ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 1299-1305
Volume 8 Nomor 1 Tahun 2024

Cara Operasi Kejahatan *Phising* di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia

Aura Nasha Ramadhanti[1], Tessa Ayuning Tias[2], Erin Dwi Lestari[3], Asmak Ul Hosnah[4]

[1,2,3,4] Program Studi Ilmu Hukum, Universitas Pakuan Bogor, Indonesia

e-mail: auranasha47@gmail.com[1] , tesyaayuningtias73@gmail.com[2] , 21erindwil@gmail.com[3] , asmak.hosnah@unpak.ac.id[4]

Abstrak

Penelitian ini membahas fenomena kejahatan siber yang cukup mengkhawatirkan, yaitu tindakan *phising*. Tujuan utama penelitian ini adalah untuk memahami cara operasi kejahatan *phising* di ranah siber, khususnya dalam konteks hukum positif Indonesia. Kejahatan *phising* adalah metode penipuan yang mengelabui individu atau entitas dengan menyamar sebagai entitas terpercaya untuk memperoleh informasi pribadi. Penelitian ini mengidentifikasi dan menganalisis modus operandi yang digunakan oleh pelaku kejahatan *phising*, serta menghubungkannya dengan kerangka hukum yang ada di Indonesia. Hasil penelitian menunjukkan bahwa pelaku kejahatan *phising* secara cermat memanfaatkan berbagai metode manipulatif untuk mencapai tujuan mereka, dan kerap mengabaikan undang-undang yang mengatur keamanan siber dan privasi data. Penelitian ini juga mengulas regulasi hukum positif Indonesia yang relevan dalam menangani kejahatan siber, termasuk *phising*, dan mengevaluasi efektivitas kerangka hukum tersebut dalam memberikan perlindungan terhadap individu dan organisasi. Penelitian ini memiliki fokus pada penerapan metode hukum normatif dan penelitian deskriptif analitis. Penggunaan sumber data memakai beberapa data sekunder. Metode untuk mengumpulkan datanya yakni dengan memakai metode yang berupa penelitian kepustakaan. Hasil penelitian menunjukkan bahwa pelaku kejahatan *phising* secara cermat memanfaatkan berbagai metode manipulatif untuk mencapai tujuan mereka, dan kerap mengabaikan undang-undang yang mengatur keamanan siber dan privasi data. Penelitian ini juga mengulas regulasi hukum positif Indonesia yang relevan dalam menangani kejahatan siber, termasuk *phising*, dan mengevaluasi efektivitas kerangka hukum tersebut dalam memberikan perlindungan terhadap individu dan organisasi.

Kata Kunci: *Tindak Pidana Phising, Siber, Cara Operasi Kejahatan.*

Abstract

This research discusses the phenomenon of cyber crime which is quite worrying, namely phishing. The main aim of this research is to understand how phishing crimes operate in the cyber domain, especially in the context of Indonesian positive law. Phishing crimes are fraudulent methods that trick individuals or entities by posing as trusted entities to obtain personal information. This research identifies and analyzes the modus operandi used by phishing crime perpetrators, and relates it to the existing legal framework in Indonesia. The research results show that phishing criminals carefully utilize various manipulative methods to achieve their goals, and often ignore laws governing cyber security and data privacy. This research also reviews Indonesia's positive legal regulations that are relevant in dealing with cybercrime, including phishing, and evaluates the effectiveness of the legal framework in providing protection for individuals and organizations. This research focuses on the application of normative legal methods and analytical descriptive research. The use of data sources uses several secondary data. The method for collecting data is by using a method in

the form of library research. The research results show that phishing criminals carefully utilize various manipulative methods to achieve their goals, and often ignore laws governing cyber security and data privacy. This research also reviews Indonesia's positive legal regulations that are relevant in dealing with cybercrime, including phishing, and evaluates the effectiveness of the legal framework in providing protection for individuals and organizations.

