ANALISIS HUKUM TERHADAP PRAKTIK PHISING DALAM GAME ONLINE

KARYA ILMIAH

OLEH :

RIZKY AGUNG PRASETYO

NPM : 18300159

UNIVERSITAS WIJAYA KUSUMA SURABAYA

FAKULTAS HUKUM

PROGRAM STUDI HUKUM PROGRAM SARJANA

2023

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas rahmat, nikmat, dan karunia-Nya sehingga Karya Ilmiah dengan judul "Analisis Hukum Terhadap Praktik Phising Dalam Game Online" dapat terselesaikan dengan baik, walaupun jauh dari kata sempurna. Adapun maksud dan tujuan penyusunan Karya Ilmiah ini, yaitu dalam rangka memenuhi persyaratan guna memperoleh gelar Sarjana Hukum Program Studi Hukum Universitas Wijaya Kusuma Surabaya.

Semoga karya ilmiah yang telah tersusun ini dapat bermanfaat, dapat dijadikan pedoman bagi para pembaca, dan menambah wawasan serta pengalaman. Penulis juga menyadari bahwa masih banyak terdapat kekurangan yang ditemukan dalam Karya Ilmiah ini. Oleh sebab itu, penulis mengharapkan saran dan kritik yang membangun sebagai bahan evaluasi guna memperbaiki Karya Ilmiah ini. Terima kasih.

Surabaya, 11 Agustus 2023

Penulis

DAFTAR ISI

BAB I
PENDAHULUAN

1.1. Latar Belakang

Game Online adalah permainan yang dimainkan secara online melalui LAN (*Local Area Network*), internet, atau bahkan telekomunikasi. *Game Online* berbeda dari video dan permainan komputer yang tidak terhubung ke jaringan, *Game Online* merupakan salah satu sarana hiburan baru yang saat ini banyak digemari mulai dari anak-anak, remaja, hingga dewasa. Masyarakat dapat mengakses *game online* melalui perangkat komputer, laptop maupun *smartphone*. Game Online yang digemari pada perangkat komputer atau laptop *adalah Dota 2*, *Fortnite*, *Apex Legends*, *Grand Theft Auto V* (GTA*)*, dan *Valorant*, sedangkan pada *smartphone* yang banyak digemari adalah *Player Unknown's Battle Ground Mobile* (PUBGM), *Mobile Legends*, *Clash of Clans*, dan *Free Fire*.

Salah satu permasalahan yang perlu diperhatikan adalah kejahatan siber. Kejahatan siber (*cyber crime*) merupakan bentuk kejahatan virtual yang memanfaatkan media yang terhubung dengan internet dan hal ini dapat merugikan pengguna jasa internet. Modus operandi dari kejahatan siber sendiri sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi. Kejahatan siber memiliki dua fokus utama, yaitu penyalahgunaan teknologi siber sebagai fasilitas untuk melakukan suatu kejahatan dan menjadikan siber itu sendiri sebagai obyek kejahatan. Hal ini membuat hukum yang telah diterapkan menjadi aturan siber sebagai suatu tumpuhan hukum dalam mendukung penegahan hukum atas kriminalitas yang sudah dilakukan.

Kejahatan siber dalam *game online* salah satunya adalah phising. Phising merupakan aktifitas yang menggunakan rekayasa sosial dan tipuan teknis untuk mencuri data pribadi dan kredensial akun dalam hal ini adalah akun *game online*. Proses phising ini bermaksud untuk menangkap informasi yang sensitif seperti username, password, maupun informasi lainnya dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya (*legitimate organization*) dan biasanya berkomunikasi secara elektronik.

1.2. Rumusan Masalah

Adapun perumusan masalah dari laporan ilmiah ini, yaitu:

1. Bagaimana teknik pelaku praktik phising dalam *game online* terhadap *cyber crime* ?
2. Bagaimana pertanggungjawaban pidana terhadap praktik phising dalam *game online* ?

