



KAJIAN HUKUM TERHADAP TINDAK PIDANA *CYBER PHISING* YANG DIGUNAKAN UNTUK MENGAMBIL DATA PRIBADI PADA *SITUS DIGITAL TRADING* DIHUBUNGKAN DENGAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI TRANSAKSI DAN ELEKTRONIK

Ande Aditya Iman Ferrary, Sri Hartini, Prihatini Purwaningsih

Universitas Ibn Khaldun Bogor, Indonesia

Email: andeaditya@uika-bogor.ac.id

Abstrak

Tindak Pidana *Cyber Phising* yang digunakan untuk mengambil data pribadi pada *Situs Digital Trading* di mana Pelaku setelah membuat situs *phising* tersebut lalu mengirimkan sebuah *e-mail* dengan isi sebuah Link URL yang mengarahkan ke *website* palsu. Dimana didalam isi *e-mail* tersebut, calon korban diperintahkan untuk memperbarui informasi pribadinya, dan korban mengikuti arahan isi *e-mail* untuk memperbarui Informasi Pribadinya di *website phising*. Identifikasi masalah dalam penelitian ini adalah Apa yang menjadi latar belakang tindak pidana *cyber phising* yang digunakan untuk mengambil data pribadi pada situs digital *trading*. Metode penelitian dengan pendekatan masalah yang digunakan adalah metode yuridis sosiologis (empiris). Penelitian hukum empiris adalah suatu model penelitian ilmiah baik kualitatif maupun kuantitatif yang bersifat empirical-sosio-legal. Menganalisis data tersebut penulis menggunakan metode analisis secara kualitatif yaitu menghubungkan masalah permasalahan yang dikemukakan dengan teori yang relevan sehingga data yang tersusun sistematis dalam bentuk kalimat sesuai gambaran dari apa yang telah diteliti. Hasil penelitian adalah dampak terhadap *trader* dengan adanya tindak pidana *cyber phising* yang digunakan untuk mengambil data pribadi pada situs digital *trading*. Salah satu yang sering terjadi antara lain adalah *Cyber Crime Phising*, masyarakat sering tidak menyadari kejahatan *Cyber Crime Phising* sangat merugikan bagi korban yang pernah mengalami kejahatan ini. *Phising (password harvesting fishing)* adalah tindak kejahatan penipuan dengan memanfaatkan *e-mail* palsu atau situs *website* palsu yang bertujuan untuk mengelabui user lain. Pemanfaatan *e-mail* palsu atau *website* palsu ini ditujukan untuk mendapatkan data user tersebut. Upaya yang Dilakukan oleh Pemerintah dalam Mengatasi Tindak Pidana *Cyber Phising* yang Digunakan Mengambil Data Pribadi Pada Situs Digital *Trading*. Kebijakan dalam perundang-undangan mutlak diperlukan oleh para penegak hukum dan pemerintah untuk menaggulangi dan menindak pelaku kejahatan, sama halnya dengan tindak kejahatan mayantara (*cyber crime*), tentunya jenis hukum perundang-undangan haruslah sesuai dengan jenis kejahatan dan cara untuk mengungkap kasus keajahtan dunia maya. Pemerintah republik Indonesia sudah berkoitmen untuk memerangi kejahatan dunia maya.

Kata Kunci: Tindak Pidana *Cyber Phising*, Data Pribadi, Transaksi Elektronik.

A. PENDAHULUAN

Dewasa ini teknologi informasi dan komunikasi telah mengalami perkembangan yang begitu pesat di dunia, terutama di Indonesia yang tidak mau ketinggalan dalam hal penggunaan dan pemanfaatan kemajuan dibidang teknologi informasi dan komunikasi, hal



ini dapat dilihat dari banyaknya masyarakat yang telah menggunakan alat komunikasi dan teknologi seperti komputer atau laptop, *handphone*, dan internet. Kemajuan teknologi ini telah membantu masyarakat dalam hal berkomunikasi lebih efektif dan memudahkan pekerjaan yang sulit menjadi lebih sederhana, sehingga penggunaan dan pemanfaatan teknologi informasi dan komunikasi hampir seluruh bidang kehidupan manusia telah menggunakan teknologi.¹

