Skripsi Rizky (Turnitin)..pdf

by

Submission date: 10-Jul-2023 12:16PM (UTC+0800)
Submission ID: 2128900114
File name: Skripsi Rizky (Turnitin)..pdf (796.91K)
Word count: 11240
Character count: 69948

ANALISIS HUKUM TERHADAP PRAKTIK PHISING DALAM *GAME ONLINE*

SKRIPSI

OLEH :

RIZKY AGUNG PRASETYO

NPM : 18300159

UNIVERSITAS WIJAYA KUSUMA SURABAYA

FAKULTAS HUKUM

PROGRAM STUDI HUKUM PROGRAM SARJANA

2023

BAB I
PENDAHULUAN

1.1 Latar Belakang dan Perumusan Masalah

Perkembangan teknologi yang semakin maju maka pertumbuhan kasus kejahatan yang terjadi di dalam masyarakat juga meningkat. Perkembangan teknologi juga ikut memberikan dampak positif maupun negatif yang tidak dapat dihindari. Kemajuan dan perkembangan revolusi industri maupun teknologi pada internet sudah tidak asing lagi di kalangan masyarakat, hal ini didasari oleh tersebar luasnya koneksi internet dan kemudahan untuk mengaksesnya. Internet tidak hanya digunakan pada perangkat seperti komputer atau laptop tetapi juga bisa digunakan melalui *smartphone*.

Smartphone adalah telepon seluler yang memiliki kemampuan lebih baik dari segi resolusi, fitur, hingga komputasi termasuk adanya sistem operasi *mobile* didalamnya.[1] Era globalisasi saat ini tidak hanya menggunakan s*martphone* sebagai alat bantu komunikasi tetapi masyarakat dapat mengakses berbagai macam aplikasi yang terhubung di internet diantaranya adalah sosial media, *game online*

[1] Intan Trivena Maria Daeng, N.N Mewengkang, Edmon R Kalesaran, Penggunaan Smartphone Dalam Menunjang Aktivitas Perkuliahan Oleh Mahasiswa Fispol Unsrat Manado, Vol. 6, No. 1, Tahun 2017, Hal. 1.

marketplace, aplikasi bank, streaming video dan musik, aplikasi kesehatan bahkan aplikasi kencan dapat diakses melalui *smartphone*.[2]

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.[3] *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*.[4]

Perkembangan *game online* di Indonesia terus mengalami kemajuan yang cukup signifikan seiring dengan bertambahnya jumlah pengguna *smartphone*. Berdasarkan data *AppAnnie*, 30% unduhan *game mobile* di Asia Tenggara ada di Indonesia pada tahun 2020. Posisi kedua ditempati Vietnam (22%), Filipina (16%), dan Malaysia 8%. Sejalan dengan hal tersebut, Indonesia merupakan negara yang

---

[2] Malahayati, Darul Fata, Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising, Vol. 2, No. 1 Tahun 2021, Hal. 22.

[3] Ying-Chieh Chen, Patrick S. Chen, Ronggong Song, Larry Korba, Online Gaming Crime and Security Issue Cases and Countermeasures from Taiwan, Tahun 2004.

[4] Eryzal Novrialdy, Kecanduan *Game Online* pada Remaja: Dampak dan Pencegahannya, Vol. 27, No. 2, Hal. 149.

paling banyak pengguna *game online* di Kawasan Asia Tenggara dengan rata-rata masyarakatnya mengabiskan waktu dengan *game online* sebanyak 16,5%.[5]

Berdasarkan data yang ada pengguna *game online* di Indonesia pada tahun 2017 sebanyak 43,7 juta, sehingga membuat Indonesia menduduki peringkat 16 besar dunia dalam hal pendapatan *game*.[6] Kemudahan akses dan banyaknya pengguna dapat berdampak buruk jika tidak disikapi dengan baik, berbagai permasalahan yang terjadi karena *game online* banyak mendapat perhatian dari masyarakat luas. Berbagai permasalahan tersebut seperti yang terjadi pada remaja adalah sering bolos sekolah, mencuri, berbohong, pemborosan, perilaku menyimpang, kekerasan, hubungan dengan keluarga atau teman berkurang dan kejahatan siber.

