuatan Steven Haryanto yang mengganggu sebuah sistem milik orang lain yang dilindungi privasinya dan pemalsuan situs internet banking milik BCA sehingga perkara ini dikategorikan sebagai perkara perdata.[19]

Dari berbagai pengertian mengenai *phising* yang sudah diuraikan diatas, dapat diketahui cara kerja *phising* memiliki tujuan untuk mendapatkan informasi rahasia dari korban, terdapat beberapa dampak yang timbul yang diakibatkan oleh pelaku *phising*, jenis kerugian yang dapat ditimbulkan berupa kerugian materiil

[17] Aliya Hafiz, 'Sejarah, Cara Kerja, Dan Tool Phising' (Aliyhafiz, 2020) <https://aliyhafiz.com/pengertian-sejarah-cara-kerja-tool-phishing/>, diakses pada 02 November 2020.

[18] Eril, 'langkah terbaik untuk mengatasi Phising dan Pencegahannya' (Gudang. SSL, 2020) <https://gudangssl.id/mengatasi-phising/>, diakses pada 02 November 2020.

[19] Setiyardi, 'Kreasi Pelesetan Pemicu Delik' (Tempo, 2017) <https://majalah.tempo.co/read/ilmu-dan-teknologi/80886/kreasi-pelesetan-pemicu-delik/>, diakses pada 02 November 2020.

maupun non-materiil. Pengetahuan pengguna teknologi yang minim terhadap alat yang digunakan menjadi sasaran empuk bagi para pelaku *phising*, maka dari itu diperlukan adanya pengetahuan dalam mengoprasikan sebuah teknologi, pada dasarnya yang menjadi celah dari adanya tindak pidana dalam ruang lingkup siber adalah kurangnya pengetahuan pengguna akan teknologi itu sendiri.

Tahapan Dan Modus Operandi Yang Dilakukan Pelaku Tindak Pidana *Phising* Dalam Dunia Siber

Di Indonesia ditemukan beberapa penyebab utama adanya kejahatan siber diantaranya akses terhadap internet yang tidak terbatas, pengguna komputer yang lalai, tingkat keamanan dan resiko yang kecil sehingga cukup mudah untuk dilakukan, kurangnya perhatian mengenai kejahatan siber itu sendiri.[20] Dengan kata lain terdapat sangat banyak kekurangan yang terdapat dalam edukasi masyarakat di Indonesia yang akibatnya membuat peretas dengan mudah masuk ke dalam sistem komputer orang lain yang ditujunya maupun merusak sistem tersebut.

Pelaku kejahatan dalam dunia siber merupakan orang-orang yang pintar, dalam hal ini dikarenakan para pelaku menguasai mengenai sistem komputer dan juga sangat ahli dalam mencari celah-celah keamanan dalam sebuah sistem komputer, dapat dikatakan mereka memiliki penguasaan dalam komputer lebih daripada orang pada umumnya. Pelaku dalam kejahatan siber juga memiliki latar belakang yang sangat beragam dan tidak memiliki klasifikasi tertentu, para hacker tidak mengenal usia, dan status mereka dalam kehidupan bermasyarakat pun sangat beragam, mulai dari pelajar, ibu rumah tangga, pejabat perusahaan, dan lain-lain. Namun terdapat beberapa karakter khusus umum yang selalu menjadi ciri khas para hacker, antara lain:[21]

1. Pemuja kesenangan, hal ini dinilai dari kesenangan mereka apabila berhasil membobol pertahanan atau keamanan sistem komputer yang sudah dirancang sedemikian rupa, karena hal tersebut dianggap dapat menguji kemampuan dan mengasah otak mereka.

[20] Nudirman Munir, *Op.Cit.*[212].
[21] Maskun, *Op.Cit.*[68].

2. Manusia-manusia kreatif, kebanyakan hacker tidak memiliki sumber daya yang mumpuni, sehingga mereka harus memutar otak agar dapat memecahkan masalah sistem yang ada.
3. Tidak mudah bosan, hal ini dinilai dari kebiasaan mereka yang sanggup duduk berjam-jam di depan layar komputer untuk mengerjakan hal yang berulang-ulang dan cenderung membosankan, biasanya diperlukan waktu 48 jam untuk mengamati lalu lintas data atau sebuah kegiatan yang berlangsung dalam jaringan komputer.
4. Menginginkan kebebasan absolut, para *hacker* adalah orang yang apabila dilarang justru akan dilakukan, maka dari itu musuh utama para *hacker* adalah birokrasi dan otoritas pemerintah yang selalu merahasiakan sesuatu, mereka dengan tegas mengatakan tidak akan berhenti apabila belum mendapatkan akses kedalam sistem yang mereka inginkan secara bebas.