Kejahatan yang dilakukan oleh *cracking* ataupun *cracker* salah satunya ialah *Phising* karena kejahatan ini tujuannya untuk menguntungkan diri sendiri dan tentunya merugikan pihak lain jika menjadi korban dari *cyber crime* dalam bentuk *phising* ini. Dalam ruang lingkup keamanan komputer, *phising* adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses *phising* ini bermaksud untuk menangkap informasi yang sangat sensitif seperti *username*, *password* dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya atau *legitimate organization* dan biasanya berkomunikasi secara elektronik. *Phising* ini juga biasanya ditujukan kepada pengguna *online banking*, karena menggunakan isian data (ID) pengguna dan kata sandi, dan tidak menutup kemungkinan untuk ditujukan ke pengguna *online* lainnya. Ketika pengguna memasukkan isian data pengguna miliknya dan kata sandinya ke *form login* yang merupakan *fake form login* maka akan diketahui oleh pelaku *cyber crime* dalam bentuk *phising* tersebut. Aksi *phising* ini semakin marak terjadi. Tercatat secara global, jumlah penipuan bermodus *phising* 42% (empat puluh dua persen) dari modus selain *phising* yang dinyatakan dalam *website Anti-Phising Working Group (APWG)*. Hal ini dapat disimpulkan bahwa *cyber crime* dalam bentuk *phising* tersebut sangat banyak terjadi bahkan di seluruh dunia. *Phising* ini juga biasanya dilakukan melalui media-media sosial yang terhubung ke jaringan internet seperti melalui *e-mail* dan *website*.²

Cyber Crime dalam bentuk *phising* saat ini di Indonesia dimungkinkan dapat dikenakan Pasal 35 jo Pasal 51 ayat (1) 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 ayat (1) jo Pasal 45A ayat (1) 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. Pasal 35 dan Pasal 28 berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik *Cyber crime* dalam bentuk *phising* ini merupakan kejahatan siber yang tidak hanya melakukan pemalsuan data pada sebuah *website* palsu yang tampilannya menyerupai *website* aslinya.³

Disimpulkan *phising* adalah perbuatan yang dilakukan oleh seseorang untuk memancing orang lain untuk memasukkan informasi pribadi rahasia pengguna milik orang itu ke dalam sebuah *website* yang telah *dideface* atau diubah mirip dengan yang asli resminya dengan cara menggunakan *e-mail* yang mengarahkan ke situs *web* palsu guna mendapatkan

¹ Ahmad, Amar. 2012. *Perkembangan Teknologi Komunikasi Dan Informasi: Akar Revolusi Dan Berbagai Standarnya*. Universitas Indonesia, Jakarta, hlm.11.

² Al Wisnubroto, 2011, *Konsep Hukum Pidana Telematika*, Universitas Atmajaya, Yogyakarta, hlm.12

³ Josua Sitompul, 2012, *Cyberspace Cyberlaw Tinjauan Aspek Hukum Pidana*, PT.Tatanusa, Jakarta, hlm.28.



informasi pribadi rahasia pengguna orang lain, sehingga muncul sebuah pertanyaan, apakah dalam menangani *cyber crime* dalam bentuk *Phising* di Indonesia tidak hanya dikenakan Pasal 35 jo Pasal 51 ayat (1) dan Pasal 28 ayat (1) jo Pasal 45A ayat (1) saja atau dapat berkaitan dengan pasal-pasal yang lain di dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan juga mungkin dapat dikenakan dengan pasal-pasal diluar Undang-Undang Informasi dan Transaksi Elektronik seperti KUHP.

Trading merupakan suatu proses jual beli mata uang *Digital* yang dapat dikatakan sudah menjadi gaya hidup generasi modern saat ini, kemudian juga apabila nantinya memutuskan untuk menjadi seorang *trader* maka sudah dipastikan membutuhkan aplikasi tradingnya, atau jasa broker untuk melakukan aktivitas jual beli *forex* tersebut, dapat dikatakan bahwa salah satu penyebab kamu mendapatkan hasil dengan keuntungan yang besar adalah terletak pada penentuan broker *forex* tersebut. *Trading* terbaik dan terpercaya yang dapat membantu untuk meraih kesuksesan, sudah tepat berada dalam aplikasi *trading* yang terpercaya maka dipastikan peluang untuk mendapatkan hasil keuntungannya akan semakin besar. *Agrodana Futures* merupakan salah satu *Trade Forex* lokal, karena salah satu hasil besutan dari *broker Agrodana Futures* sendiri.⁴

Beberapa poin yang biasanya dimiliki oleh *platform trading* maupun saham dengan legalitas resmi dan terpercaya, sebagai poin dibawah ini: Akun Demo, Spread yang Direkomendasikan, Regulasi, *Forex Trading Tools*, Layanan Bantuan, Keamanan, Biaya Transaksi, Penarikan Dana dan Penyetoran, *Platform*, Eksekusi Order atau Pemenuhan Order. Informasi elektronik atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik Perbuatan *phising* ini juga tidak hanya membuat sebuah situs yang seolah-olah mirip dengan situs asli yang resmi, namun juga perbuatan *phising* ini melakukan sebuah tindakan kebohongan untuk menipu atau menyesatkan orang lain sehingga menyebabkan orang tersebut mengalami kerugian karena informasi pribadi rahasia orang itu diketahui oleh pelaku *cyber crime* dalam bentuk *phising* tersebut, oleh sebab itu, perbuatan *phising* dapat dikenakan Pasal 28 ayat (1) jo Pasal 45A ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah melakukan tindakan kebohongan.⁵

