

**BAB III**

**PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU PRAKTIK  
PHISING DALAM *GAME ONLINE***

**3.1 Unsur-Unsur Tindak Pidana Dalam Praktik Phising Di *Game Online***

Regulasi *cyberlaw* pada tindak pidana praktik phising dalam *game online* menimbulkan tantangan unik karena praktik di Indonesia menganggap hukum dan regulasi *cyberlaw* itu sendiri hanya “seumur jagung” yang artinya aturan mengenai kejahatan ini di Indonesia masih tergolong baru. Kedudukan hukum siber membawa dampak dalam masyarakat, kemajuan teknologi komputer telah mempermudah kehidupan masyarakat sehari-hari terutama dalam bidang pekerjaan. Pemanfaatan teknologi komputer sebagai sarana untuk melakukan kejahatan dalam perkembangannya menimbulkan permasalahan yang sangat kompleks khususnya dalam pembuktian pidananya, hal ini karena kejahatan pada komputer memiliki karakteristik unik yang membedakannya dari kejahatan pada umumnya.

Dalam merumuskan tindak pidana phising dalam *game online*, di Indonesia sebenarnya masih belum memiliki undang-undang yang mengatur secara khusus mengenai praktik phising dalam *game online*, tetapi terdapat dasar hukum yang menjadi acuan untuk menetapkan tindak pidana ini yang sebelumnya diatur dalam Kitab Undang-Undang Hukum Pidana yang terdapat dalam Pasal 378 dan Pasal 263 serta Undang-Undang Nomor 11 Tahun 2008 Tentang Perubahan Atas Undang-

Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik yang terdapat dalam Pasal 28 Ayat (1) jo. Pasal 45A Ayat (1) dan Pasal 35 jo. Pasal 51 Pasal 378 KUHP :

”Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan menggerakkan orang lain menyerahkan suatu barang benda kepadanya atau supaya memberi hutang maupun menghapuskan piutang dikenakan karena penipuan dengan pidana penjara paling lama 4 (empat) tahun.”

Unsur-unsur yang memenuhi dalam Tindak Pidana Praktik Phising *dalam Game Online* menurut Pasal 378 KUHP, diantaranya :

1. Unsur Subyektif :

a. Barangsiapa

Unsur ini mengacu pada subjek hukum itu sendiri yang merujuk terhadap pelaku tindak pidana itu sendiri, dimana subjek hukum ini dapat berupa orang ataupun badan hukum yang dinilai dapat mempertanggungjawabkan perbuatannya menurut hukum yaitu pelaku phising dalam *game online*.

b. Dengan Maksud Untuk Menguntungkan Diri Sendiri atau Orang Lain

Jika membahas tentang tindak pidana phising dalam *game online*, dapat disimpulkan bahwa sebagian pelaku phising ini menggunakan keahlian mereka demi mengambil keuntungan dari

orang lain, walaupun tidak berupa uang ataupun barang melainkan data diri para korbannya.

c. Secara Melawan Hukum

Perbuatan tersebut dilakukan secara melawan hukum, yang artinya dalam perbuatannya pelaku phising dalam *game online* dapat dikenakan pidana dan tidak memiliki hak sama sekali untuk menerima keuntungan apapun, yaitu hasil penipuan.

2. Unsur Obyektif :

a. Dengan Memakai Nama Palsu atau Martabat Palsu, Dengan Tipu Muslihat, Atau pun Dengan Rangkaian Kebohongan

Dalam unsur ini dengan menggunakan nama palsu atau martabat palsu, pada praktik phising di *game online* hal ini dikenal dengan sebutan *Man in the middle* yaitu pelaku akan menemepatkan dirinya diantara korban dan website resmi dengan cara membuat website yang seolah-olah web tersebut berasal dari *developer game* resmi yang didalamnya ditujukan untuk mengklaim suatu hadiah di *game* tersebut, padahal web tersebut merupakan buatan mereka sendiri yang dimodifikasi hingga menyerupai aslinya tanpa perlu membuat fungsi atau fasilitas yang sama, karena tujuannya agar korban memasukkan *username* serta *password* di dalamnya,<sup>48</sup> kemudian korban akan dibawa menuju situs yang asli agar tidak