Para peretas akan selalu mencari titik kelemahan atau sebuah celah dalam keamanan sebuah sistem komputer, akan tetapi tidak semua peretas memiliki motif yang sama, dalam beberapa kasus *phising* sendiri walaupun dianggap sebagai sebuah tindakan yang merugikan pengguna internet bukan berarti semua pelaku *phising* memiliki niatan buruk, seperti contoh kasus Steven Haryanto yang telah dijabarkan sebelumnya, dia hanya ingin mengetahui bagaimana tingkat keamanan dalam internet banking milik bank BCA, dengan kata lain *phising* dibagi menjadi beberapa kategori karena tidak semua pelaku memiliki motif yang sama.

Seperti uraian yang telah dijelaskan diatas bahwa *phising* dikategorikan kedalam berbagai jenis berdasarkan motif pelaku dan juga target yang ingin ditujunya, yaitu:[22]

a. *Spear Phising*, dimana pelaku memiliki target yang spesifik, dengan kata dasar *Spear* yang memiliki arti tombak, sehingga dalam jenis ini pelaku memiliki peluang berhasil lebih tinggi karena target yang ditujunya lebih jelas.
b. *Whaling*, jenis *phising* ini hampir sama dengan spear *phising*, akan tetapi target yang dituju adalah orang dengan jabatan tinggi dalam suatu organisasi, seperti contoh para pejabat ataupun eksekutif sebuah perusahaan, pelaku *phising* dalam jenis ini menggunakan media subpoena, dimana subpoena merupakan dokumen panggilan tertulis yang berisi agar korban yang dituju menghadap ke muka pengadilan, dengan tujuan untuk menakuti korban.
c. *Clone Phising*, *phising* jenis ini merupakan *phising* konvensional, dimana pelaku *phising* meggunakan email yang sah dan mengirimkan sebuah pesan yang identik

[22] Aliya Hafiz, 'Sejarah, Cara Kerja, Dan Tool Phising' (Aliyhafiz, 2020) <https://aliyhafiz.com/pengertian-sejarah-cara-kerja-tool-phishing/>, diakses pada 02 November 2020.

dengan isi email asli kepada korban dengan mengganti file lampiran isi pada pesan dalam email tersebut.

d. *Covert Redirect*, merupakan teknik yang sangat halus dimana pelaku merubah link yang terlihat resmi tapi sebenarnya menuju link yang dibuat oleh pelaku melalui pop up login, pada teknik ini target lebih susah mengenali karena pelaku menggunakan link maupun situs resmi dengan pop-up yang sudah dimodifikasi, sehingga tidak mudah mengetahui apakah itu merupakan form login asli atau bukan.

Disini yang perlu dibuktikan apakah seseorang telah melakukan *phising* atau tidak adalah dengan menenentukan motif dari pelaku. Selain Motif pelaku tentu adanya sarana atau media juga merupakan hal yang penting apabila seseorang melakukan *phising*, dari definisi *phising* yang telah dijelaskan sebelum-sebelumnya maka cara kerja *phising* ini membutuhkan sebuah sarana berupa komputer dan juga internet, selain itu para pelaku *phising* juga ada yang membutuhkan dana untuk membuka sebuah domain baru yang nantinya bertujuan untuk menipu target yang ditujunya, cara kerja *phising* dibedakan dalam berbagai bentuk;[23]

a. *E-mail Phising,* pada awalnya pelaku mengirimkan email palsu yang mengatasnamakan sebuah organisasi yang dikenal korban, lalu pelaku meminta korban untuk memperbarui data dirinya melalui link URL yang telah dicantumkan dalam email tersebut.
b. *Website Phising,* pelaku *phising* membuat sebuah domain website yang mirip dengan website asli sebuah organisasi atau perusahaan yang mana bertujuan untuk mengelabui korban agar memasukan informasi pribadi seperti *password* dan rekening bank.
c. *Malware Phising,* malware sendiri merupakan sebuah program komputer yang dirancang untuk menginfeksi sebuah sistem dalam komputer tanpa diketahui *user* komputer tersebut, cara kerja pelaku *phising* ini adalah dengan mengirimkan sebuah file kepada korban agar korban yang dituju mengunduh file yang didalamnya sudah berisi virus yang sehingga pelaku *phising* dapat dengan leluasa mengakses sistem komputer milik korban.