B. METODE PENELITIAN

Metode merupakan kegiatan ilmiah yang berkaitan dengan suatu cara kerja (sistematis) untuk memahami suatu subjek atau objek penelitian, sebagai upaya untuk menemukan jawaban yang dapat dipertanggungjawabkan secara ilmiah dan termasuk keabsahannya. Metode penelitian merupakan suatu unsur yang mutlak harus ada di dalam penelitian dan pengembangan ilmu pengetahuan. penelitian ini yaitu:

1. Metode Pendekatan

Metode pendekatan masalah yang digunakan adalah metode yuridis sosiologis (empiris). Penelitian hukum empiris adalah suatu model penelitian ilmiah baik kualitatif maupun kuantitatif yang bersifat empirical-sosio-legal, dengan mengambil objek kajian terhadap segi-segi hukum berkaitan dengan Tindak Pidana *Cyber Phising* yang

⁴ Hamzah Hatrik, 2014, *Asas Pertanggungjawaban Korporasi Dalam Hukum Pidana Indonesia*, PT Raja Grafindo Persada, Jakarta, hlm.23.

⁵ Ardi Saputra Ardi Saputra Gulo, 2020, *Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik*, 1 PAMPAS: Journal of Criminal, hlm.21.



Digunakan untuk Mengambil Data Pribadi Pada Situs Digital *Trading* Dihubungkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Transaksi Dan Elektronik.⁶

2. Spesifikasi Penelitian

Penelitian yang dilakukan merupakan penelitian deskriptif analisis yaitu, Tindak Pidana *Cyber Phising* yang Digunakan untuk Mengambil Data Pribadi Pada Situs Digital *Trading* Dihubungkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Transaksi Dan Elektronik dan pendapat para ahli yang bertujuan untuk mencari dan mendapatkan jawaban atas pokok masalah yang akan dibahas lebih lanjut.

3. Teknik Pengumpulan Data

Teknik pengumpulan data yang akan digunakan dalam penelitian ini adalah Penelitian Kepustakaan (*library research*), yaitu dengan mengumpulkan dan mempelajari data sekunder yang berkaitan kajian hukum tentang Tindak Pidana *Cyber Phising* yang Digunakan untuk Mengambil Data Pribadi Pada Situs Digital *Trading* Dihubungkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Transaksi Dan Elektronik. Teknik pengumpulan data sebagai berikut. Studi Dokumen Penulis mempelajari sumber dokumen yang berupa peraturan perundang-undangan, putusan pengadilan, buku-buku dan dokumen, serta artikel yang berkaitan dengan permasalahan yang penulis teliti.

4. Analisis Data

Sebelum melakukan analisis data, data diolah dengan menggunakan metode editing. Editing merupakan proses memilih kembali data yang diperoleh atau melakukan pengecekan ulang terhadap hasil penelitian sehingga data yang dipergunakan relevan dengan judul penelitian serta dapat menghasilkan suatu kesimpulan.⁷

Setelah data diperoleh atau dikumpulkan dari penelitian maka dalam menganalisis data tersebut penulis menggunakan metode analisis secara kualitatif yaitu menghubungkan masalah permasalahan yang dikemukakan dengan teori yang relevan sehingga data yang tersusun sistematis dalam bentuk kalimat sesuai gambaran dari apa yang telah diteliti, menemukan apa yang penting dan telah dibahas untuk mendapatkan suatu kesimpulan.

C. PEMBAHASAN

1. Latar Belakang Tindak Pidana *Cyber Phising* Yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital *Trading*

Banyak orang yang terjun dalam dunia *trading forex* secara *online*, menginginkan penghasilan yang sekejap dalam satu malam saja, namun alih-alih mereka mendapatkan keuntungan, mereka malah bangkrut dalam satu malam, ini di karenakan minimnya pengetahuan para investor pemula di bisnis ini, sebenarnya yang perlu diperhatikan dalam memasuki bisnis ini hanya membutuhkan sebuah kedisiplinan, manajemen keuangan yang baik, control emosi yang stabil, dan strategi masuk pasar yang baik.⁸

Permasalahan kerugian sudah di ketahui, biasanya dalam tahap pembelajaran pertama kali yaitu mengenai dasar-dasar mekanisme pasar atau yang menyebabkan pasar

⁶ Amirudin dan Zainal Asikin, 2011, *Pengantar Metode Penelitian Hukum*. Penerbit PT Raja Grafindo Persada, Jakarta, hlm.12

⁷ Amiruddin dan Zainal Asikin, 2013, *Pengantar Metode Penelitian Hukum*, PT Raja Grafindo Persada, Jakarta, hlm. 35

⁸ Sahuri Lasmadi. 2010. *Tindak Pidana Dunia Maya Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Infomarsi Dan Transaksi Elektronik*. Jurnal Ilmu Hukum, Vol.2 No.4, 39-40, hlm.24.