---

<sup>48</sup> Jordy Prayoga, <https://gudangssl.id/blog/man-in-the-middle-attack-adalah/> Diakses pada 9 Desember 2022.

timbul kecurigaan. Korban yang merasa bahwa website yang dikunjungi pantas untuk dipercaya, padahal hal tersebut tidak memiliki hubungan sama sekali.

b. Menggerakkan Orang Lain Untuk Menyerahkan Barang Atau Sesuatu Kepadanya

Dalam konteks ini sebenarnya sebuah barang bukan merupakan target pelaku phising, melainkan data pribadi milik korban, tetapi hal tersebut tetap dianggap memenuhi unsur dalam Pasal 378 KUHP karena pada dasarnya data pribadi juga termasuk suatu benda yang tidak berwujud tetapi dapat dibuktikan keberadaannya.

Pasal 263 Ayat (1) KUHP :

“Barangsiapa membuat secara tidak benar atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan atau pembebasan hutang, atau yang dipergunakan sebagai bukti dari suatu hal, dengan maksud untuk menggunakan atau menyuruh orang lain memakai surat tersebut seolah-olah isinya asli dan tidak dipalsukan, jika pemakaian tersebut menimbulkan kerugian karena memakai surat, dapat dikenakan pidana penjara paling lama 6 (enam) tahun.”

Sebagaimana yang telah dijelaskan di atas dalam kaitannya pada perbuatan phising itu sendiri, Pasal 263 ayat (1) KUHP mengatur mengenai pemalsuan surat dan penipuan diartikan sebagai perbuatan yang dimana pelaku phising membuat

sebuah email palsu atau website palsu mengatasnamakan institusi resmi yang seolah-olah email palsu atau website palsu tersebut adalah asli dan dikarenakan dalam Pasal 263 ayat (1) KUHP belum memiliki pengaturan khusus mengenai praktik phishing dalam *game online*, maka terdapat perluasan makna dikarenakan *e-mail* disini juga dianggap surat tetapi dalam bentuk elektronik. Adapun unsur-unsur yang terdapat dalam Pasal 263 ayat (1) KUHP yang sesuai dengan definisi phishing dalam *game online* tersebut, sehingga dapat dikenakan pada pelaku tindak pidana phishing. Berikut merupakan penjelasan mengenai unsur-unsur dalam Pasal 263 ayat (1) KUHP, diantaranya :

1. Unsur Subyektif :

a. Barangsiapa

Unsur ini mengacu pada subjek hukum itu sendiri yang merujuk terhadap pelaku tindak pidana itu sendiri, dimana subjek hukum ini dapat berupa orang ataupun badan hukum yang dinilai dapat mempertanggungjawabkan perbuatannya menurut hukum yaitu pelaku phishing dalam *game online*.

b. Dengan Maksud Untuk Memakai atau Menyuruh Orang Lain Agar Memakai Surat Yang Seolah-Olah Isinya Asli dan Tidak Palsu

Dari unsur ini dapat dilihat bahwa tujuan pelaku phishing dalam *game online* yaitu mengajak atau menyuruh korbannya menggunakan isi surat elektronik atau *e-mail* yang telah disebarakan oleh pelaku tersebut. Pembuatan *e-mail* palsu tersebut telah diketahui oleh pelaku dan menganggap seolah-olah isinya benar dan

tidak palsu, tetapi tetap saja hal itu digunakan pelaku dalam menjebak korbannya. Korban yang menganggap email tersebut sebagai surat resmi dan tanpa disadari telah mengikuti langkah-langkah yang telah ditetapkan oleh pelaku pembuat *e-mail* tersebut, hal itu yang nantinya dimanfaatkan oleh pelaku phishing dalam *game online* secara tidak bertanggung jawab.<sup>49</sup>

## 2. Unsur Obyektif :

### a. Membuat Surat Palsu atau Pemalsuan Surat

Pada unsur ini surat yang dimaksud dalam Pasal 263 ayat (1) KUHP yaitu segala surat yang ditulis tangan ataupun diketik menggunakan mesin, tetapi dalam tindak pidana phishing dalam *game online* surat yang dimaksud yaitu surat elektronik atau *e-mail* yang tidak dijelaskan pada rumusan Pasal 263 ayat (1) KUHP. Phishing merupakan bentuk tindak pidana yang berdasarkan penipuan, maka dalam melancarkan aksinya, pelaku phishing dalam *game online* ini membuat surat surat elektronik atau *e-mail* palsu yang mengatasnamakan suatu institusi resmi agar dianggap sebagai suatu email yang asli. Isi dari *e-mail* yang dibuat oleh pelaku phishing ini menyerupai website yang resmi, mulai dari bentuk desain sampai terdapat suatu logo sosial media yang telah disambungkan ke dalam akun sosial media milik *game* tersebut.