[23] Mia Haryawati Wibowo, 'Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime', (2017), 1 *JOEICT (Jurnal Of Education And Information Communication Technology)*.[3].

Beberapa modus yang dilakukan para pelaku *phising* adalah dengan menjebak korbannya agar secara tidak sadar memberikan data pribadi miliknya, para pelaku *phising* selalu menggunakan rangkaian kebohongan dan juga tipu muslihat, ciri-ciri umum tipu muslihat yang terjadi pada *E-mail Phising* dalam menjebak korbannya adalah dengan memainkan kata-kata dalam *subject* dan juga *content* email tersebut sehingga korban mempercayai bahwa email tersebut adalah asli, sebagai contoh permintaan untuk memverifikasi akun, lalu ancaman apabila tidak merespon dalam waktu tertentu maka akun akan ditutup, yang ketiga memakai kata sopan seperti "*Dear Valued Costumer"* karena kebanyakan pelaku *phising* memiliki target yang random dan terkadang bisa jadi langsung menggunakan nama korban, dan contoh terakhir dengan mencantumkan tautan alamat web dan menyuruh korban untuk mengklik link tersebut agar dapat mengakses akun korban.[24]

Dalam *Website Phising,* dikenal dengan istilah *Web Forgery* dikarenakan situs atau web ini dibuat dengan tujuan hanya untuk menipu pengunjungnya, yang mana cara kerja *phising* ini adalah dengan pelaku membuat sebuah domain di internet dimana dia menjadi hostnya, hal ini biasa disebut sebagai *web hosting*, dalam proses pembuatan web ini pelaku bisa memilih apakah akan menggunakan domain berbayar atau yang gratis, setelah mendapatkan domain yang diinginkan pelaku akan mulai merancang website miliknya tersebut yang mana tampilan dari website ini nantinya akan dibuat semirip mungkin dengan website asli dengan website yang akan ditirunya, mulai dari penataan layout, logo milik perusahaan, pewarnaan, objek yang disertakan, hingga detail kecil yang ada, sehingga korban akan tertipu dan memasukan data pribadi miliknya kedalam form yang berisi seperti *password* dan *username* korban yang nantinya data tersebut akan secara otomatis tersimpan dalam *database* website tersebut.[25]

---

[24] Nur Khalimatus Sa'diyah, 'Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik', (2012), 17 Perspektif.[84].

[25] Ki Jagad Tomara, "Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs Phising", Skripsi (Universitas Brawijaya 2011).[56].

Suatu perbuatan dapat dikatakan sebagai tindak pidana apabila perbuatan tersebut dirumuskan dalam suatu delik atau tindak pidana, dan bagi pelanggarnya dapat dijatuhi sanksi pidana.[26] Contoh delik pidana dalam KUHP yang dapat dikenakan sebagai sanksi terhadap pelaku *phising*, contohnya yaitu penipuan yang diatur dalam Pasal 378 KUHP, ketentuan dalam Pasal tersebut dapat dikenakan pada pelaku tindak pidana *phising* karena pada dasarnya *phising* merupakan kasus penipuan secara online, dimana pelaku menggunakan *e-mail* ataupun *website* palsu yang berisikan muatan berisi tipu muslihat ataupun rangkaian kebohongan yang bertujuan untuk mengecoh korbannya agar tergerak untuk memberikan data pribadi miliknya.