bergerak pemula tidak mengalami masalah sama sekali, namun saat memasuki cara menganalisa pasar, *trader* sering sekali di bingungkan oleh banyaknya *indicator* yang di pakai dalam menganalisa keadaan pasar, *indicator* sendiri adalah alat yang di pergunakan seorang trader ataupun investor untuk menganalisa pasar, namun karena banyaknya *indicato*.⁹

Baru-baru ini marak terjadinya tindak pidana *Cyber Phising* Yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital Trading. *Phising* yaitu suatu kejahatan jenis baru dalam dunia maya. Dalam artian bahwa kejahatan ini terlahir dalam bentuk kejahatan *cyber* yang sudah ada sejak lama. Adapun cara melakukan *phishing* dalam *digital trading* yaitu:

- a. Pengiriman *e-mail* palsu, yaitu cara ini digunakan untuk memudahkan korban percaya, maka *e-mail* tersebut di desain seperti *e-mail* aslinya dengan gaya Bahasa, kop surat, logo, dengan sedemikian rupa menyerupai bentuk aslinya. *Web Forgery* yaitu situs *web* yang sudah dirancang oleh pelaku.
- b. *Phishing* Melalui SMS (*SMS Phishing*), cara ini menggunakan metode pengiriman pesan pendek atau SMS dimana pelaku akan mengirimkan SMS kepada korban. Cara pelaku mendapatkan nomor korban yaitu dengan melihat nomor-nomor. mohon diinformasikan kembali *user* dan *password internet banking*.¹⁰

Ketentuan Peraturan Perundang-undangan untuk menjerat pelaku tindak pidana *phising* menurut Undang-Undang Informasi dan Transaksi Elektronik:

- a. Pasal 28 ayat (1), menyebutkan bahwa: “Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.”
- b. Pasal 45 ayat (2), menyebutkan bahwa: “Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)”.¹¹

Penyedia jasa internet sebagai penyedia jasa tidak dapat turut dipersalahkan, apabila pengguna jasanya terbukti melakukan tindak pidana. Apabila terbukti turut berpartisipasi dalam perbuatan pidana tersebut, maka penyedia jasa internet dapat dikenai pertanggungjawaban pidana. Karena penyedia jasa internet ini merupakan sebuah korporasi, maka pembebanan pertanggung jawabannya menggunakan sistem pertanggungjawaban korporasi.

2. Dampak Terhadap Trader Dengan Adanya Tindak Pidana *Cyber Phising* Yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital Trading

Salah satu yang sering terjadi antara lain adalah *Cyber Crime Phising*, masyarakat sering tidak menyadari kejahatan *Cyber Crime Phising* sangat merugikan bagi korban yang pernah mengalami kejahatan ini. *Phising (password harvesting fishing)* adalah tindak kejahatan penipuan dengan memanfaatkan *e-mail* palsu atau situs *website* palsu

⁹ Barry Franky Siregar, 2016, *Pertimbangan Hakim Dalam Menjatuhkan Putusan*, Universitas Atma Jaya Yogyakarta, hlm.24.

¹⁰ Dian Ekawati Ismail, 2011, *Cyber Crime di Indonesia. Fakultas Ilmu Sosial Universitas Negeri Gorontalo*, Volume 6 Nomor 3. Gorontalo, hlm.32

¹¹ Hardianto Djanggih, 2013, *Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime*. Jurnal Media Hukum Vol 1 dan 2, hlm.24.



yang bertujuan untuk mengelabui user lain. Pemanfaatan *e-mail* palsu atau *website* palsu ini ditujukan untuk mendapatkan data user tersebut. Penggunaan data *user* seringkali untuk mengirim *e-mail* yang seolah-olah berasal dari sebuah perusahaan resmi, misalnya bank dengan tujuan untuk mendapatkan data-data pribadi seseorang.¹²

Cyber Crime Phising biasanya dilakukan dengan menyamar sebagai orang lain, biasanya dengan situs *web* palsu atau *link* palsu untuk menipu seseorang untuk mendapatkan atau mencuri informasi pribadi. Pada hal ini, penyerang mengirimkan email yang seolah-olah berasal dari nama logo perusahaan, dalam tautan yang berbeda, E-mail tersebut biasanya merupakan tautan *phising* yang seolah-olah ditujukan ke situs *web*.¹³ Pasal 35 setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik. Pasal 48 ayat (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah). Pasal 51 ayat (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). Adapun perkara atau kasus yang pernah terjadi dalam *Cyber Crime Phising*, yaitu pencurian UserID seseorang dengan berkedok penipuan link untuk melakukan kejahatan yang berupa ujaran kebencian dan penyebaran berita palsu atau hoax, pelaku melakukan hal tersebut menggunakan UserID seseorang untuk memanipulasi publik, dengan begitu publik menyangka hal tersebut adalah tindakan korban, padahal ada seseorang yang merupakan pelaku sebenarnya yang mengontrol UserID korban.

Terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “Dengan sengaja dan tanpa hak mendistribusikan dan membuat dapat diaksesnya Informasi Elektronik dan Dokumen Elektronik yang memiliki muatan penghinaan dan pencemaran nama baik, sebagaimana diatur dan diancam pidana dalam Pasal 45 ayat (3) Undang-Undang Republik Indonesia No. 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik jo. Pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana dalam Dakwaan Pertama Subsidair Penuntut Umum.¹⁴

Cara kerja *phising* adalah memanipulasi informasi dan memanfaatkan kelalaian korban dalam situs *digital trading*, menggunakan contoh *web phising* dengan memanfaatkan nama *PayPal* seperti ditemukan *welivesecurity.com*.

a. Pelaku Memilih Calon Korban Situs *Digital Trading*

Tahap awal kegiatan *web phising* akan dimulai dengan menentukan siapa calon korbannya. Pada umumnya, korban yang disukai adalah pengguna *platform*.

b. Pelaku Menentukan Tujuan *Phising*

¹² H. Sofwan Jannah & M. Naufal, 2012, *Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif*. Remaja Rosdakarya, Bandung, hlm.23.

¹³ Rosalinda Elsina latumahina, 2011, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*. Fakultas Hukum Universitas Pelita Harapan Surabaya, hlm.25.

¹⁴ Undang-Undang Republik Indonesia No. 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik



Mendapatkan calon korban yang potensial, pelaku akan mulai memikirkan apa yang akan dicapai dari kegiatan *web phishing* yang dilakukan, menarget *username* dan *password* pengguna untuk menguasai akun, apa malah mendapatkan semua informasi korban melalui sebuah prosedur yang disiapkan.

c. Pelaku Membuat *Website Phishing*

Melancarkan aksinya, pelaku akan mulai menyiapkan *website* palsu untuk melakukan aksi *phishing*. Mulai dari mendesain *website* palsu, memilih nama domain yang mirip dengan domain asli hingga menyiapkan konten dengan tulisan yang meyakinkan.

d. Calon Korban Mengakses *Website Phishing*

Tampilan *website* dan informasi yang meyakinkan, tidak sedikit calon korban yang akhirnya mengakses *website phishing* milik pelaku. Langkah ini biasanya didahului dengan mengajak calon korban melalui *email phishing* atau *link* yang disebarkan via SMS atau akun media sosial.

e. Calon Korban Mengikuti Instruksi Pelaku

Inilah kunci dari terjadinya aksi *phishing*. Jika calon korban melakukan instruksi yang diberikan pelaku, maka pelaku akan berhasil mencapai tujuannya.

3. Upaya yang Dilakukan oleh Pemerintah dalam Mengatasi Tindak Pidana *Cyber Phishing* yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital Trading.

Kebijakan dalam perundang-undangan mutlak diperlukan oleh para penegak hukum dan pemerintah untuk menaggulangi dan menindak pelaku kejahatan, sama halnya dengan tindak kejahatan mayantara (*cyber crime*), tentunya jenis hukum perundang-undangan haruslah sesuai dengan jenis kejahatan dan cara untuk mengungkap kasus keajahtan dunia maya. Pemerintah republik Indonesia sudah berkoitmen untuk memerangi kejahatan dunia maya. Pemberlakuan dan pengesahan Undang-Undang Informasi Dan Transaksi Elektronik Tahun 2008 Atau Undang-Undang ITE 2008 merupakan salah satu babak baru bagi pemerintah republik Indonesia untuk melawan kejahatan berbasis teknologi komunikasi dan informasi. Dengan aturan ini maka akan membuka jalan bagi penegak hukum untuk bertindak dan mengadili pelaku kejahatan teknologi informasi.¹⁵

Semakin pesatnya penggunaan teknologi maka semakin rawan untuk tingkat kejahatannya yang dilakukan oleh orang-orang yang tidak bertanggung jawab untuk melakukan aksinya baik penipuan, pencurian dan pencemaran nama baik melalui internet. Pada bab ini akan dijelaskan dan apa sajakah upaya yang dilakukan oleh pemerintah indonesia dalam menindak kejahatan-kejahatan berbasis teknologi informasi dan komunikasi baik yang dilakukan di dalam negeri maupun oleh sindikat internasional yang beroperasi wilayah kedaulatan Negara Kesatuan Republik Indonesia. Kebijakan memerangi *cyber crime* kebijakan diartikan sebagai rangkaian konsep dan asas yang menjadi garis besar dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak tentang pemerintahan, organisasi dan sebagainya. Pernyataan cita-cita, tujuan, Prinsip dan garis pedoman untuk manakjemen dalam usaha mencapai sasaran.¹⁶

Kebijakan publik dapat bersifat nasional, regional maupun lokal seperti undang-undang, peraturan pemerintah, peraturan presiden, peraturan menteri, peraturan daerah

¹⁵ Hardianto Djanggih, 2013, *Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime*. Jurnal Media Hukum Vol 1 dan 2, hlm.24.