---

<sup>49</sup> Eko Adi Susanto, 2018, "*Pertanggungjawaban Pidana Yang Memakai Surat Palsu Ditinjau Dari Pasal 263 Ayat (2) KUHP*", Vol. 1, No. 1, h. 8.

Pasal dalam Undang-Undang No.1 Tahun 2023 tidak merubah serta memindahkan terkait Pasal yang mengatur mengenai praktik phising dalam *game online* pada Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008. Berikut Pasal dalam UU ITE yang dipindahkan dalam KUHP Terbaru :

- a. Pasal 27 ayat (1) dan Pasal 45 ayat (1) UU ITE tentang distribusi konten yang melanggar kesusilaan sebelumnya dihapus dan diatur pada Pasal 407 KUHP tentang Pornografi
- b. Pasal 27 ayat (3) dan Pasal 45 ayat (3) UU ITE tentang distribusi konten yang berisi pencemaran nama baik sebelumnya dihapus dan diatur pada Pasal 433-438 KUHP tentang Pencemaran Nama Baik.
- c. Pasal 28 ayat (2) dan Pasal 45 ayat (2) UU ITE tentang distribusi konten berbau SARA dihapus dan diatur pada Pasal 243 KUHP tentang Penghinaan terhadap Golongan Penduduk.
- d. Pasal 30 dan Pasal 46 UU ITE tentang peretasan komputer atau sistem elektronik milik orang lain dihapus dan diatur pada Pasal 332 KUHP tentang Penggunaan dan Perusakan Informasi Elektronik.
- e. Pasal 31 ayat (1) dan ayat (2) serta Pasal 47 UU ITE tentang Penyadapan atas komputer atau sistem elektronik milik orang lain dihapus dan diatur pada Pasal 258 KUHP tentang Penyadapan.

Seperti yang diketahui, *cyber crime* mengacu pada penggunaan sistem informasi dan transaksi elektronik yang bertujuan untuk merugikan orang lain atau

instansi terkait dan pengguna fasilitasnya dalam mendapatkan keuntungan pribadi maupun orang lain. Disisi lain, teknologi informasi khususnya Internet telah digunakan sebagai sarana untuk membangun masyarakat yang berbudaya informasi, maka dari itu upaya penanganan mengenai *cyber crime* harus ditanggapi secara serius oleh semua pihak. Keberadaan undang-undang mengenai *cyber crime* sangat diperlukan, meskipun dalam peraturan perundang-undangan masih belum mengatur secara khusus mengenai tindak pidana phishing. Maka perlu adanya kerjasama atau kemitraan antara pemerintah dan masyarakat dalam hal mengedukasi tentang dampak yang diberikan terhadap phishing tersebut.

Dalam KUHP aturan mengenai *cyber crime* masih dalam pembahasan secara umum, pada peraturan hukum di Indonesia dikenal asas *Lex Specialis derogat legi Generalis* dalam bahasa latin yang berarti bahwa peraturan hukum yang lebih khusus mengesampingkan peraturan hukum yang lebih umum, asas ini hanya berlaku terhadap dua peraturan perundang-undangan yang memiliki kedudukan sederajat serta mengatur pada substansi yang sama.<sup>50</sup> Dalam hal itu, Indonesia memiliki undang-undang yang mengatur tentang *cyber crime* secara khusus yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), perbuatan yang melanggar dalam penggunaan teknologi informasi ini telah diatur dalam undang-undang tersebut dan UU ITE telah dijadikan sebagai acuan untuk merumuskan tindak pidana phishing di Indonesia.

---

<sup>50</sup> Valerie A. Budianto, S.H, <https://www.hukumonline.com/klinik/a/3-asas-hukum--ilex-superior-i--ilex-specialis-i--dan-ilex-posterior-i-beserta-contohnya-cl6806>, Diakses pada 11 Desember 2022.