Pengaturan Terhadap Tindak Pidana *Phising* Dalam Hukum Positif Indonesia

Dalam praktik di Indonesia aturan mengenai hukum siber merupakan suatu hal yang memiliki tantangan tersendiri, hal ini karena peraturan perundang-undangan yang mengatur mengenai hukum siber sendiri dinilai masih "seumur jagung".[27] kedudukan hukum siber membawa implikasi kedalam perubahan yang terjadi di dalam masyarakat, perubahan seperti semakin canggihnya teknologi komputer telah membantu manusia dalam kehidupan sehari-hari yang lebih mudah terutama pada bidang pekerjaan, penyalahgunaan teknologi komputer sebagai sarana untuk melakukan kejahatan dalam perkembangannya menimbulkan persoalan yang cukup rumit terutama pada proses pembuktian pidananya, hal ini dikarenakan kejahatan yang dilakukan dengan komputer dinilai memiliki karakteristik sendiri sehingga berbeda dengan kejahatan pada umumnya.[28]

Klasifikasi kejahatan dalam hukum siber yang diatur dalam UU ITE dijelaskan pada Pasal 27 sampai Pasal 37, dalam pasal-pasal tersebut mengatur lebih lanjut mengenai klasifikasi kejahatan dalam dunia siber seperti contoh pasal 27 mengatur mengenai pelanggaran kesusilaan, perjudian, pencemaran nama baik,

[26] Didik Endro Purwoleksono, *Hukum Pidana* (Airlangga University Press 2015).[45].
[27] Maskun, *Op.Cit.*[58].
[28] *ibid*.[17].

dan tindakan pemerasan dan pengancaman.[29] Unsur-unsur yang terdapat dalam pasal 27 merupakan pengembangan modus kejahatan seperti yang terdapat pada KUHP hanya saja pada UU ITE modus kejahatan dilakukan dengan media komputer.[30]

Sebelum berbicara mengenai aturan yang berlaku di Indonesia, terlebih dahulu akan dijelaskan mengenai yurisdiksi *cyber space*. Yurisdiksi sendiri merupakan kekuasaan atau kompetensi hukum suatu Negara terhadap orang, benda maupun peristiwa hukum yang direfleksikan dari prinsip dasar kedaulatan, kesamaan derajat, dan tidak campur tangan sebuah Negara. Makna dari yurisdiksi sendiri selalu membahas mengenai persoalan wilayah, akan tetapi dalam praktiknya setiap Negara tetap memiliki kedaulatan untuk mengadili suatu tindak pidana yang dilakukan diluar wilayah negaranya, dikarenakan hal tersebut didasari dengan adanya prinsip-prinsip dalam Hukum Internasional yang berlaku, diantaranya:[31]

1. Prinsip teritorial, dalam hal kejahatan siber prinsip ini dapat digunakan karena dalam perkembangannya mengalami perluasan makna sehingga dapat meliputi perbuatan pidana yang dilakukan menggunakan media komputer atau internet, yang seharusnya bersifat tidak dapat disentuh.
2. Prinsip nasionalitas, memiliki makna suatu Negara dapat mengadili warga negaranya dimanapun dia berada, prinsip ini dibedakan menjadi dua, yaitu prinsip nasional aktif dan juga prinsip nasional pasif.
3. Prinsip perlindungan, prinsip ini merupakan sebuah upaya sebuah Negara untuk melindungi kepentingan vital Negara tersebut, sehingga Negara memiliki kewenangan untuk mengadili Warga Negara Asing yang berbuat kejahatan di dalam maupun luar negaranya yang mengancam keamanan Negara tersebut.
4. Prinsip universal, menilai bahwa setiap Negara memiliki kewenangan untuk mengadili tindak kejahatan tertentu, dan hal tersebut diterima secara umum karena dianggap sebagai tindakan yang mengancam masyarakat internasional.

Dalam menentukan kewenangan hukum pidana siber di Indonesia, diuraikan dari segi tempat atau biasa disebut *locus delicti* yang mana untuk menentukan apakah hukum pidana Indonesia berlaku untuk mengadili perbuatan pidana tersebut atau tidak, berhubungan dengan kompetensi relatif pengadilan mana yang berwenang mengadili perkara tersebut.[32]

---

[29] *ibid*.[33].
[30] *ibid*.[34].
[31] *ibid*.[93-98].
[32] Moeljatno, *Asas-Asas Hukum Pidana (Edisi Revisi)* (Rineka Cipta 2008).[85].