Keywords: *Phishing Crime, Cyber, How Crimes Operate.*

PENDAHULUAN

Indonesia mengalami pertumbuhan yang tercermin dari banyak program pembangunan di berbagai sektor. Namun, teknologi informasi dan komunikasi juga membawa risiko tindak kejahatan baru yang dikenal sebagai *cybercrime*. Teknologi informasi dan komunikasi seperti pedang bermata dua, memberikan manfaat positif dalam meningkatkan kesejahteraan dan kemajuan manusia, tetapi juga memiliki potensi sebagai alat untuk melanggar hukum. Kemajuan dalam teknologi komputer dan telekomunikasi terutama melalui internet telah memungkinkan penyebaran informasi yang luas dalam kehidupan sehari-hari. Namun, dampak negatifnya adalah peningkatan penyalahgunaan internet seperti praktik *phising* yang digunakan untuk mencuri data pribadi seperti username dan password. *Cybercrime* atau kejahatan siber adalah bentuk kejahatan baru yang menjadi perhatian dunia internasional. *Cybercrime* dianggap sebagai perilaku anti-sosial yang semakin berkembang di era digital.

Kejahatan siber adalah tindakan kriminal yang memanfaatkan teknologi komputer, jaringan, atau internet. Ini melibatkan penggunaan teknologi untuk melakukan aktivitas ilegal, mengejar target tertentu, atau mengeksploitasi kelemahan dalam sistem digital. Kejahatan siber mencakup berbagai metode yang digunakan oleh pelaku untuk menargetkan individu. Ini termasuk tindakan klasik seperti penipuan, pencurian identitas, atau penyebaran konten ilegal, namun semuanya dilakukan secara digital dan dapat mencakup banyak korban. Kejahatan siber juga mencakup penggunaan kode berbahaya dan eksploitasi yang dapat merusak operasi komputer secara global, serta mengancam bisnis *online* dan *e-commerce*.

Salah satu jenis kejahatan yang dilakukan oleh *cracker* adalah *phishing*, yang bertujuan untuk keuntungan pribadi dan merugikan pihak lain jika mereka menjadi korban. Dalam konteks keamanan komputer, *phising* adalah salah satu bentuk penipuan elektronik yang prosesnya bertujuan untuk mencuri informasi yang sangat sensitif, seperti *username, password,* dan rincian kartu kredit, dengan menyamar sebagai entitas yang dapat dipercayai atau organisasi sah.

Pengetahuan yang terbatas pada pengguna terhadap perangkat teknologi yang mereka gunakan adalah faktor pemicu terjadinya *phising*. Oleh karena itu, pengguna teknologi perlu diberikan pengetahuan tentang cara mengoperasikan teknologi. Terdapat sebuah teori yang mengemukakan bahwa kejahatan adalah hasil dari masyarakat itu sendiri, yang berarti bahwa masyarakatlah yang menciptakan kejahatan.

Saat ini, sangat penting untuk memiliki peraturan hukum yang mengatur tindak kejahatan di dunia maya, terutama dalam konteks penelitian ini yang membahas kejahatan *cyber* dalam bentuk *phising*. Dalam konteks latar belakang ini, telah dibahas mengenai fenomena kejahatan *phising* di ranah siber, yang semakin meresahkan dan mengancam keamanan digital. Selain itu, telah disoroti pentingnya peraturan hukum yang mengatur tindakan *cybercrime*, khususnya terkait dengan *phising*, dalam kerangka hukum positif Indonesia. Dalam rangka memahami lebih dalam permasalahan tersebut dan mencari solusi yang tepat, penelitian ini akan merumuskan masalah mengenai cara operasi kejahatan *phising* di ranah siber, dan terkait dengan pengaturan terhadap *cybercrime* dalam bentuk tindak pidana *phising* diatur dalam hukum positif Indonesia.

Dengan merujuk pada informasi yang disampaikan dalam pengantar mengenai tindak pidana *phising*, penulis tertarik untuk melakukan studi yang berkaitan dengan pengaturan hukum dalam menghadapi *cybercrime* dalam bentuk tindak pidana *phising*. Penelitian ini

berjudul: “Cara Operasi Kejahatan *Phising* di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia”.

METODE

Penelitian ini merupakan usaha ilmiah yang didasarkan pada pendekatan metodologis, struktur, dan konsep khusus, dengan tujuan untuk menyelidiki satu atau beberapa aspek dalam bidang hukum. Penelitian ini mengadopsi pendekatan kualitatif dengan metode hukum normatif, di mana penelitian hukum dilakukan dengan menganalisis literatur atau data sekunder sebagai sumber informasi utama. Sifat penelitian ini adalah deksriptif analitis, yakni proses pembahasan dilakukan dengan cara memaparkan dan menjelaskan data secara komprehensif, terperinci, dan terstruktur. Metode pendekatan pada penulisan hukum ini menggunakan pendekatan undang-undang. Sementara itu, untuk mendapatkan data yang mendukung penulisan hukum ini, penulis menggunakan proses pengumpulan data dilakukan melalui penelitian kepustakaan dengan menghimpun informasi dari literatur dan materi lain yang relevan dengan topik penulisan hukum ini. penulis susun. Hasil analisis yang telah diperoleh kemudian digunakan dalam metode penarikan kesimpulan yang berupa pendekatan dengan melalui hukum dalam peraturan perundang-undangan yamg diidentifikasi terlebih dahulu, kemudian dilihat bagaimana hukum tersebut diterapkan dalam kejahatan *phising* di ranah siber dalam konteks hukum positif Indonesia.