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.[7] 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

---

[5] Katadata, "Masa Depan Cerah Gim Online di Indonesia", dalam katadata.co.id, diakses tanggal 1 Februari 2022.

[6] Newzoo, "The Indonesian Gamer", dalam newzoo.com, diakses tanggal 27 Januari 2022.

[7] Fiorida Mathilda, Cyber Crime Dalam Sistem Hukum Indonesia, Vol. 4, No. 2, Tahun 2012, Hal. 34 dan 44.

sebagai suatu tumpuhan hukum dalam mendukung penegahan hukum atas kriminalitas yang sudah dilakukan.[8]

Kejahatan siber dalam *game online* salah satunya adalah phising. Phising merupakan aktifitas yang memakai tipuan sosial dan rekayasa teknis untuk mengambil identitas diri dan isi akun dalam hal ini adalah akun *game online*. Proses phising ini bermaksud untuk mendapatkan informasi yang penting seperti username, password, maupun informasi lainnya dalam wujud mencontoh sebagai sebuah organisasi yang dapat dipercaya (*legitimate organization*) serta berkomunikasi secara eIektronik.[9]

Berdasarkan data yang ada kejahatan siber bermodus phising ini menunjukkan angka 42% dari teknik selain phising yang disebutkan dalam website *Anti-Phising Working Group* (APWG), hal ini membuat kejahatan phising tersebut perlu diperhatikan. Phising dalam *game online* perantara yang digunakan adalah apapun yang terhubung ke internet seperti dari surat elektronik maupun website.[10] Salah satu contoh biasanya penjahat siber akan membagikan dan memberikan tautan dengan iming-iming hadiah pada game online agar orang lain ingin membukanya. Padahal saat dibuka *link* tersebut merupakan jebakan yang bertujuan untuk mengumpulkan data diri kita. Rancangan jebakan yang digunakan untuk mengarahkan korban adalah dengan skema rekayasa sosial yang menggunakan *e-*

---

[8] Barda Nawawi Arief, Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia, Tahun 2006, Hal. 1.

[9] Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi, Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, Vol. 1, No. 2, Tahun 2020, Hal. 70-71.

[10] Ibid., Hal. 71.

mail palsu dan mengaku berasal dari institusi bisnis yang sah sehingga bisa mengelabui korban, nantinya korban dapat membocorkan data-data seperti nama dan kata sandi akun *game online* maupun *e-mail*.[11]

Pengetahuan pengguna *game online* yang minim terhadap hal tersebut adalah dampak sehingga terjadilah praktik phising, terlebih masih banyak pemakai game online dengan rentang anak-anak hingga remaja. Oleh karena itu, pemakai teknologi juga harus banyak menambah ilmu khususnya terkait phising ini. Banyaknya pengguna game online yang dapat mengundang terjadinya kejahatan phising ini membuat perlu adanya Peraturan Perundang-Undangan yang berkaitan tentang kejahatan di dunia maya terutama dalam hal ini adalah praktik kejahatan phising. Berdasarkan latar belakang tersebut, hal ini membuat penulis tertarik mengangkat judul **"ANALISIS HUKUM TERHADAP PRAKTIK PHISING DALAM *GAME ONLINE*"**

Adapun perumusan masalah oleh penulis dalam penelitian ini adalah :

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

---

[11] Aseh Ginanjar, Nur Widiyasono, Rohmat Gunawan, Analisis Serangan Web Phising pada Layanan E-commerce dengan Metode Network Forensic Process, Vol. 2, No. 2, Tahun 2018, Hal.148.

1.2 Tujuan Penelitian

1. Untuk mengerti dan memahami apakah tindak pidana phising dalam *game online* termasuk *cyber crime*
2. Untuk mengetahui terkait pertanggungjawaban pidana terhadap praktik phising dalam *game online*.