Pasal yang terdapat di KUHP dan UU ITE terdapat hal-hal yang berbeda dalam pengaturan dan sanksi pidananya. Dari sisi formulasi perumusan tindak pidananya tidak dirumuskan secara delik formil tetapi secara delik materiil yang dipandang dari segi esensinya unsur-unsur di KUHP terdapat unsur-unsur untuk menguntungkan diri sendiri dan orang lain, sedangkan di UU ITE tidak terdapat unsur menguntungkan diri sendiri dan orang lain. Di KUHP tidak menjelaskan mengenai kegiatan pada internet serta sarana dalam melakukan kejahatan di internet, sedangkan dalam UU ITE telah mengenal terkait informasi, transaksi dan media elektronik yang digunakan.<sup>51</sup> Di KUHP dan UU ITE terdapat perbedaan terkait dampak dan tujuan dari tindakan yang telah dijelaskan dalam undang-undang tersebut, misalnya Pasal dalam KUHP dimaksudkan untuk menguntungkan diri sendiri dan orang lain yang mengakibatkan korban mengalami kerugian barang atau benda dari tindak pidana yang dilakukan pelaku, sedangkan Pasal dalam UU ITE tidak menjelaskan mengenai unsur pelaku tindak pidana tersebut untuk mendapatkan keuntungan yang belum jelas untuk siapa, tetapi hanya menjelaskan mengenai akibat dari tindak pidana tersebut.

Peraturan mengenai cyber crime di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Pasal yang dapat dikenakan terhadap pelaku tindak pidana phishing itu sendiri, diantaranya Pasal 28 ayat (1) jo.

---

<sup>51</sup> Ida Ayu Ary Yulandari, Anak Agung Sagung Laksmi Dewi, I Made Minggu Widyantara, 2021, "*Tindakan Yuridis Pengaturan Tindak Pidana Terhadap Kejahatan Benda Virtual Dalam Game Online*", Jurnal Preferensi Hukum, Vol. 2, No. 3, h.. 505

Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) UU ITE.<sup>52</sup> Unsur-unsur yang terdapat dalam UU ITE merupakan hasil pengembangan dari jenis tindak pidana menurut KUHP, hanya saja dalam UU ITE tindak kejahatan tersebut dilakukan menggunakan media internet.

Rumusan Pasal 28 Ayat (1) UU ITE :

”Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik”

Unsur-unsur Pasal 28 ayat (1) UU ITE yang memenuhi pada tindak pidana praktik phising dalam *game online* dibagi menjadi dua yaitu unsur subyektif dan unsur obyektif, diantaranya :

1. Unsur Subyektif :

a. Dengan Sengaja dan Tanpa Hak

Pada unsur ini, dapat diketahui praktik tindak pidana phising merupakan suatu perbuatan yang melanggar norma atau aturan hukum yang berlaku. Dalam perbuatannya pelaku phising dalam *game online* dengan sengaja telah menyebarkan surat elektronik atau *e-mail* palsu yang seolah-olah dianggap sebagai *e-mail* asli dari institusi resmi untuk menjebak korbannya, tanpa di sadari pelaku phising tersebut telah melakukan suatu tindakan yang dapat dikenakan pidana penjara ataupun denda.

---

<sup>52</sup> Ardi Saputra Gulo, 2020, “*Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik*”, PAMPAS: Journal of Criminal, h. 75-76.

## 2. Unsur Obyektif :

### a. Perbuatan Menyebarkan Berita Bohong dan Mengakibatkan Kerugian Konsumen Dalam Transaksi Elektronik

Dalam unsur ini, perbuatan yang dilakukan oleh pelaku tindak pidana praktik phising dalam *game online* yaitu dengan cara menyebarkan website atau link palsu yang telah dimodifikasi hingga menyerupai aslinya, isi dari website yang dibuat oleh pelaku terdapat suatu instruksi atau ajakan untuk menggunakan website tersebut dengan imbalan hadiah yang terdapat di dalam *game* yang dimainkan. Korban yang tergiur dan menganggap website tersebut merupakan resmi dari pihak *developer game* itu sendiri, secara tidak sadar telah menggunakan dan mengikuti langkah-langkah yang terdapat dalam website palsu tersebut. Hal itu yang dimanfaatkan oleh pelaku phising dalam *game online* untuk mendapatkan keuntungan berupa informasi pribadi hingga hilangnya *account game* milik korban, sehingga telah mengakibatkan kerugian atas tindakan pelaku terhadap korban.