HASIL DAN PEMBAHASAN

1. Cara Operasi Kejahatan *Phising* di Ranah Siber

Kejahatan siber di Indonesia dipengaruhi oleh beberapa faktor utama. Pertama, akses internet yang luas dan mudah diakses membuka peluang bagi penjahat siber untuk beroperasi secara anonim. Kedua, kelalaian pengguna komputer juga berperan penting, termasuk penggunaan kata sandi yang lemah dan tindakan sembrono terhadap tautan atau lampiran mencurigakan. Selain itu, kekurangan dalam tingkat keamanan dan pemahaman tentang risiko serangan turut mempermudah pelaku kejahatan siber. Akhirnya, kurangnya kesadaran tentang kejahatan siber dan cara melindungi diri dari ancaman juga menjadi tantangan. Untuk mengatasi masalah ini, diperlukan upaya edukasi, perbaikan keamanan teknologi, dan peningkatan kesadaran tentang risiko kejahatan siber di Indonesia.

Orang-orang yang terlibat dalam kejahatan siber adalah individu yang memiliki pengetahuan mendalam tentang sistem komputer dan keahlian dalam mengeksplorasi celah-celah keamanan di dalamnya. Latar belakang yang sangat bervariasi dan tidak dapat dikelompokkan dalam kategori tertentu. Para peretas siber tidak dibatasi oleh usia atau status sosial mereka dalam masyarakat. Ketidakberpihakan dalam profil para pelaku kejahatan siber menunjukkan betapa inklusifnya dunia kejahatan siber dan bahwa siapa pun dengan pengetahuan dan kemauan yang cukup dapat terlibat dalam aktivitas ini. Terdapat beberapa karakteristik khusus yang sering menjadi ciri khas para peretas, di antaranya:

a. Pemuja kesenangan, yang mana tercermin dalam kegembiraan mereka ketika berhasil menembus pertahanan atau sistem komputer yang dirancang dengan sangat baik. Mereka melihat pencapaian ini sebagai cara untuk menguji kemampuan dan merangsang kecerdasan mereka.
b. Orang-orang yang memiliki kreativitas tinggi, sebagian besar peretas tidak memiliki sumber daya yang cukup kuat, sehingga mereka harus mengeluarkan upaya ekstra untuk menyelesaikan masalah dalam sistem yang ada.
c. Mereka tidak mudah merasa jenuh, yang tercermin dari kebiasaan mereka menghabiskan waktu selama 48 jam untuk memantau lalu lintas data atau aktivitas dalam jaringan komputer.
d. Mereka menginginkan kebebasan tanpa batas, dan para peretas sering menganggap larangan sebagai sesuatu yang harus mereka atasi. Oleh karena itu, birokrasi dan pemerintah yang sering merahasiakan informasi dianggap sebagai musuh utama oleh para peretas. Mereka dengan tekad menyatakan bahwa mereka akan terus berupaya untuk mendapatkan akses ke sistem yang mereka inginkan tanpa ada pembatasan.

Peretas selalu mencari titik lemah atau celah dalam sistem komputer untuk masuk. Namun, perlu diperhatikan bahwa tidak semua peretas memiliki motivasi yang serupa. Misalnya, dalam situasi *phising*, meskipun tindakan tersebut bisa merugikan pengguna internet, tidak semua pelaku phising memiliki niat jahat yang identik. Sebagai contoh, ada pelaku *phising* dengan motivasi berbeda. Beberapa dari mereka mungkin mencoba mencuri data pribadi, seperti informasi keuangan atau kata sandi, dengan niat merugikan pengguna internet. Namun, ada individu yang menggunakan teknik *phising* untuk tujuan keamanan atau peretasan etis. Mereka mencoba mengidentifikasi celah keamanan dalam sistem untuk membantu perbaikan keamanan, bukan untuk merugikan orang lain.