Dalam kasus *phising* sendiri merupakan kejahatan yang hanya memerlukan ruang maya untuk melakukan aktivitasnya, sehingga seperti yang telah dijelaskan mengenai pembahasan yurisdiksi diatas, bahwa teori-teori yurisdiksi dalam suatu Negara pada bidang siber telah dikembangkan mengingat ruang siber sendiri merupakan bentuk perluasan lingkungan hidup manusia, sehingga Indonesia memiliki wewenang untuk mengadili perbuatan pidana yang dilakukan di dalam maupun di luar Negara Indonesia selama dianggap merugikan kemanan maupun kepentingan Negara.[33]

Dalam merumuskan delik pidana pada pidana *phising* sendiri, mengacu pada pembahasan mengenai *phising* sebelumnya, beberapa pasal dalam KUHP yang dijadikan acuan dalam menjatuhkan pidana *phising* yaitu terdapat pada pasal 378, Pasal 263, dan pasal 362 KUHP. Pada pasal 378 KUHP mengenai penipuan yang mengatakan bahwa barangsiapa secara melawan hukum menggunakan nama atau martabat palsu untuk menguntungkan diri sendiri atau orang lain dengan tipu muslihat atau rangkaian kebohongan yang bertujuan menggerakan orang tersebut untuk menyerahkan sesuatu atau memberi sesuatu diancam karena penipuan dengan pidana penjara paling lama empat tahun, maka dari itu pembahasan berikutnya penulis akan membedah mengenai unsur-unsur yang terdapat pada pasal 378 KUHP sehingga dapat dikatakan sebagai pasal yang menjadi salah satu acuan dalam menjatuhi pidana *phising* itu sendiri.

Pertama mengenai unsur Barangsiapa, yang dimaksud dengan unsur tersebut adalah mengenai subjek hukum itu sendiri, yang mana subjek hukum ini dapat berupa orang maupun badan hukum yang dinilai dapat mempertanggungjawabkan perbuatannya menurut hukum.[34] Lalu yang kedua terdapat unsur menguntungkan diri sendiri, jika sudah berbicaara mengenai tindak pidana *phising*, dapat disimpulkan kebanyakan pelaku phising menggunakan kemampuan mereka demi meraup keuntungan dari orang lain walaupun kebanyakan tidak dalam bentuk uang ataupun barang.

---

[33] Ayu Putriyanti, 'Yurisdiksi di Internet/Cyberspace', (2009), 9 *Media Hukum*.[15].
[34] Pengadilan Negeri Pagar Alam, "Putusan No : 60/Pid.B/2018/Pn.Pga".[12].

Unsur memakai nama palsu atau martabat palsu dengan tipu muslihat atau rangkaian kebohongan, seringkali ditemukan pelaku tindak pidana *phising* menggunakan nama ataupun martabat palsu yang bertujuan untuk mengecoh korbannya, telah dijelaskan bahwa pelaku *phising* bertujuan untuk memancing korbannya, dengan kata lain pelaku sebisa mungkin harus memakai nama ataupun martabat sebuah organisasi atau perusahaan besar, lalu isi *e-mail* maupun website palsu tersebut juga harus didesain sedemikian rupa agar mirip dengan aslinya, hal tersebut bertujuan agar korban dapat dengan mudah percaya mengenai keaslian *email* atau website palsu milik pelaku *phising.*

Yang terakhir unsur menggerakan orang lain untuk menyerahkan suatu barang, meskipun dalam konteks *phising* yang menjadi sasaran bukan merupakan sebuah barang, melainkan data pribadi korban, namun tetap saja hal tersebut dianggap memenuhi unsur pada pasal 378 KUHP, karena pada dasarnya data pribadi juga merupakan sebuah benda yang tidak berwujud namun dapat dibuktikan keberadaannya.

Adapula pengaturan dalam pasal 263 KUHP mengenai pemalsuan surat, seperti yang telah dijelaskan sebelumnya mengenai perbuatan *phising* sendiri merupakan tindakan penipuan dimana pelaku membuat sebuah *e-mail* palsu atau website palsu yang seolah-olah *email* atau website tersebut adalah asli, dan juga dikarenakan belum adanya pengaturan mengenai *phising* lebih lanjut maka dari itu pasal 263 mengalami perluasan makna, karena *e-mail* disini juga dianggap sebagai sebuah surat namun dalam bentuk elektronik. Adapula unsur-unsur yang terdapat pada pasal tersebut juga sesuai dengan pengertian phising yang telah dijelaskan sebelumnya. Berikut ini akan dijelaskan mengenai unsur-unsur yang terdapat pada pasal tersebut sehingga dapat dikenakan pada pelaku tindak pidana *phising*.