¹⁶ Victor, Jozef Rudy dan Yawan, Jefry Bernhard. 2010. *Cara Mudah Forex Trading Online*. STIH Manokwari, Manokwari, hlm.16



atau provinsi, keputusan gubernur, peraturan daerah Kabupaten atau kota, dan keputusan Bupati atau Walikota, secara Terminologi kebijakan publik (*public policy*) itu ternyata banyak sekali, tergantung dari sudut mana mengartikanya Easton memberikan definisi kebijakan publik sebagai *the authoritative allocation of values for whole society* atau sebagai pengalokasian nilai-nilai secara paksa kepada seluruh anggota masyarakat.

Laswell dan Kaplan juga mengartikan kebijakan publik sebagai *a projected program of goal, value, and practice* atau sesuatu program pencapaian tujuan, nilai-nilai dalam praktek-praktek yang terarah. Pada sub bab ini akan dijelaskan pendekatan-pendekatan hukum apa saja yang telah dilakukan oleh pemerintah Indonesia dalam menaggulangi kejahatan *cybercrime* dalam rangka menaggulangi kejahatan diperlukan strategi yang mantap dari negara dan masyarakat, dan harus dilakukan dengan cara bersama-sama secara simultan. Usaha pertama dilakukan dengan cara pencegahan sebelum melakukan penindakan dengan cara menggunakan sistem peradilan pidana, sedangkan usaha yang kedua dilakukan dengan cara penetrasi melalui penetapan sistem peradilan pidana, usaha penegakan hukum yang sukses perlu ditopang oleh masyarakat, baik pencegahan kejahatan preventif maupun penindakan secara represif.¹⁷

Pada mulanya asas ini menentukan bahwa setiap Negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini diperluas sehingga mencakup pula pada kejahatan kemanusiaan (*crimes against humanity*) misalnya genosida, pembajakan udara dan lain-lain. meskipun dimasa mendatang asas *jurisdiksi universal* ini mungkin dikembangkan untuk internet piracy, seperti computer *cracking*, *carding hacking*, and *viruses*. Namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan pada perkembangan hukum internasional.

Resiko kejahatan *phising* bisa dikatakan sangat tidak main-main. Beberapa orang harus mengalami kerugian yang tidak sedikit atau bahkan kehilangan akun sosial media yang telah memiliki followers jutaan. *Phising* merupakan salah satu *cybercrime* yang marak dilakukan di era digital seperti saat ini. Ada banyak orang berusaha mengambil keuntungan untuk diri sendiri atau pihak lain dengan cara melakukan kegiatan pembohongan untuk mengelabui para korbannya.¹⁸

Cara mengatasi kejahatan *phising* sendiri dapat dikatakan tidak semudah yang dibayangkan. Tentunya pihak kepolisian membutuhkan peran aktif dari masyarakat untuk melaporkan berbagai macam tindakan *phising* yang terjadi. Jika mengalami atau menjadi salah satu korban dari tindakan kejahatan di dunia maya maka melaporkan kepada polisi *cyber*. Sehingga nantinya bisa ada proses hukum yang berjalan untuk menangani kasus yang Anda alami, sangat penting bagi untuk mengetahui ciri ciri kejahatan *phising* agar tidak menjadi salah satu korbannya. Ciri paling umum yang digunakan oleh para pelaku untuk melakukan penipuan yaitu adalah dengan mengiming-imingi hadiah dan kemudian meminta untuk memberikan beberapa data pribadi, oleh karena itu ketika mendapatkan sebuah pesan yang mungkin dirasa tidak masuk akal maka tidak perlu merespon. juga harus berhati-hati ketika ada orang yang mengirimkan link yang terlihat mencurigakan.

Menghindari *Phising* menjadi korban kejahatan melalui internet memang sangat tidak menyenangkan. *Phising* merupakan salah satu dari sekian banyak kejahatan internet. *cybercrime* yang banyak terjadi di era modern lainnya yaitu *skimming*. Walaupun sama-sama *cybercrime* akan tetapi ada *perbedaan skimming dan phishing*. *Skimming*

¹⁷ Kusrini, 2012, *Sistem Pakar dan Teori Aplikasi Trading*. Yogyakarta: Penerbit Andi, hlm.24.

¹⁸ Chakraborty, M., 2012, "The Equity Market Around the Ex-Split Date: Evidence from India", *Vikalpa*, 37(1).



merupakan sebuah tindakan yang dilakukan untuk mengetahui data-data penting. Tujuannya sudah jelas yaitu adalah mendapatkan uang atau keuntungan dari data tersebut. Hampir seluruh kejahatan di dalam dunia digital pasti bertujuan untuk mendapatkan keuntungan baik untuk diri sendiri atau pihak lain. Cara menghindari kejahatan di dunia maya yang paling mudah untuk dilakukan yaitu adalah dengan tidak memberikan *password* atau *username* kepada pihak lain. Selain itu ketika ada seseorang yang tidak dikenal meminta memberikan data-data penting maka tidak perlu memberikan jawaban apapun.¹⁹

Ketika mendapatkan hal-hal yang mencurigakan juga dapat langsung melaporkan kepada pihak berwajib. Aturan hukum kejahatan *phising* sendiri sudah jelas tertuang dalam undang-undang informasi dan transaksi elektronik (UU ITE). Pada intinya adalah untuk menghindari kejahatan melalui dunia maya memang harus dimulai dari diri sendiri. Sangat penting bagi untuk menjaga keamanan data pribadi dan akun sehingga bisa terbebas dari berbagai macam *cybercrime*.