1.3 Manfaat Penelitian

1. Dari segi teoritis, hasil penelitian ini diharapkan dapat memperluas pengetahuan penulis dan diharapkan dapat memberikan kepustakaan bagi pengembangan ilmu di bidang hukum pidana. Selain itu, agar menjadi dasar pemikiran teoritis sehingga dapat memberikan kemanfaatan, keadilan, dan kepastian hukum.
2. Dari segi praktis, hasil penelitian ini diharapkan dapat membantu penulis mengembangkan ilmu yang telah dipelajari dan diharapkan dapat menjadi bahan pertimbangan bagi pembentuk undang-undang khususnya DPR (Dewan Perwakilan Rakyat) terkait dengan RUU-KUHP terutama tentang kejahatan siber (phising).

1.4 Kerangka Konseptual

1.4.1 Tinjauan Umum mengenai Tindak Pidana

Strafbaarfeit merupakan istilah tindak pidana yang tertuang dalam KUHP, sedangkan pada beberapa kepustakaan mengenai hukum pidana kerap memakai delik sebagai istilahnya, di sisi lain, para pencipta undang-undang pada perumusan undang-undang memakai tindak pidana, perbuatan pidana, ataupun peristiwa

pidana sebagai istilahnya.[12] Dalam ilmu hukum, tindak pidana mengandung pengertian dasar yakni sebagai istilah yang diwujudkan melalui kesadaran dalam membagikan karakteristik tertentu dalam peristiwa hukum pidana. Dalam hal ini, tindak pidana memiliki definisi yang bersifat abstrak dari kejadian-kejadian konkrit pada lapangan hukum pidana, dengan demikian tindak pidana wajib ditandai dengan arti yang memiliki sifat ilmiah serta ditargetkan secara jelas guna menjadi pemisahan dengan istilah yang digunakan dalam keseharian masyarakat.

Tindak pidana adalah suatu istilah guna mendeskripsikan sesuatu perilaku yang bisa dipidana, atau yang dalam Bahasa Belanda kita kenal dengan *straftbaarfeit*. Adapun istilah lain yang juga bisa digunakan untuk mendeskripsikan perilaku yang bisa dipidana yakni:

1. Peristwa pidana;
2. Perbuuatan pidana;
3. Pelangggaran pidana;
4. Perbuatan yg biisa dihukum.[13]

Tindak pidana adalah pengertian paling mendasar pada hukum pidana. Tindak pidana sebenarnya adalah pengertian secara yuridis, yang berbeda dibandingkan dengan istilah suatu kejahatan. Tindak kejahatan dalam arti yuridis formal adalah wujud dari perilaku yang dianggap telah melanggar undang-undang dalam hal pidana. Oleh karena demikian, setiap perbuatan yang telah jelas tidak diizinkan oleh undang-undang harus dihindari dan setiap peraturannya wajib ditaati,

[12] Andi Hamzah, Asas-Asas Hukum Pidana, Rineka Cipta, Jakarta, 1994, Hal. 72.
[13] Masruchin Rubai, Asas-Asas Hukum Pidana, UM press dan FH UB, Malang, 2001, Hal.21.

manakala seseorang melanggar maka orang tersebut dapat dikenakan sanksi pidana. Jadi, seluruh larangan beserta kewajiban menjadi keharusan untuk ditaati setiap masyarakat sebagaimana tercantum dalam undang-undang beserta peraturaan-peraturan dari pemerintah dari pusat hingga daerah.[14]

Pada umumnya, delik merupakan sinonim dari tindak pidana yang berasal dari bahasa Latin yaitu *delictum*. *Delict* merupakan sebutan bahasa jerman dan bahasa belanda, dan delik sebutan dalam bahasa indonesia. Dalam KBBI sendiri, delik merupakan perbuatan yang bisa diberikan hukuman sebab telah menajdi pelanggaran dari suatu tindak pidana.[15] Menurut Simons, delik yang dalam *strafbaarfeit* termasuk perlakuan yang melanggar hukum oleh seseorang baik dilakukan sengaja maupun tidak sengaja yang atas tindakan tersebut bisa dipertanggungjwabkan dan bisa dihukum berdasarkan undang-undang yang telah menyatakan perbuatan tersebut melanggar hukum.[16]