1.3. Tujuan

Tujuan dan manfaat dari laporan ilmiah ini untuk mengerti dan memahami bagaimana teknik pelaku phising dalam *game online s*ehingga termasuk *cyber crime* dan untuk mengetahui terkait pertanggungjawaban pidana terhadap praktik phising dalam *game online.*

BAB II
KAJIAN PUSTAKA

2.1 *Cyber Crime* Dalam Bentuk Phising

Phising (password harvesting fishing) adalah tindakan penipuan yang menggunakan email palsu atau situs website palsu yang bertujuan untuk mengelabui pengguna sehingga pelaku bisa mendapatkan data pengguna tersebut. Penipuan ini berupa sebuah email yang seolah-olah berasal dari sebuah perusahaan resmi, misalnya bank dengan tujuan untuk mendapatkan data-data pribadi seseorang, seperti kata sandi, nomor rekening, nomor kartu kredit, dan sebagainya**.**

Terjadinya phising dilakukan saat seseorang menyamar sebagai orang lain yang menggunakan situs web palsu, untuk mengelabui korban agar berbagi informasi pribadi. Tindakan phising biasa dilakukan dengan cara penyerang mengirimkan email yang seolah-olah berasal dari bank atau layanan web terpercaya yang biasa digunakan korban. Subjek email phising tersebut biasanya berisi "Harap perbarui informasi anda di bank!" Email tersebut akan berisi tautan phising yang seakan mengarahkan korban ke situs website resmi, yang mana sebenarnya akan mengarahkan korban ke situs web penipu. Pada website phising korban akan diminta untuk masuk dan tanpa sengaja mengungkapkan nomor rekening bank, nomor kartu kredit, sandi atau informasi sensitif lainnya kepada penipu

2.2. Praktik Phising dalam *Game Online* Termasuk *Cyber Crime*

Game online menghubungkan kita dengan orang – orang di seluruh dunia, tetapi juga memaparkan kita terhadap resiko keamanan *cyber* seperti serangan phising, virus, dan pencurian identitas. Resiko ini dapat menyebabkan kerugian yang mempengaruhi kita secara individu atau organisasi dan bisnis yang terhubung dengan

kita. Dalam game online serangan phising ini bertujuan untuk mendapatkan akses ke akun game milik korban yang di manfaatkan untuk mencuri barang berharga game, karakter dalam game, uang virtual, item virtual, dan inventaris lainnya. Terkadang, serangan ini mengambil alih dan menjual akun korban di pasar gelap. Dalam beberapa kasus, pelaku phising menggunakan informasi keuangan korban lebih jauh untuk melakukan pembelian dari akun korban tanpa sepengetahuan atau izin dari korban.

Cara kerja pelaku phising adalah dengan membagikan link yang seolah – olah resmi dari platform game tersebut melalui profil media sosial seperti Twitter atau Facebook untuk mendapatkan hadiah. Ketika para korban tergiur, otomatis mereka akan *click* link tersebut dan di wajibkan mengisi *username* dan *password* akun platform game. Setelah pengguna mengisi, akan muncul notifikasi bahwa proses *entry* gagal pengguna diminta untuk memberikan informasi tambahan seperti nama lengkap, email pribadi, nomor telepon, dan informasi tambahan lainnya. Akibatnya pelaku phising tidak hanya mendapatkan akun game korban saja, tetapi juga detail pribadi lainnya. Hal ini bertujuan untuk mendapatkan keuntungan dengan cara menjual akun game milik korban.

2.3. Metode dan Teknik Serangan Phising

Banyak cara yang dilakukan pelaku phising untuk mendapatkan korban dan hal ini biasanya terus berkembang sesuai dengan perkembangan yang ada di dalam dunia internet, diantaranya :

1. Email

   Pelaku phising mengggunakan Email untuk penipuan dikarenakan murah dan mudah untuk digunakan. Pelaku phising dapat mengirimkan jutaan email setiap harinya tanpa perlu mengeluarkan biaya yang cukup besar.

2. Sosial Media

   Sosial Media menjadi media favorit bagi pelaku phising, karena saat ini sosial media menjadi platform terbesar sebagai tempat berinteraksi dan menyediakan fasilitas untuk melakukan aktifitas sosial bagi penggunanya.