Beberapa resiko kejahatan *phising* yang merugikan, seperti yang sudah dikatakan sebelumnya jika *phising* dapat memberikan kerugian yang sangat besar. Salah satu hal yang paling Umum dilakukan para pelaku kejahatan *phising* yaitu adalah mencuri data-data pribadi. Data-data pribadi yang dimiliki dapat disalahgunakan atau dijual ke pihak lain. Hal seperti ini tentunya akan sangat merugikan. Kasus kejahatan *phising* dalam digital trading yaitu adalah anggota diminta untuk mengisi sebuah *form* berisi tentang pertanyaan data pribadi dan mengatasmakan aplikasi trading. Padahal sebenarnya *form* tersebut hanya digunakan untuk mencuri data pribadi saja. Resiko lain dari korban *phising* juga mengalami kerugian berupa uang.²⁰

Cara Mengatasi *Phising* di *Website Wordpress*. Di sisi lain, jika Anda adalah seorang pemilik *website* yang menjadi sasaran kegiatan *phising*, inilah cara mengatasi kejahatan *online* tersebut di *website Wordpress* :

a. Gunakan *Plugin* untuk Membersihkan *Malware Phising*

Jangan sampai *website* dimanfaatkan untuk sarana pencurian data pengunjung atau pelanggan toko *online*, maka, gunakanlah *plugin* anti *malware* di *website Wordpress*. pilihan *plugin* yang dapat digunakan.

b. Selalu *Update Wordpress*.

Wordpress merupakan *platform* yang rutin melakukan *update*. Selain penambahan fitur, *update* juga digunakan untuk menambah celah keamanan yang kerap dimanfaatkan pelaku *phishing*. Untuk mencegah *website* terserang *malware*

c. Pasang Sertifikat SSL untuk Keamanan *Website*.

Seperti telah dibahas sebelumnya, peran SSL sangat penting untuk menjamin keamanan transaksi di sebuah *website*. Jika belum menggunakannya, segera pasang sertifikat SSL di *website Wordpress*. memasang SSL itu mudah.

d. Lakukan Manajemen Pengguna dengan Ketat

Jika *website Wordpress* dikelola banyak orang, lakukan manajemen pengguna dengan baik.²¹ Jangan berikan hak akses admin ke semua orang. Hak akses *user* harus

¹⁹ Kusriani, 2012, *Sistem Pakar dan Teori Aplikasi Trading*. Yogyakarta: Penerbit Andi, hlm.24.

²⁰ Endri, E. 2012. *Analisis Teknikal dan Fundamental Saham: Aplikasi Model Data Panel*. Jurnal Akuntabilitas, hlm.12.

²¹ Yustisia, Bandung 2016. *Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy*. Prama Arta, Jakarta, hlm.24.



disesuaikan dengan kewenangan dan kemampuannya dalam menjaga keamanan *website* dengan baik.

D. SIMPULAN

- a. Latar Belakang Tindak Pidana *Cyber Phising* Yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital *Trading*.
Banyak orang yang terjun dalam dunia *trading forex* secara *online*, menginginkan penghasilan yang sekejap dalam satu malam saja, namun alih-alih mereka mendapatkan keuntungan, malah bangkrut dalam satu malam, ini di karenakan minimnya pengetahuan para investor pemula di bisnis ini, sebenarnya yang perlu diperhatikan dalam memasuki bisnis ini hanya membutuhkan sebuah kedisiplinan, manajemen keuangan yang baik, control emosi yang stabil, dan strategi masuk pasar yang baik. Permasalahan kerugian sudah di ketahui, biasanya dalam tahap pembelajaran pertama kali yaitu mengenai dasar-dasar mekanisme pasar atau yang menyebabkan pasar bergerak pemula tidak mengalami masalah sama sekali, namun saat memasuki cara menganalisa pasar, *trader* sering sekali dibingungkan oleh banyaknya *indicator* yang di pakai dalam menganalisa keadaan pasar, *indicator* sendiri adalah alat yang di pergunakan seorang *trader* ataupun investor untuk menganalisa pasar.
- b. Dampak terhadap *trader* dengan adanya tindak pidana *cyber phising* yang digunakan untuk mengambil data pribadi pada situs digital *trading*
Salah satu yang sering terjadi antara lain adalah *Cyber Crime Phising*, masyarakat sering tidak menyadari kejahatan *Cyber Crime Phising* sangat merugikan bagi korban yang pernah mengalami kejahatan ini. *Phising (password harvesting fishing)* adalah tindak kejahatan penipuan dengan memanfaatkan *e-mail* palsu atau situs *website* palsu yang bertujuan untuk mengelabui user lain. Pemanfaatan *e-mail* palsu atau *website* palsu ini ditujukan untuk mendapatkan data user tersebut.
- c. Upaya yang Dilakukan oleh Pemerintah dalam Mengatasi Tindak Pidana *Cyber Phising* yang Digunakan Mengambil Data Pribadi Pada Situs Digital *Trading*
Kebijakan dalam perundang-undangan mutlak diperlukan oleh para penegak hukum dan pemerintah untuk menaggulangi dan menindak pelaku kejahatan, sama halnya dengan tindak kejahatan maya (*cyber crime*), tentunya jenis hukum perundang-undangan haruslah sesuai dengan jenis kejahatan dan cara untuk mengungkap kasus kejahatan dunia maya. Pemerintah republik Indonesia sudah berkoitmen untuk memerangi kejahatan dunia maya