1.4.2 Tinjauan Umum mengenai Cyber Crime

Jika mnyebut *cyber crime*, maka kita mengulas mengenai keamanan dari jaringan suatu computer ataupun juga berkaitan dengan keamanan dari informasi teknologi dan telekomunikasi. Khususnya pada zaman globalisasi ini yang kian menghantarkan kita pada pesatnya perkembangan teknologi yang tidak dapat dipisahkan dari kemungkinan penyalahginaan pemanfaatan dari teknologi tersebut. Teknlogi yang sudah mengalami kemajuan tidak dipungkiri memberikan dampak

---

[14] P.A.F. Lamintang, Dasar-Dasar Hukum Pidana Indonesia, PT. Citra Adityta Bakti, Bandung, 1996, Hal. 7.

[15] Teguh Prasetyo, 2011,Hukum Pidana, Rajawali Pers, Jakarta, Hal. 47.

[16] Andi Hamzah, Azas-Azas Hukum Pidana, Yarsif Watampone, Jakarta,2005, Hal. 95.

signifikan pada masyarakat, baik dari sisi dampak positifnya maupun dampak negatif bagi keberlangsugan peradaban manusia. Adapun dampak negatif yang dimaksudkan dalam hal ini teknologi yang digunakan untuk melangsungkan suatu kejahatan. J. E. Shaetapy menjelaskan bawa kejahatan itu berkaitan erat serta menjadi bagian dari hasil atau ciptaan budaya itu sendiri. Dengan demikian, dapat dikatakan bahwa ketika budaya pada suatu bangsa semakin tinggi atau makin modern, maka akan wujud, metode, dan pelaksanaan dari kejahatan juga akan makin modern.[17]

Menilik kembali perkembangan dunia digital mulai dari teknologi komputer, informasi, hingga teknologi komunikasi kini telah mengalami kemunculan tindak delik baru yang berbeda dengan tindakan yang dilakukan dengan cara konvensional. Dari ketiga dampak perkembangan tekonologi tersebut, penyalahgunaan teknologi komputer memiliki sifat dengan karakteristik tersendiri, sehingga menjadikan permasalahan yang *complicated* dan sulit untuk menemukan pemecahan masalah penanggulannya baik dari tahap penyelidikan, penyidikan, maupun penuntutan.[18] Oleh karena demikian, berdasarkan pendapat-pendapat tersebut, bisa dikatakan bahwa terjadinya perkembangan teknologi dan informasi yang terus mengalami kemajuan selain bisa membantuk manusia guna komoditi informasi, namun turut memberikan dampak negatif berupa penyalahgunaan dari teknologi yang berujung menjadi tindak pidana dengan istilah *cyber crime*.

37

[17] J. E Prasetyo dalam Abdul Andik, 2002, Kriminologi dan Kejahatan Kontemporer, Lembaga Penerbitan Fakultas Hukum Unisma, Malang.

Perlu dicatat bahwa tindak pidana *cyber crime* mempunyai ciri-ciri tersendiri sebab berkaitan dengan jaringan dari teknologi komputer, maka cara menanganinya pun akan berbeda dengan penanganan tindak pidana yang dilakukan secara konvensional. *Cyber crime* adalah kejahatan yang tidak sama dibandingkan *street crime* atau kejahatan secara konvensional, *cyber crime* ini lahir secara bersama dengan munculnya revolusi teknologi informasi. Pemaknaan dari *cyber crime* dapat diartikan dalam artian yang lebar dan pendek. *Cyber crime* dalam arti sempit dapat diartikan tindakan pelanggaran aturan yang dilakukan melalui pemanfaatan teknologi komputer. Di sisi lain, *cyber crime* dalam arti luas diatikan sebagai keseluruhan dari wujud kejahatan yang diperuntukkan bagi komputer, baik itu dari segi jaringan ataupun *user* dan juga kejahatan secara konvensional dengan memakai teknologi komputer. Dalam peraturan perundang-undangan di negara kita, *cyber crime* disebut sebagai tindak pidana yang memiliki keterkaitan dengan teknologi informasi.