Phising dapat dikategorikan menjadi berbagai jenis berdasarkan motif pelaku dan target yang ingin mereka tuju:

1. *Spear Phishing* adalah taktik *phising* yang difokuskan, di mana pelaku memiliki sasaran yang khusus. Penggunaan istilah "spear," yang merujuk pada tombak, menunjukkan bahwa dalam jenis serangan ini, pelaku memiliki kesempatan yang lebih tinggi untuk berhasil karena sasaran yang teridentifikasi dengan jelas dan spesifik.
2. *Whaling*, yang mirip dengan *spear phising*, menargetkan individu yang memiliki posisi tinggi dalam suatu organisasi, seperti pejabat atau eksekutif perusahaan. Pelaku dalam jenis ini sering menggunakan dokumen panggilan tertulis, yang disebut subpoena, untuk menakuti korban dengan mengancam tindakan hukum.
3. *Clone Phishing* adalah bentuk *phising* yang mirip dengan *phising* konvensional. Pelaku memanfaatkan surel yang sah dan mengirim pesan yang sama dengan email yang asli, namun mereka mengubah konten lampiran pesan asli dengan informasi palsu.
4. *Covert Redirect* adalah teknik *phishing* yang sangat canggih di mana pelaku memodifikasi tautan yang terlihat resmi, tetapi sebenarnya mengarahkan korban ke tautan yang dibuat oleh pelaku melalui *pop-up login* yang telah dimodifikasi. Dalam metode ini, target sulit untuk membedakan apakah itu adalah formulir *login* yang sah atau palsu karena pelaku menggunakan tautan dan situs resmi dengan pop-up yang telah dimanipulasi.

Tindakan *phising* memerlukan sarana atau media tertentu, yang biasanya berupa komputer dan akses internet. Selain itu, beberapa pelaku *phising* mungkin memerlukan dana untuk mendaftarkan domain baru yang akan digunakan untuk mengecoh target mereka. Cara kerja *phising* dapat berbeda dalam berbagai bentuk sebagai berikut:

1. *E-mail Phising*, di mana pelaku awalnya mengirimkan email palsu yang menyamar sebagai organisasi yang dikenal oleh korban. Setelah itu, pelaku meminta korban untuk memperbarui data pribadinya melalui tautan URL yang ada dalam email tersebut.
2. *Website Phising*, di mana pelaku *phishing* menciptakan sebuah domain situs web yang menyerupai situs web asli dari suatu organisasi atau perusahaan. Tujuannya adalah untuk menipu korban agar memasukkan informasi pribadi, seperti kata sandi dan data rekening bank.
3. *Malware Phising*, di mana *malware* adalah program komputer yang diciptakan untuk menginfeksi sistem komputer tanpa sepengetahuan pengguna. Cara pelaku *phishing* dalam situasi ini adalah dengan mengirimkan file kepada korban, yang berpotensi mengandung *malware* yang mengandung virus dan akan menginfeksi sistem korban tanpa sepengetahuan mereka. Virus tersebut memungkinkan pelaku *phising* untuk dengan bebas mengakses sistem komputer korban.

Praktik *phising* sering terjadi melalui berbagai platform media sosial yang terhubung ke internet, seperti *email*, SMS, dan situs web. *Phising* melalui *email* atau SMS melibatkan pengiriman pesan dengan dua jenis modus yang umum:

1. Pesan meminta pertolongan. Pesan ini mencoba menipu penerima dengan mengaku sebagai seorang kerabat atau teman yang mengatakan bahwa mereka memerlukan bantuan mendesak dalam situasi masalah.
2. Pesan pemberitahuan kemenangan. Pesan ini berpura-pura memberitahu penerima bahwa mereka telah memenangkan sesuatu, seringkali dalam bentuk lotre, dan diharuskan untuk mengklaim hadiahnya. Namun, seringkali terdapat jebakan di dalamnya

yang meminta penerima untuk mengunggah data pribadi ke situs web tertentu yang mungkin telah dimanipulasi untuk tujuan penipuan.