Selanjutnya Pasal 35 UU ITE merupakan Pasal yang paling sering digunakan oleh lembaga penegak hukum saat menentukan sanksi pidana terhadap pelaku tindak pidana phising tersebut, karena kandungan yang terdapat dalam Pasal 35 UU ITE sangat sesuai dengan permasalahan phising itu sendiri. Isi dari Pasal 35 UU ITE yang mengatur sebagai berikut :

### Pasal 35

“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.”

Rumusan Pasal diatas memiliki unsur-unsur yang mengatur mengenai mekanisme phishing dalam *game online* yaitu pelaku telah melakukan perbuatan menyebarkan suatu informasi elektronik berupa *e-mail* palsu yang dianggap seolah-olah data yang otentik. Menurut Kamus Besar Bahasa Indonesia (KBBI), kata “Otentik” memiliki makna yang sama dengan “Autentik” yang berarti asli, dapat dipercaya, tulen atau sah.<sup>53</sup>

Menurut penjelasan diatas, pengertian mengenai Informasi Elektronik telah diatur dalam Pasal 1 angka 1 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu :

“Informasi Elektronik adalah satu atau sekumpulan sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, angka, tanda, kode akses, simbol, atau perforasi yang telah diolah memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.”

---

<sup>53</sup> Deas Markustianto, 2019, “Tindak Pidana Pembuatan Akun Palsu Dalam Media Sosial Atas Nama Orang Lain”, *Recidive* Vol. 8, h. 49.

Adapun unsur-unsur dalam Pasal 35 UU ITE yang memenuhi Tindak Pidana Praktik Phising Dalam *Game Online* dibagi menjadi unsur subyektif dan obyektif, diantaranya :

1. Unsur Subyektif :

a. Setiap Orang Dengan Sengaja Dan Tanpa Hak

Yang dimaksud pada unsur ini mengenai “Setiap Orang”, yaitu pelaku phising dalam *game online* selaku subjek hukum dan kepadanya dapat dimintai pertanggungjawaban atas perbuatan yang dilakukan. Dapat diketahui, praktik tindak pidana phising merupakan suatu perbuatan yang melanggar norma atau aturan hukum yang berlaku.

2. Unsur Obyektif :

a. Dengan Sengaja Melakukan Penciptaan Informasi Elektronik Dengan Tujuan Agar Informasi Elektronik Tersebut Dianggap Data Yang Otentik

Berdasarkan fakta-fakta yang terdapat dalam tindak pidana phising dalam *game online* , rangkaian perbuatan yang dilakukan oleh pelaku tersebut dilakukan dengan sengaja. Dalam perbuatannya pelaku phising dalam *game online* dengan sengaja telah memanipulasi Informasi Elektronik berupa surat elektronik atau *e-mail* yang seolah-olah dianggap sebagai *e-mail* asli dari institusi resmi untuk menjebak korbannya. Apabila pelaku terbukti bertindak sebagai individu yang dianggap sah untuk menyebarkan surat

tersebut, maka dalam perbuatannya ini sesuai dengan unsur penciptaan dan manipulasi surat elektronik yang dipercaya sebagai data yang otentik dan tanpa di sadari perbuatan pelaku phising telah melakukan suatu tindakan yang dapat dikenakan pidana penjara ataupun denda.

Tindak pidana phising itu sendiri merupakan tindak penipuan yang menggunakan media elektronik dengan cara memanfaatkan suatu link palsu untuk diarahkan ke dalam situs web palsu yang dibuat oleh pelaku dengan tujuan mendapatkan data pribadi seseorang sehingga menyebabkan kerugian bagi orang tersebut. Oleh karena itu, phising tidak bisa disamakan dengan perbuatan-perbuatan yang ditentukan dan diatur dalam KUHP dikarenakan phising tersebut dilakukan dengan *locus delicti* yang tidak sama dengan tindak pidana konvensional, karena pada dasarnya tindak pidana phising itu sendiri lebih berkaitan dengan kejahatan siber dan informasi pribadi yang berupa dokumen elektronik.