1.4.3 Tinjauan Umum mengenai Game Online

Berbicara mengenai permainan dalam wujud digital atau yang kerap dikenal sebagai *game online,* merupakan berbagai jenis permainan namun hanya bisa dimainkan dikala kita terhubung dengan perangkat yang menampung jaringan internet. Dari sinilah kemudian pemain *game online* bisa bermain dengan pengguna lainnya dalam hal mengakses permainan tersebut pada waktu yang bersamaan. *Game online* dapat diartikan sebagai game onlin yang kemudian digunakan selama terhubung dengan jaringan komputer, memakai komputer pribadi ataupun konsol *video game*. Kadang-kadang, *gim onlen* disajkan oleh para penyedia jasa internet

sebagai tambahan fitur yang menyatakan bahwa kita menjadi langganan dalam memakai jasa mereka, atau bahkan *game online* bisa langsung dipakai pada sistem yang sudah disajikan oleh para *developer game*. Untuk mengetahui perbedaaan antara *game online* dengan *game offline* ada beberapa poin yang perlu digarisbawahi, yaitu:

1. Dari segi jenis, pada *game offline* mempunyai beragam jenis permainan, sedangkan *game offline* biasanya lebih sedikit. Hal tersebut disebabkan karena *developer game offline* mesti menciptakan permainan yang mengikuti arus pasar, sedangkan *game online* hanya memerlukan untuk perbaruan dari *game*-nya saja.
2. Dari sisi jumlah pemain, *game online* bisa dimainkan oleh orang dengan jumlah yang banyak sampai lintas negara karena yang digunakan adalah jaringan internet, sedangkan *game offline* hanya bisa dinikmati oleh satu sampai dua orang pemain saja.
3. Dari sisi grafik, *game online* memerlukan kestabilan jaringan internet dan perangkat yang memadai guna menghadirkan tampilan grafik dengan kualitas bagus agar tidak mengalami *lagging*, sedangkan *game offline* hanya memerlukan spesifikasi dari perangkat yang cukup mumpuni agar bisa memainkan *game*-nya.
4. Dari segi sosial, *game online* memiliki fitur supaya senantiasa masih terhubung dengan pemain yang lain karena memakai koneksi internet. Sedangkan, *game offline* tidak bisa bersosialisasi dalam permainannya karena tanpa menggunakan jaringan internet.

5. Dari segi alur ceritanya, *game online* mempunyai alur cerita yang tak terbatas karena diwajibkan untuk senantiasa menggali dunianya serta mempunyai berbagai misi untuk bisa dijalankan. Namun, *game offline* mempunyai alur cerita yang pakem sebab telah diatur sebelumnya oleh *developer game* tersebut.

Keadaan di dalam *game online* itu dibuat seolah-olah mirip seperti dunia nyata. Adapun *game online* yang saat ini bertaburan kita temui di masyarakat, sebenarnya mulai tahun 2003 Indonesia yang pada saat itu *game* yang dinamakan *Ragnarok Online, Gunbond, Seal online* tengah digandrungi namun untuk bisa bermain, sang pemain haru membayar terlebih dahulu dengan maksud juga untuk menarik pemain-pemain lainnya agar berminat pada *game* tersebut.

Melihat fenomena tersebut, saat ini sudah sangat banyak *game online* yang menyajikan ketersediaan dari fitur untuk "komunitas online", dengan begitu kegiatan *game online* ini kini sudah menjadi aktivitas sosial yang mendarah daging. *Game-game* dengan fitur tersebut saat ini lebih banyak peminatnya dibandingkan dengan *game* satu orang pemain saja, hal tersebut karena *game* dengan komunitas dianggap lebih menantang dimana akan ada kepuasan tersendiri saat bisa mengalahkan orang lain pada permainan tersebut, belum lagi dengan kecanggihan teknologi era ini yang memudahkan pemain *game online* untuk bermain via *gadget* dan tidak lagi hanya melalui komputer. Dalam *game online* sendiri, pemain bisa bebas melalukan apapun yang diinginkan, namun seringnya dalam ruang virtual ini,

pemain *game online* kerap tidak menyadari apa yang dilakukan dalam *game* tersebut ternyata dilarang atau justru berbahaya dan bisa merugikan dirinya.[19]