DAFTAR PUSTAKA

A. Buku

- Amiruddin dan Zainal Asikin, 2013, *Pengantar Metode Penelitian Hukum*, PT Raja Grafindo Persada, Jakarta
- Arief, Barda Nawawi. 2011. *Kebijakan Legislatif dalam Penanggulangan Kejahatan Dengan Pidana Penjara*. Universitas Diponegoro, Semarang.
- Bambang Poernomo, 2012. *Azas-azas Hukum Pidana*. Ghalia Indonesia, Jakarta.
- Bambang Sunggono. 2011, *Metodologi Penelitian Hukum*. PT Raja Grafindo Persada, Jakarta.
- Dami Khazawi, 2011, *Hukum Pidana di Indonesia*, PT. Gramedia Pustaka Utama, Jakarta
- Danrivanto Budhijanto, 2013, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi Regulasi dan Konvergensi*, Revika Aditama, Bandung.
- David. I. Bainbridge, 2014, *Komputer dan Hukum*, Sinar Grafika, Jakarta.
- Dedi Mulyadi, 2012, *Kebijakan Legislatif Tentang Sanksi Pidana Legislatif Di Indonesia Dalam Prespektif Demokrasi*, Gremata Publishing, Bekasi.
- Didik M. Arief Mansur dan Elisatris Gultom, 2010, *Urgensi Perlindungan Korban Kejahatan*, PT Raja Grafindo Persada, Jakarta.
- Dwidja Priyatno, 2005, *Kapita Selekta Hukum Pidana*, STBH Pres, Bandung.
- Rohrohmana, Basir. 2001. *Tindak Pidana, Unsur Tindak Pidana, Pidana dan Pemidanaan*, Fakultas Hukum Universitas Cenderawasih, Jayapura.
- Rosalinda Elsinia latumahina, 2011, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*. Fakultas Hukum Universitas Pelita Harapan Surabaya.
- Suhariyanto, Budi. 2013, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. PT Rajagrafindo Persada, Jakarta.
- Suparni, Niniek. 2012, *Cyberspace Problematika dan Antisipasi Pengaturannya*. Sinar Grafika, Jakarta.
- Widya Padjajaran, 2015. *Penelitian Tentang Perlindungan Hukum Data Digital, Badan Pembinaan Hukum Nasional*, Balai Pustaka, Jakarta

B. Peraturan Perundang-Undangan

- Undang-Undang Dasar 1945;
- Kitab Undang-Undang Hukum Dagang;
- Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban
- Undang-Undang Republik Indonesia Nomor 31 Tahun 2014 Perlindungan Saksi dan Korban
- Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Dan Elektronik
- Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Transaksi Dan Elektronik.

C. Jurnal, Artikel Internet.

- Dwidja Priyatno dan M. Rendi Aridhayandi, 2016, *Resensi Buku(Book Review) Satjipto Rahardjo, 2014, Ilmu Hukum*, PT. Citra Aditya, Bandung, Jurnal Mimbar Justitia Vol. 2 No 2, Fakultas Hukum Universitas Suryakencana, Cianjur.
- Henny Nuraeny, 2017, *Penyuluhan Hukum Mengenai Undang-Undang Nomor 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang Bagi Guru*



Bimbingan Konseling dan Siswa/Siswi SMK/SMA/MA Se-Kabupaten Cianjur, Journal Of Empowerment Vol. 1 No. 1, Universitas Suryakencana.

Hesti Dwi Astuti, 2015, *Kendala Penyelesaian Sengketa Konsumen melalui Badan Penyelesaian Sengketa Konsumen (BPSK) Jurnal Hukum Mimbar Justitia Volume 15 No 3. Desember*

Trini Handayani, 2016, *Perlindungan dan Penegakan Hukum Terhadap Kasus Kekerasan Seksual pada Anak, Jurnal Mimbar Justitia, Vol. 2 No. 2, Fakultas Hukum Universitas Suryakencana, Cianjur.*