### **3.2 Pertanggungjawaban Pidana Terhadap Pelaku Praktik Phising Dalam Game Online**

Peraturan hukum di Indonesia mengenal asas *Lex Specialis derogat legi Generalis* dalam bahasa latin yang berarti peraturan hukum yang lebih khusus mengesampingkan peraturan hukum yang lebih umum.<sup>54</sup> Karena phising termasuk dalam *cyber crime*, maka pertanggungjawaban pidana pada pelaku phising dalam

---

<sup>54</sup> Shinta Agustina, 2010, "Implementasi Asas Lex Specialis Derogat Legi Generali Dalam Sistem Peradilan Pidana", h. 504.

*game online* ini tidak menggunakan peraturan dalam KUHP melainkan Undang - Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi Dan Transaksi Elektronik karena Undang-Undang tersebut bersifat khusus. Untuk saat ini lembaga penegak hukum di Indonesia menggunakan Pasal 35 jo. Pasal 51 ayat (1) dan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dalam memutuskan dakwaannya terhadap pelaku phishing tersebut.

Pelaku phishing dalam *game online* ini tidak hanya membuat sebuah website yang seolah-olah asli seperti website dari institusi yang resmi, tetapi pelaku phishing tersebut juga melakukan tindakan penipuan untuk menyesatkan orang lain yang bertujuan dalam mendapatkan data pribadi seseorang sehingga menyebabkan kerugian bagi orang tersebut. Maka perbuatan tersebut 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. Rumusan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) sebagai berikut :

Pasal 28 ayat (1)

“Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik”

Pasal 45 ayat (1)

“Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah)”.

Selanjutnya rumusan Pasal 35 jo. Pasal 51 ayat (1), sebagai berikut :

Pasal 35

“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.”

Pasal 51

“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 Rp. 12.000.000.000,00 (dua belas miliar rupiah).”

Berdasarkan rumusan Pasal di atas, tindak pidana phishing dalam *game online* telah melakukan suatu tindakan melawan hukum yang melanggar ketentuan Pasal 35 karena telah membuat website palsu yang seolah-olah mirip dengan



website yang asli, selain itu juga melanggar ketentuan Pasal 28 ayat (1) dengan melakukan suatu kebohongan untuk mengarahkan korban ke dalam web palsu milik pelaku sehingga menyebabkan kerugian terhadap orang lain.

Pertanggungjawaban pidana terhadap praktik phishing dalam *game online* dapat dikenakan pasal berlapis yaitu Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) serta tidak boleh melebihi maksimum pidana yang terberat ditambah sepertiga, sistem ini dikenal sebagai kumulasi diperlunak.<sup>55</sup> Istilah mengenai hal tersebut yaitu perbarengan peraturan atau "*Concursus Realis*" yang terjadi ketika seseorang melakukan lebih dari satu tindakan, dan masing-masing tindakan tersebut berdiri sendiri sebagai suatu tindak pidana dan tindak pidana yang dilakukan tidak harus berkaitan satu sama lain. Maka yang dipakai adalah ketentuan pidana pokok yang terberat.<sup>56</sup>

Apabila "*Concursus Realis*" diterapkan pada tindak pidana phishing dalam *game online*, maka penerapannya dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dikenakan dengan pidana penjara paling lama 6 (enam tahun) dan denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah) kemudian Pasal 35 jo. Pasal 51 ayat (1) dikenakan dengan pidana penjara paling lama 12 (dua belas tahun) dan denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah), maka penetapan pada Pasal 35 jo. Pasal 51 ayat (1) dapat ditentukan sebagai pidana yang paling berat, yaitu hukuman maksimal 12 tahun penjara dan denda paling banyak

---

<sup>55</sup> Teguh Prasetyo, 2013, *Hukum Pidana*, PT. Raja Grafindo Persada, Jakarta, h. 182.

<sup>56</sup> *Ibid*, h. 181.

sebesar Rp. 12.000.000.000,00, kemudian pidana yang berat tersebut ditambah sepertiga untuk setiap pidananya. Pada pidana penjara,  $12 \text{ tahun} + (1/3 \times 12) = 16$  tahun penjara, lalu pada pidana denda Rp. 12.000.000.000,00 +  $(1/3 \times 12.000.000.000) = \text{Rp. } 16.000.000.000,00$  (enam belas miliar rupiah).