2. Pengaturan Terhadap *Cybercrime* dalam Bentuk Tindak Pidana *Phising* pada Hukum Positif Indonesia

Dalam merumuskan delik pidana terkait dengan tindakan *phishing*, berdasarkan pembahasan sebelumnya, beberapa pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang dapat menjadi acuan untuk menegakkan hukum terkait dengan *phishing* adalah Pasal 378 KUHP yang berkaitan dengan penipuan, Pasal 263 KUHP yang terkait dengan pemalsuan surat, dan Pasal 362 KUHP yang berkaitan dengan penggelapan data elektronik atau informasi. Sebelumnya, pengaturan hukum terhadap kejahatan siber dalam bentuk *phising* diatur dalam Pasal 378 KUHP tentang penipuan, karena *phising* pada dasarnya merupakan tindakan penipuan.

Dalam tindak pidana *phising*, seringkali terdapat penggunaan nama palsu atau identitas palsu dengan tujuan menipu atau mengelabui korban. Pelaku *phising* cenderung menggunakan nama atau identitas palsu yang menyerupai organisasi atau perusahaan besar untuk menarik perhatian korban. Mereka juga merancang isi *email* atau situs web palsu dengan sangat hati-hati sehingga mirip dengan yang asli, hal ini dilakukan agar korban mudah percaya bahwa *email* atau situs web tersebut adalah milik pelaku *phising*. Selain itu, terdapat unsur dalam *phising* yang mendorong orang lain untuk menyerahkan data pribadi mereka. Meskipun dalam konteks *phising*, yang diminta bukanlah barang fisik, melainkan data pribadi, tetapi hal ini tetap memenuhi unsur yang ada dalam Pasal 378 KUHP. Data pribadi dianggap sebagai entitas non-fisik yang bisa dibuktikan keberadaannya.

Nico Keijzer berpendapat bahwa Pasal 378 adalah delik yang paling relevan bagi seseorang yang memanipulasi komputer untuk tujuan keuntungan, karena melibatkan aspek hak. Namun, Pasal 378 tidak mencakup unsur mengenai informasi elektronik dan/atau dokumen elektronik yang salah, sehingga sebenarnya Pasal 378 bukanlah pasal yang cocok untuk menangani *cybercrime* dalam bentuk *phising*.

Pasal 263 KUHP memiliki relevansi dengan tindakan *phising* yang merupakan tindakan penipuan dengan membuat *email* atau situs web palsu. Dalam konteks hukum, *email* dianggap sebagai surat elektronik. Pasal ini memiliki unsur-unsur yang sesuai dengan konsep *phising* yang telah dijelaskan sebelumnya. Pertama, unsur pembuatan atau pemalsuan surat yang dapat mengakibatkan hak, perjanjian, atau penghapusan hutang, atau sebagai bukti suatu peristiwa. Dalam tindakan *phising*, pelaku membuat surat elektronik yang mengaku berasal dari organisasi tertentu, membuatnya tampak asli, dan berisi tautan yang mengarahkan korban untuk memperbarui data pribadi mereka.

Unsur kedua adalah maksud untuk menggunakan atau memerintahkan orang lain untuk menggunakan surat tersebut seolah-olah surat itu benar dan tidak palsu. Ini adalah tujuan utama tindakan *phising*, di mana korban diarahkan untuk menggunakan isi *email* palsu dengan maksud untuk memperbarui data pribadi mereka. Data ini kemudian dapat disalahgunakan oleh pelaku *phising*, seperti berbelanja menggunakan kartu kredit atau uang di rekening korban. Semua tindakan ini juga memenuhi unsur terakhir dalam Pasal 263 KUHP, yang menyatakan bahwa pelaku dapat dihukum jika penggunaan surat palsu tersebut mengakibatkan kerugian bagi korban karena pemalsuan surat.

Pasal 362 KUHP yang berhubungan dengan. Ini disebabkan karena tindak pidana *phishing* pada dasarnya merupakan serangkaian tindakan yang bertujuan untuk mengambil sesuatu yang dimiliki oleh korban, dengan maksud untuk memiliki barang tersebut secara ilegal. Dalam konteks ini, pelaku phishing biasanya memiliki niat untuk mencuri data pribadi korban, dengan tujuan untuk memanfaatkan data pribadi tersebut demi keuntungan pribadi mereka. Dalam konteks hukum Indonesia, peraturan mengenai hukum siber masih disusun dengan cakupan yang umum. Prinsip "*Lex Specialis derogat legi Generalis*" tetap berlaku, yang berarti undang-undang atau aturan hukum yang lebih khusus akan mengatasi undang-undang atau aturan hukum yang lebih umum. Di Indonesia, regulasi hukum khusus yang mengatasi isu hukum siber adalah Undang-Undang Informasi dan Transaksi Elektronik (UU

ITE). UU ITE mengatur tindakan yang tidak diperbolehkan dalam penggunaan teknologi informasi, meskipun tidak secara khusus merinci masalah phishing. Namun, penegak hukum di Indonesia menggunakan pasal-pasal dalam UU ITE sebagai pedoman dalam menangani kejahatan phishing di Indonesia.