Pertama, unsur membuat surat palsu atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan atau pembebasan hutang, atau yang diperuntukan sebagai bukti daripada suatu hal, sebagaimana *phising* merupakan tindakan pidana yang didasari dengan penipuan maka dari itu dalam melaksanakan aktivitasnya para

pelaku *phising* disini membuat surat elektronik atau *e-mail* yang mengatasnamakan sebuah organisasi agar dianggap seolah-olah *e-mail* tersebut adalah asli, isi dari *e-mail* tersebut meliputi tautan yang berisikan sebuah link untuk memperbarui data pribadi korban.

Unsur kedua dengan maksud untuk memakai atau menyuruh orang lain memakai surat tersebut seolah-olah isinya benar dan tidak palsu, dari unsur tersebut dapat dilihat merupakan tujuan dari *phising* itu sendiri, yang mana korban dituntun dengan menggunakan isi *e-mail* yang seolah-olah asli bertujuan untuk memperbarui data pribadi korban yang nanti akan digunakan oleh pelaku tindak pidana *phising* dengan sewenang-wenang seperti berbelanja menggunakan kartu kredit maupun uang rekening korban,[35] hal tersebut juga memenuhi unsur terakhir dari pasal 263 KUHP yang menyebutkan bahwa pelaku akan diancam pidana apabila pemakaian tersebut menimbulkan kerugian pada korban karena pemalsuan surat.

Pasal 362 KUHP mengenai pencurian juga menjadi salah satu acuan penuntut umum dalam mendakwakan tuntutannya pada pelaku tindak pidana *phising* karena tindak pidana *phising* sendiri merupakan sebuah rangkaian perbuatan yang memiliki tujuan untuk mengambil sesuatu atau seluruhnya milik korban yang dituju dengan maksut untuk dimiliki secara melawan hukum, disini pelaku *phising* sendiri secara umumnya memiliki tujuan untuk mencuri data pribadi milik korban dengan tujuan memakai data pribadi tersebut untuk keuntungan pribadi pelaku.

Dalam KUHP sendiri pengaturan mengenai hukum dalam bidang siber masih dibahas secara umum, di dalam peraturan hukum Indonesia dikenal asas *Lex Specialis derogat legi Generalis* yang memiliki arti perundang-undangan atau aturan hukum yang khusus mengesampingkan perundang-undangan atau aturan hukum yang umum, dengan kata lain di Indonesia terdapat undang-undang yang mengatur mengenai hukum siber lebih khusus yaitu Undang-undang Informasi dan Transaksi Elektronik, pengaturan mengenai perbuatan yang dilarang dalam hal menggunakan teknologi informasi diatur dalam undang-undang tersebut, UU

[35] Pengadilan Negeri Cirebon, "Putusan No : 155/Pid.Sus/2018/PN.Cbn".[29].

ITE dijadikan acuan dalam merumuskan perbuatan pidana *phising* di Indonesia, walaupun tidak dirumuskan secara rinci mengenai *phising* itu sendiri akan tetapi para penegak hukum di Indonesia memakai pasal-pasal tersebut dalam merumuskan dakwaannya.

Sebagaimana telah dijelaskan sebelumnya, UU ITE mengatur mengenai perbuatan yang dilarang dalam menggunakan teknologi informasi lebih rinci, adapula pasal yang sekiranya dapat dikenakan kepada pelaku tindak pidana *phising* sebagaimana pengertian mengenai *phising* yang telah dijelaskan pada sub-bab sebelumnya, diantaranya Pasal 28 ayat (1) jo. Pasal 45A ayat (1), lalu Pasal 30 ayat (2) jo. Pasal 46 ayat (2), dan juga Pasal 35 jo. Pasal 51 ayat (1) UU ITE.[36]