1.4.4 Tinjauan Umum mengenai Praktik Phising

Praktik phising diambil dari kata "*fishing*" yang berarti memancing. Hal ini, bisa diartikan sama seperti memancing, phising merupakan kejahatan yang dilakukan dengan cara memancing atau memanfaatkan umpan. Umpan biasanya berupa berita palsu yang dibuat seolah-olah berawal dari pihak yang berwenang dan berisi informasi yang beragam berupa ajakan untuk melakukan pembaruan informasi akun yang ditargetkan.[20] Terdapat modus praktik phising dalam *game online*, yang paling sering adalah phising melalui *link* yang menghubungkan ke suatu *web forgery* atau web phising yang dirancang untuk membohongi pengunjungnya. Biasanya tampilan web tersebut dibuat semirip mungkin dan pengunjung dituntun untuk memasukkan identitasnya dalam suatu formulir yang telah disiapkan oleh pelaku. Sesudah korban menginput beberapa data pribadi, nantinya data tersebut akan tersimpan dalam *database* pelaku, data ini lah yang diincar pelaku untuk disalahgunakan. Dalam hal *game online*, biasanya para pelaku akan menggunakan data tersebut untuk mengambil alih akun-akun pengguna *game online* yang di dalamnya terdapat *virtual property*. Salah satu contoh adalah pada *virtual property* dalam *game online Mobile Legend* yaitu *skin hero*, *diamond*, dan pangkat (*tier*) dari game tersebut yang mana jika nilainya tinggi maka pelaku

---

[20] Erizka Permatasari, S.H., Jerat Hukum Pelaku Phising dan Modusnya, dalam hukumonline.com, diakses pada tanggal 1 Februari 2022.

mendapatkan keuntungan dengan cara menjual kembali akun tersebut dengan harga tinggi.

Pelaku praktik phising sendiri dapat dijerat sesuai dengan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi EIektronik. Pelaku praktik phising dalam *game online* ini juga dapat dikenakan dengan sebagian tindak pidana seperti penipuan, penciptaan dan manipulasi surat atau dokumen eIektronik.

Pasal 378 KUHP mengatur penipuan dengan menyatakan bahwa peIaku yang memenuhi unsur dalam pasal tersebut akan dikenakan kurungan penjara selama 4 tahun. Pemalsuan surat dijerat Pasal 263 ayatt (1) KUHP yangmembuktikan bahwa pelaku yang memenuhi unsur tersebut dapat dikenai pidna penjara paIing lama 6 tahun. PeIaku yang mengirimkan link seolah-olah asli (manipulasi) akan dijerat Pasal 35 *jo.* Pasal 51 UU ITE yang menyatakan bahwa peIaku yang jika masuk unsur dari pasal tersebut maka akan dikenakan pidana penjara paling lama 12 tahun dan/atau denda paling banyak 12 miliar. Selain itu, peIaku yang sengaja serta tanpa hak menyebarluaskan berita tidak benar dan dapat mengakibatkan kerugian dijerat dengan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE, pelaku yang memenuhi unsur pada Pasal tersebut bisa dikenai pidana penjara paling lma 6 tahun dan denda palingg banyak 1 miliar.