Undang-Undang ITE telah disahkan dan diberlakukan, awalnya dibentuk sebagai Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang masih berlaku hingga sekarang. UU ITE mengatur dengan lebih rinci mengenai perbuatan yang dilarang dalam penggunaan teknologi informasi. Beberapa pasal dalam UU ITE yang mungkin dapat diterapkan pada pelaku tindak pidana *phishing*, antara lain Pasal 28 ayat (1) jo. Pasal 45A ayat (1), Pasal 30 ayat (2) jo. Pasal 46 ayat (2), dan Pasal 35 jo. Pasal 51 ayat (1) UU ITE.

Tindakan yang dilakukan oleh pelaku *phising* tidak hanya sebatas memanipulasi situs web atau surel untuk menyesatkan korban, tetapi juga melibatkan penggunaan kebohongan dengan maksud menipu korban, yang pada akhirnya menyebabkan kerugian bagi korban. Pasal 28 ayat (1) UU ITE melarang tindakan yang dapat menyebabkan kerugian bagi konsumen dalam transaksi elektronik dengan menyesatkan orang lain. Informasi pribadi korban yang diperoleh oleh pelaku kemudian dapat disalahgunakan, yang pada akhirnya merugikan korban dalam transaksi elektronik. Perlu diperhatikan bahwa perbedaan pokok terletak pada unsur transaksi yang terjadi. Dalam *phising*, fokus hanya pada tindakan menyesatkan dalam konteks transaksi elektronik, sehingga Pasal 28 Ayat (1) UU ITE tidak berlaku untuk transaksi konvensional.

Pasal 30 ayat (2) UU ITE berlaku untuk individu yang mengakses sistem elektronik atau komputer dengan maksud memperoleh informasi elektronik atau dokumen elektronik, yang merupakan inti dari praktik *phising*. Pasal ini juga menjelaskan bahwa tindakan yang dilarang dapat dilakukan dengan cara mengirimkan hal-hal tersebut kepada pihak yang tidak memiliki hak atasnya. Dalam praktik *phising*, pelaku mengirimkan dokumen kepada korban dengan tujuan memperoleh informasi atau dokumen elektronik milik korban.

Pasal 46 ayat (2) mengatur hukuman pidana jika seseorang melanggar Pasal 30 ayat (2). Dibandingkan dengan Tindak Pidana Pencurian yang diatur dalam KUHP, ada perbedaan mendasar dalam hal apa yang diambil oleh pelaku tanpa izin. Dalam tindakan *phishing*, yang diambil oleh pelaku adalah data berupa informasi elektronik. Dengan kata lain, tindakan phishing memiliki karakteristik yang lebih spesifik daripada pencurian biasa.

Dalam situasi yang berkaitan dengan *phising*, Pasal 35 UU ITE sering menjadi dasar yang paling umum digunakan oleh penegak hukum untuk menentukan sanksi yang diberlakukan kepada pelaku *phising*. Pelanggaran terhadap ketentuan dalam pasal tersebut akan mengakibatkan penerapan sanksi pidana berdasarkan Pasal 51 ayat (1) UU ITE. Dalam praktik *phising*, pelaku melakukan manipulasi dengan menciptakan situs web palsu atau surel palsu dengan maksud memperdaya korban. Tujuannya adalah membuat korban percaya bahwa situs web atau surel tersebut adalah informasi yang sah. Tindak pidana *phising* memiliki karakteristik yang lebih spesifik dan relevan dengan lingkungan digital, di mana pelaku menggunakan teknik manipulasi elektronik untuk mencuri informasi atau data pribadi. Ini berbeda dengan tindak pidana konvensional yang lebih terkait dengan tindakan fisik atau pencurian barang secara fisik. Oleh karena itu, karena perbedaan lokasi dan konteks tindakan ini, *phising* diatur oleh hukum yang berbeda, yaitu Undang-Undang ITE, yang secara khusus mengatasi tindakan kriminal dalam ranah siber dan teknologi informasi.