Perbuatan para pelaku *phising* tidak hanya sekedar memanipulasi sebuah website ataupun *e-mail* untuk mengecoh korban, tapi juga dalam rangkaian perbuatannya pelaku *phising* juga melakukan kebohongan yang bertujuan menipu korbannya atau dengan kata lain menyesatkan korbannya, sehingga korban mengalami kerugian. Dalam unsur yang terdapat pada pasal 28 ayat (1) melarang bagi siapapun untuk melakukan perbuatan yang dapat menyesatkan orang lain sehingga menimbulkan kerugian konsumen dalam transaksi elektronik. Kerugian yang ditimbulkan dari tindak pidana ini dikarenakan informasi pribadi milik korban diketahui oleh pelaku dan dapat digunakan secara sewenang-wenang. Apabila dikaitkan dengan Penipuan yang diatur pada KUHP maka dapat terlihat bahwa terdapat perbedaan yang mendasar pada Unsur Transaksi yang terjadi. Pada Tindak Pidana *phising* hanya mencakup perbuatan menyesatkan dalam transaksi elektronik saja, Artinya untuk transaksi yang bersifat konvensional tidak dapat dikenakan Pasal 28 Ayat (1) Undang-Undang ITE.

Sedangkan dalam Pasal 30 ayat (2) UU ITE sendiri dikenakan terhadap pelaku yang mengakses sistem elektronik ataupun komputer yang bertujuan untuk memperoleh informasi elektronik maupun dokumen elektronik yang mana hal tersebut merupakan tujuan daripada *phising* itu sendiri, dalam penjelasan

[36] Ardi Saputra Gulo, 'Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik' (2020) 1 PAMPAS: Journal of Criminal.[75-76].

pasal tersebut juga menjelaskan mengenai teknis mengenai perbuatan yang dilarang dapat dilakukan dengan cara mengirimkan hal-hal tersebut pada orang yang tidak berhak atasnya. Dalam melakukan *phising* pelaku akan mengirimkan sebuah dokumen kepada korbannya yang bertujuan agar memperoleh informasi atau dokumen elektronik milik korban, dalam pasal 46 ayat (2) sendiri mengatur mengenai sanksi pidana yang berlaku apabila terdapat orang yang melanggar pasal 30 ayat (2) tersebut. Apabila dikaitkan dengan Tindak pidana pencurian yang diatur pada KUHP maka dapat terlihat perbedaan mendasar pada pengambilan barang yang terjadi. Pada Tindak pidana *Phising* barang yang diambil tanpa hak oleh pelaku adalah data-data berupa informasi elektronik, Artinya Tindak pidana *phising* merupakan pencurian yang memilki cirikhas lebih khusus dibandingkan dengan tindak pidana pencurian biasa.

Selanjutnya pada pasal 35 UU ITE, dalam beberapa kasus mengenai *phising* pasal ini merupakan pasal yang paling sering digunakan oleh para penegak hukum dalam merumuskan hukuman yang berlaku bagi para pelaku *phising*, dalam pasal ini terdapat unsur sebagai berikut:

- Setiap Orang;
- Dengan sengaja dan tanpa hak atau melawan hukum;
- Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan, Informasi Elektronik dan/atau Dokumen Elektronik;
- Dengan tujuan Informasi Elektronik dan/atau Dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Selanjutnya terhadap sanksi pidana yang diberlakukan bagi siapapun yang melanggar ketentuan dalam pasal tersebut akan dikenakan pasal 51 ayat (1) UU ITE. Pada melakukan aktivitasnya, pelaku *phising* tidak akan luput dari yang namanya melakukan sebuah manipulasi seperti yang telah dijelaskan, dalam melakukan perbuatannya pelaku *phising* akan terlebih dahulu membuat sebuah situs website palsu ataupun sebuah *e-mail* palsu demi mengecoh korbannya, selanjutnya tujuan daripada hal tersebut adalah agar korbannya menganggap seolah-olah website ataupun *e-mail* tersebut merupakan data yang otentik.

Oleh karena itulah, Tindak pidana *Phising* tidak dapat dipersamakan dengan perbuatan-perbuatan yang dimaksud dan diatur dalam KUHP. Hal tersebut

dikarenakan Tindak pidana *phising* dilakukan dalam locus delicti yang berbeda dengan tindak pidana konvensional, Tindak Pidana *phising* lebih berkaitan dengan dunia Siber dan informasi-informasi berupa data elektronik.

Kesimpulan

Phising menurut UU ITE dapat disebut sebagai sebuah tindak pidana, akan tetapi unsur yang terdapat dalam pasal-pasal UU ITE belum ada yang menjelaskan mengenai konsep tindak pidana *phising* secara lengkap, karena konsep phising pada kenyataannya tidak hanya mengenai perbuatan memanipulasi dokumen elektronik agar dianggap sebagai dokumen yang asli, akan tetapi konsep phising adalah perbuatan seseorang yang menjebak korbannya agar memasukan data pribadi dengan cara membuat sebuah dokumen atau informasi elektronik yang seolah-olah asli.