Dengan demikian, ancaman pidana dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) jika dijumlahkan yaitu 6 tahun + 12 tahun = 18 tahun, penjatuhan pidana tersebut tidak diperkenankan karena melebihi batas maksimum pidana penjara terberat setelah ditambah sepertiganya yaitu 16 tahun penjara, maka maksimum pidana penjara yang akan dijatuhkan adalah 16 tahun. Selain itu, jika pidana denda dijumlahkan Rp. 1.000.000.000 + Rp. 12.000.000.000 = Rp. 13.000.000.000,00 (tiga belas miliar rupiah), pidana denda tersebut diperkenankan karena tidak melebihi batas pidana denda terberat setelah ditambah sepertiganya yaitu Rp. 16.000.000.000,00.

Sesuai dengan uraian di atas, dapat disimpulkan bahwa pelaku phishing dalam *game online* telah dijatuhkan pidana sesuai dengan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 ayat (1) jo. Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan ancaman pidana paling lama 16 (enam belas) tahun penjara dan denda paling banyak sebesar Rp. 13.000.000.000,00 (tiga belas miliar rupiah).

Jenis pidana yang diberikan terhadap pelaku phishing dalam *game online* adalah pidana pokok yang meliputi pidana penjara dan pidana denda menurut

*stelsel straf* maksimum yang digunakan dalam KUHP. Hakim dapat memutuskan hukuman yang akan dijatuhkan (berapa tahun penjara dan besarnya denda) berdasarkan aturan dalam UU ITE. Ketentuan dalam pemidanaan tersebut, hakim dapat menggabungkan sistem alternatif atau sistem kumulatif, yang berarti hakim memiliki pilihan apakah tindak pidana tersebut dijatuhkan pidana penjara atau denda ataupun keduanya. Pemidanaan penjara terhadap pelaku phising dalam *game online* yaitu dengan memberlakukan pembatasan kebebasan bergerak seperti pelaku tindak pidana yang lain, selanjutnya pelaku di tahan di dalam lembaga pemasyarakatan dengan kewajiban menaati segala aturan yang berlaku di dalamnya.<sup>57</sup>

Dalam perumusan terhadap ancaman tindak pidana yang bersifat imperatif, merupakan warisan dari pemikiran aliran klasik dalam menentukan pidana dengan *definite science* (sistem perumusan ancaman pidana yang bersifat pasti).<sup>58</sup> Pidana penjara merupakan bentuk pidana yang paling sering digunakan oleh hakim untuk mengadili suatu perkara di Indonesia, bahkan hampir semua jenis tindak pidana yang ada terdapat ancaman pidana penjara. Akan tetapi, Muladi berpendapat bahwa akibat dari pidana penjara tersebut dapat menimbulkan prisonisasi, dehumanisasi bahkan dapat menyebabkan stigma buruk bagi mantan narapidana dalam kehidupan masyarakat.<sup>59</sup>

---

<sup>57</sup> P.A.F. Lamintang, 1984, "*Hukum Penitensier Indonesia*", Armico, Bandung, h. 69.

<sup>58</sup> Barda Nawawi Arief, 1994, "*Kebijakan Legislatif dalam Penanggulangan Kejahatan Dengan Pidana Penjara*", h.. 201-202.

<sup>59</sup> Widodo, 2009, "*Sistem Pemidanaan dalam Cyber Crime*", Aswaja, Yogyakarta, h.. 49.

Selanjutnya, pemidanaan bagi pelaku phising dalam *game online* yaitu pidana denda. Pidana denda termasuk jenis pidana yang paling ringan diantara jenis pidana yang lainnya dan merupakan salah satu pidana pokok yang tercantum dalam Pasal 10 KUHP. Pidana denda merupakan suatu aturan yang mewajibkan bagi pelaku tindak pidana untuk membayar sesuatu dalam bentuk uang, karena telah melanggar aturan hukum yang berlaku pada masyarakat. Pidana denda memiliki jenis yang berbeda dengan pidana penjara, pada pidana penjara memiliki tujuan untuk menghilangkan kemerdekaan, sedangkan pidana denda ditujukan pada harta benda yang dimiliki oleh pelaku tindak pidana.<sup>60</sup>