1.4.5 Tinjauan Umum mengenai Penanggulangan Tindak Pidana

Ketika melihat berdasarkan sudut kebijakan kriminal, cara melakukan penanggulangan kejahatan menggunakan sarana *penal* tidak termasuk kebijakan yang terbaik, karena seperti yang kita ketahui kebijakan memiliki batas dan ada kelemahan dan hal negatif. Oleh karena itu, melakukan penanggulangan kejahatan melalui jalur *non penal* atau diluar hukum pidana lebih baik digunakan karena menonjolkan pada sifat pencegahan atau preventif. Kebijakan *Non penal* yaitu kebijakan yng berhubungan pada pencegahan kejahatan yang sifatnya pencegahan sebelum terjadii tindak pidana yang tujuannya menyelesaikan dan menghapus faktor-faktor kondsif yang bisa menimbulkan terjadinya tindk pidana. *Non Penal Policy* sebagai upaya penanggulangan kejahatan diluar hukum memiliki sasaran utama dengan menyelesaikan beberapa faktor permasalahan pada terjadinya tindak kejhatan. Beberapa faktor kondusif tersebut ialah berpusat dalam permasalahan ataupun kondisi pada sosial yang secra langsung atau tidak langsung dapat memunculkan kejahatan.[21]

Melakukan penanggulangan kejahatan jalur non penal merupakan tindakan pencegahan dari terjadinya kejahatan, dengan sasaran paling utama terkait dengan faktor kondusif yang menjadi penyebab terjadinya suatu kejhatan baik yang berpusat pada masalah atau kondisi sosial yang langsung atau tidak langsung menimbulkan suatu kejahatan. Jika dilihat dari sudut politik kriminal baik melalui cara makro maupun global, maka melakukan penanggulangan kejahatan jalur *non*

[21] Barda Nawawi Arief, 2008, *Op cit*. Hal. 72

penal menduduki tempat yang strategis dari keseluruhan dalam politiik kriminal. Melakukan penanggulangan *non penal* bisa terjadi dari berbagai sumber lainnya yang juga mempunyai kemampuan efek preventif, contohnya sosial mediia, dimanfaatkannya kemajuan teknologi dan pemanfaatan potensi efek-preventif dari aparatur penegakan hukum.

1.4.6 Tinjauan Umum Mengenai Pertanggungjawaban Pidana

Pertanggunjawaban pidana memiliki arti yang lain yaitu *teorekenbardheid* atau criminal *responbility* yang menjurus pada pemidanaan terhadap pelakunya, yang bertujuan untuk menentukan dapat atau tidaknya terdakwa atau tersangka bertangung jawaab atas tindak pidana yang dikenakan. Dalam Bahasa Belanda, menurut Pompee istilah pertanggungjawaban pidana memiliki persamaan bukan orangnya, melainkan perbuatan yang dipertanggungjawabkan terhadap seseorang.

dalam perbuatan melanggar hukum merupakan persoalan pemilihan di antara bebeberapa alternatif. Oleh karena itu, penetapan dan pemilihan pertanggung jawabaan pidana tidak bisa lepas dari banyaknya pemrtimbangan yang sifat rasional serta adil sesuai pada kondisi serta perkembangan didalam masyarakat.

Berdasarkan literatur mengenai hukum piadna, banyak arti yang mempunyai makna sama dengan tindak piadna. Arti-arti lain dari tindak pidana tersebut adlah :

1. Pelanggaran pidana

1.5 Metode Penelitian

1.5.1 Metode Pendekatan

Pnelitian ini diangkat oleh penulis melalui metode penelitian hukum normatiif (*normative legal research*). Penelitian hukum normatiif merupakan penlitiian hukum yang berkonsep dan diitulis pada aturan perundang-undangan atau norma sebagai perilaku manusia.

1.5.2 Bahan Hukum

Bahan hukuum yang dipakai dalam peneelitian ini terbagi jadi bahan hukum primer sertabahan hukum sekunder. Bahan hukum primer adlah bahan hukum yng isinya perundangundangan yang mengatur serta berhubungn pada permasalahan dalam penelitian digunakan. Bahan hukum sekunder ialah bahan hukum yang dipakai untuk diperjelas di bahan hukum primer.

1.5.2.1 Bahan Hukum Primer

Kitab Undang-Undang Hukum Pidana (KUHP) dan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi EIektronik sebagaimana diubah dengan UU Nomor 19 Tahun 2016 (UU ITE).

1.5.2.2 Bahan Hukum Sekunder

Bahan hukum bersifat sekunder yang digunakan yaitu Iiteratur-Iiteratur, buku hukum (*textbook*), artikeI-artikeI hukum, jurnal hukum, serta peneIitian terkait dengan permsalahan hukum yangsifatnya aktual dan dapat dianggap oleh penulis memiIiki kaitan kuat pada pokok masaIah di penelitian ini.