Daftar Bacaan

Buku

Maskun, *Kejahatan Siber (Cyber Crime) : Suatu Pengantar* (Kencana 2013).

Moeljatno, *Asas-Asas Hukum Pidana (Edisi Revisi)* (Rineka Cipta 2008).

Nudirman Munir, *Pengantar Hukum Siber Indonesia* (Rajawali Pers 2017).

Didik Endro Purwoleksono, *Hukum Pidana* (Airlangga University Press 2015).

Karya Ilmiah

Ki Jagad Tomara, "Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs Phising", Skripsi (Universitas Brawijaya 2011).

Jurnal

Ardi Saputra Ardi Saputra Gulo, 'Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik', (2020), 1 PAMPAS: Journal of Criminal.

Ayu Putriyanti, 'Yurisdiksi di Internet/Cyberspace' (2009) Vol. 9 Media Hukum.

Dian Rachmawati, 'Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber' (2014) 13 Jurnal SAINTIKOM.

Nur Khalimatus Sa'diyah, 'Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik' (2012) 17 Perspektif.

Mia Haryati Wibowo, 'Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime' (2017) 1 JOEICT (Jurnal Of Education And Information Communication Technology).

Laman

BPMPK KEMDIKBUD, 'Dampak IPTEK Terhadap Perubahan Tata Nilai Pada Diri Individu' (m-edukasi, 2016) <https://m-edukasi.kemdikbud.go.id/medukasi/produk-files/kontenkm/km2016/KM2016 37/materi1.html> diakses pada 13 Juni 2020.

Eril, 'langkah terbaik untuk mengatasi Phising dan Pencegahannya' (Gudang. SSL, 2020) <https://gudangssl.id/mengatasi-phising/>, diakses pada 02 November 2020.

Aliya Hafiz, 'Sejarah, Cara Kerja, Dan Tool Phising' (Aliyhafiz, 2020) <https://aliyhafiz.com/pengertian-sejarah-cara-kerja-tool-phishing/>, diakses pada 02 November 2020.

Cepi Prayoga, '10 Hacker Berbahaya di Dunia' (CodePolitan, 2017) <https://www.codepolitan.com/10-hacker-paling-berbahaya-didunia-5a361efbceca9>, diakses pada 03 September 2020.

PT Cloud Hosting Indonesia, 'Mengenal Apa itu Phising, Penyebab, dan Mengatasinya' (Id Cloudhost, 2016) <https://idcloudhost.com/mengenal-apa-itu-phising-penyebab-dan-mengatasinya/>, diakses pada 15 September 2020.

Fadjar Efendy Rasjid, 'Hacker Dan Cracker' (Ubaya, 2014) <https://www.ubaya.ac.id/2018/content/articles_detail/148/Hacker-dan-Cracker.html>,diakses pada 03 September 2020.

Ronal, 'Tinjauan Yuridis Terhadap Cyber Crime' (Media Neliti, 2015) <https://media.neliti.com/media/publications/149003-ID-none.pdf>, diakses pada 13 Juni 2020.

Setiyardi, 'Kreasi Pelesetan Pemicu Delik' (Tempo, 2017) <https://majalah.tempo.co/read/ilmu-dan-teknologi/80886/kreasi-pelesetan-pemicu-delik/>, diakses pada 02 November 2020.

William Stark, 'Apa yang dimaksud dengan bug? serta apa penyebab bug dalam suatu program?' (Dictio, 2017) <https://www.dictio.id/t/apa-yang-dimaksud-dengan-bug-serta-apa-penyebab-bug-dalam-suatu-program/12466>, diakses pada 05 September 2020.

Putusan

Pengadilan Negeri Cirebon, "Putusan No : 155/Pid.Sus/2018/PN.Cbn".

Pengadilan Negeri Jember, "Putusan Nomor 650/Pid.sus/2019/PN.Jmr".

Pengadilan Negeri Pagar Alam, "Putusan No : 60/Pid.B/2018/Pn.Pga".

Pengadilan Negeri Sengkang, "Putusan Nomor 30/Pid.sus/2019/PN.Skg".