Dalam peraturan perundang-undangan, tidak dijelaskan secara tegas mengenai subjek hukum yang wajib memenuhi pidana denda terhadap suatu tindak pidana, hal tersebut dapat disimpulkan bahwa pembayaran denda bisa dilakukan oleh orang lain maupun pihak ketiga dari pelaku. Ketika denda yang seharusnya dijatuhkan kepada pelaku agar menimbulkan efek jera tidak sepenuhnya dilakukan oleh pelaku tersebut, maka tujuan pemidanaan denda terhadap pelaku phising dalam *game online* ini menjadi kurang maksimal.

Aturan hukum mengenai *cyber crime* khususnya tindak pidana phising dalam *game online* menurut peraturan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik masih mengalami keaburan hukum terhadap pengaturannya, hal itu disebabkan phising termasuk suatu perbuatan melanggar

---

<sup>60</sup> Sudarsono, 2002, "*Kasus Hukum*", Rineka Cipta, Jakarta, h. 16.

hukum yang menyebabkan kerugian bagi orang lain. Kerugian yang ditimbulkan dari tindak pidana ini merupakan suatu delik materiil, karena dalam perbuatannya telah merugikan orang lain berupa informasi pribadi yang diketahui oleh pelaku phising dan dapat menyebabkan hilangnya *account game* milik korban.

Menurut Pasal 35 jo. Pasal 51 ayat (1) UU ITE tidak memuat unsur kebohongan yang merugikan orang lain. Selain itu, dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE tidak memuat unsur manipulasi, penciptaan dan perubahan informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, hal ini berarti unsur seseorang membuat situs web yang seolah-olah mirip situs web asli tidak diatur dalam Pasal tersebut.<sup>61</sup>

Suatu aturan hukum tidak dapat diterapkan kepada pelaku tindak pidana apabila hukumnya mengalami masih mengalami kekaburan, misalnya dalam Pasal tersebut tidak memiliki konsep pidananya dan penafsiran yang bermacam-macam. Oleh karena itu, kebijakan hukum harus dilakukan terhadap UU ITE tersebut dengan merumuskan konsep secara khusus mengenai phising dalam *game online* serta merubah Pasal 35 UU ITE, karena isi Pasal 35 UU ITE untuk saat ini paling mendekati dengan konsep phising dalam *game online* tetapi masih terdapat beberapa unsur yang tidak di rumuskan dalam Pasal tersebut, sehingga Pasal 35 UU ITE masih mengalami kekaburan hukum.

---

<sup>61</sup> Ardi Saputra Gulo, 2020, "Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik", PAMPAS: Journal of Criminal, h. 78.

## BAB IV

### PENUTUP

#### 4.1 Kesimpulan

1. Teknik Pelaku Praktik Phising Dalam *Game Online* Terhadap *Cyber Crime*

Terjadinya phising dilakukan saat pelaku menyamar sebagai institusi resmi yang menggunakan situs web palsu, untuk mengelabui korban agar berbagi informasi pribadi. Tindakan phising biasanya memanfaatkan *e-mail*, website palsu, software dan berbagai media lainnya untuk melakukan aksinya. Dalam *game online* sendiri, serangan phising ini bertujuan untuk mendapatkan akses ke akun game milik korban yang di manfaatkan untuk mendapatkan barang berharga dalam *game* seperti karakter *game*, uang virtual, item virtual, dan inventaris lainnya. Hal tersebut dilakukan dengan cara membuat beberapa nama website yang mirip situs aslinya dan dianggap otentik. *Cyber crime* merupakan tindak kejahatan yang menggunakan media internet, oleh karena itu praktik phising dalam game online merupakan *cyber crime*.

2. Pertanggungjawaban Pidana Terhadap Pelaku Praktik Phising Dalam *Game Online*

Hukum di Indonesia mengenal asas *Lex Specialis Derogat Legi Generalis* yang berarti peraturan hukum yang lebih khusus mengesampingkan peraturan hukum yang lebih umum. Tindak pidana phising dalam game online merupakan suatu tindakan yang melawan hukum, maka penjatuhan pidana terhadap pelaku phising dalam game online dapat dikenakan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016