3. Web-baseddelivery

   Pelaku biasanya membuat website yang mirip dengan website-website terkenal untuk mengelabui korbannya. Membuat website yang mirip dengan website perusahaan besar sangatlah mudah untuk dilakukan karena pelaku hanya perlu membuat tampilan yang sama, tanpa perlu memperhatikan fungsi atau fasilitas yang sama karena tujuannya adalah agar korban memasukkan username dan password di dalamnya

4. Instant Messaging

   Media chatting banyak digunakan oleh pelaku phising untuk mengirimkan alamat-alamat yang menjebak kepada korbannya. Biasanya pelaku mengirimkan tautan ini secara acak namun ada juga yang melakukan pendekatan terlebih dahulu sebelum mengirimkan informasi situs palsu ini.

5. Trojan

   Pelaku phising, tak jarang melakukan tindakan menipu korbannya untuk menginstall trojan dan memanfaatkan trojan tersebut untuk mengelabui korbannya. Trojan sendiri memungkinkan pengontrolan secara penuh komputer korban sehingga korban bisa dialihkan ke situs yang telah disediakan jebakan.

2.4. 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. Karena phising termasuk dalam *cyber crime*, maka pertanggungjawaban pidana pada pelaku phising dalam *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 phising tersebut.

Pasal yang terdapat di KUHP dan UU ITE terdapat hal-hal yang berbeda dalam pengaturan dan sanksi pidananya. Dari sisi formulasi perumusuan 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. 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.

Pertanggungjawaban pidana terhadap praktik phising dalam *Game Online* dapat dikenakan Pasal berlapis yaitu 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 serta tidak boleh melebihi maksimum pidana yang terberat ditambah sepertiga, sistem ini dikenal sebagai kumulasi diperlunak. Dapat disimpulkan bahwa pelaku phising dalam *game online* telah dijatuhkan pidana sesuai dengan Pasal tersebut dengan ancaman pidana penjara paling lama 16 tahun dan denda paling banyak sebesar 13 milliar rupiah.

BAB III
PEMBAHASAN

3.1. Hasil dan Pembahasan

Phising merupakan aktifitas yang menggunakan rekayasa sosial dan tipuan teknis untuk mencuri data pribadi dan kredensial akun dalam hal ini adalah akun *game online*. Proses phising ini bermaksud untuk menangkap informasi yang sensitif seperti username, password, maupun informasi lainnya dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya (*legitimate organization*) dan biasanya berkomunikasi secara elektronik. Jadi phising dalam *game online* merupakan suatu tindak kejahatan yang menggunakan sarana yang terhubung melalui jaringan internet atau telekomunikasi, maka dari itu phising dalam game online dapat dikategorikan dalam kejahatan siber (*cyber crime*). Untuk pertanggungjawaban pidana pelaku praktik phising dalam game online, karena Indonesia mengenal asas *Lex Specialis derogat legi Generalis*, jadi pelaku tindak pidana phising dalam game online tidak dapat dikenakan Pasal dalam KUHP, melainkan UU ITE yaitu dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) dengan Pidana penjara maksimal 16 Tahun dan Pidana denda maksimal 13 Milliar Rupiah.

BAB IV
PENUTUP

4.1. KESIMPULAN

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*.

4.2. SARAN

Wawasan masyarakat terhadap dampak yang ditimbulkan terhadap *cyber crime* perlu ditingkatkan kembali, karena dalam aktifitas sehari-hari di era modern saat ini tidak dapat dipisahkan dari sebuah gadget atau internet. Maka perlu adanya kerjasama antara masyarakat dan pemerintah dalam mengatasi kejahatan phising tersebut, karena kejahatan yang terjadi di dunia maya semakin hari semakin berkembang baik dari jenis kejahatannya maupun modus operandinya.

DAFTAR PUSTAKA

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

Aseh Ginanjar, Nur Widiyasono, Rohmat Gunawan, 2018, "Analisis Serangan Web Phising pada Layanan E-commerce dengan Metode Network Forensic Process", 2 (2).

Eko Adi Susanto, 2018. *"Pertanggungjawaban Pidana Yang Memakai Surat Palsu Ditinjau Dari Pasal 263 Ayat (2) KUHP"*, 1 (1)

Florida Mathilda, 2012, "Cyber Crime Dalam Sistem Hukum Indonesia", 4 (2).

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, 2 (3).

Malahayati, Darul Fata, 2021, "Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising", 2 (1).