SIMPULAN

Kesimpulan dari rumusan masalah ini adalah bahwa tindak kejahatan *phising* dalam ranah siber adalah suatu praktik yang memanfaatkan teknologi untuk melakukan penipuan dan mencuri informasi pribadi korban. Tindakan *phising* ini beroperasi melalui berbagai cara, seperti *email* palsu, situs web palsu, dan penggunaan teknik manipulasi elektronik untuk menyesatkan korban. Di Indonesia, pengaturan terhadap kejahatan siber dalam bentuk

tindak pidana *phising* belum diatur secara khusus, sehingga Pasal-pasal yang relevan dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) digunakan sebagai acuan untuk menangani tindak pidana *phising*. Beberapa pasal dalam UU ITE yang mungkin dapat diterapkan pada pelaku tindak pidana *phishing*, antara lain Pasal 28 ayat (1) jo. Pasal 45A ayat (1), Pasal 30 ayat (2) jo. Pasal 46 ayat (2), dan Pasal 35 jo. Pasal 51 ayat (1) UU ITE.

SARAN

Dalam rangka mengatasi kejahatan *phising* di ranah siber dan meningkatkan regulasi terhadap *cybercrime* dalam bentuk tindak pidana *phising* di Indonesia, beberapa langkah dapat diambil. Pertama, perlu peningkatan kesadaran masyarakat terkait risiko *phising* dan upaya perlindungan data pribadi mereka melalui pendidikan dan kampanye publik. Kedua, pembuatan peraturan hukum yang lebih spesifik dan rinci mengenai tindak pidana *phising* dapat membantu penegak hukum dalam menindak pelaku *phising*. Ketiga, penegak hukum perlu mendapatkan pelatihan khusus dalam mengidentifikasi dan menyelidiki tindakan *phising*. Keempat, kerja sama internasional sangat penting karena kejahatan siber seringkali melibatkan pelaku dari berbagai negara. Kelima, perusahaan dan organisasi perlu meningkatkan keamanan siber mereka untuk melindungi data sensitif dan mencegah serangan *phising*. Terakhir, masyarakat perlu didorong untuk melaporkan upaya *phising* dan insiden kejahatan siber kepada pihak berwenang agar tindakan tanggap dan efektif dapat diambil. Dengan langkah-langkah ini, diharapkan dapat mengurangi dampak kejahatan *phising* dan meningkatkan perlindungan masyarakat dalam ranah siber.

DAFTAR PUSTAKA

Dimyati, Khudzaifah dan Kelik Wardiono, *Metode Penelitian Hukum*. Surakarta: Universitas Muhammadiyah Surakarta, 2004.

Hamzah, Andi. *Delik-Delik Tertentu (Speciale Delicten) Didalam KUHP Edisi Kedua*. Jakarta: Sinar Grafika, 2015.

Mansur, Dikdik M. Arief dan Elisatris Gultom. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: PT. Refika Aditama, 2010.

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

Mustafa, Hasan. *Teknik Sampling*. Bandung: Alfabeta, 2003.

Nawawi, Barda. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: PT. RajaGrafindo Persada, 2005.

Nudirman Munir. *Pengantar Hukum Siber Indonesia*. Depok: PT Raja Grafindo Persada, 2017.

Soekanto, Soerjono dan Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada, 2010.

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

Bamai Uma, "Apa itu *Phising*? Pengertian, Ciri, Jenis & Cara Menghindari", tersedia di: https://bamai.uma.ac.id/2022/08/18/apa-itu-phising-pengertiancirijeniscaramenghindari/#:~:text=Pelaku%20mengincar%20target%20korban%20%28biasanya%20sudah%20ditargetkan%20berapa,data%20diri%2C%20pin%20rekening%2C%20atau%20informasi%20rahasia%20lainnya%29, diakses tanggal 7 November 2023.

Broadhurst, Roderic. "*Developments in the Global Law Enforcement of Cyber-crime," Policing: An International Journal of Police Strategies & Management*. Vol. 29 No. 3 Tahun 2006.

Gulo, Ardi Saputra. "*Cybercrime* dalam bentuk *Phising* Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik". *Journal of Criminal,* diterbitkan oleh 1 PAMPAS.

Wibowo, Mia Haryawati. "Ancaman *Phising* Terhadap Pengguna Sosial Media dalam Dunia *Cybercrime*". *Jurnal Of Education And Information Communication Technology*, diterbitkan oleh JOEICT, Tahun 2017.