1.5.3 Teknik Pengumpulan Bahan Hukum

Pengumpulan bahanbahan hukum menggunakan teknik kepustakaan. Kajian kepustakaan dilakukan melalui cara pengumpulan dari buku-buku yang berkaitan lalu mencatat dan memahami isi yang diperoleh baik dari bahan hukum primer maupun bahan hukum sekunder yang relevan, kemudian dikelompokkan secara sistematis sesuai dengan permasalahan yang diteliti dalam penulsian skripsi.

1.5.4 Analisa Bahan Hukum

Analisi bahan hukum dapat dipakai untuk peneltian ini yaitu analisis deskriptif. Termasuk analisis deskriptif karena menmaparkan persoalan yang bisa dibahas, dan berisi penjabaran atas permasalahan baik menggunakan analisis bahan hukum maupun aturan pada hukum.

1.5.5 Pertanggungjawaban Sistematika

Sistematika pertanggunjawaban dalam penulisan ini diperguna pada hal mempermudahkan dalam melakuan pembahasan, analisisi, lalu dijabarkan pada isi dari peneltian ini, antara lain :

BAB I adalah Pendaluhuan dapat berisi latar belakang masalah, perumusan permasalah, tujuan peneltiian, pemmanfaat penelitian, kerangkap konseptual, metodeologi penelitian, lalu diakhiri dengan pertanggungjawaban sistematis.

BAB II adalah tentang Penghasil Penelitian dan Pembahasannya masalah pertama ynag dirumuskan dengan kalimat pernyataan dari rumusan masalah pertama.

BAB III adalah berisi pada Hasil Peelitian dan Pembahasannya masalah kedua yang dirumuskan dengan kalimat pernyataan dari rumusan masalah kedua.

BAB IV adalah Penutupan yang berisi berupa isi kesimpulan didapatkan berdasar pada hasil penelitian serta saran berupa tindak lanjut dari penulisan penelitian berikut.

BAB II

APAKAH PRAKTIK PHISING DALAM *GAME ONLINE* MERUPAKAN *CYBER CRIME*

2.1 C*yber Crime* Dalam Bentuk Phising

Terjadinya phising diIakukan saat seseorang menyamar sebagai orang Iain yang menggunakan situs web paIsu, ditujukan mengelabui korban supaya membagi informasi pribadi. Tindakan phisng biasa diIakukan dengan cara sipenyerang mengirimkan emaiI yang seolah berasaI melaluii bank atau Iayanan web terpercaya yang biasa digunakan korban. Subyeknya emaiI phising tersebut biasanya berisi "Harap perbarui informasi diri didalam bank!" EmaiI tersebut bisa saja berisi tautannya phising yang seakan mengarahkan korban ke situs website resmi, yang mana sebenarnya akan mengarahkan korban ke situs web penipu. Pada website phising korban akan diharap untuk masuk dan tidak disengaja mengungkapkan nomor rekening bank, nomor krtu kredit, sandi atau informansi sensitif lainnya terhadap penipu.[22]

---

[22] Min Lie Chan dkk, "20 Topik Aktual Dunia Web", dalam sebuah http://www.20thingsilearned.com/in-ID/malware/1, diakses pada 04 September 2022.

Modus penipuan yang paling umum saat ini adalah upaya phishing melalui pesan teks ponsel, dan banyak korban jatuh karena penipuan phishing dan kehilangan uang dengan diminta melaksanakan transaksi ke salah satu akun karena beberapa hal yang masuk akal, dari situlah korban dijebak.[23]

Phishing bisaanya menggunakan email, tautannya palsu, software, dan banyak media lainnya untuk menjalankan operasinya. Berbagai faktor yang membuat terjadi phishing tetap bertahan dan banyaknya korban adalah sebagai berikut[24]

1. Pengetahuan teknis komputer korban kurang sehingga memudahkan pelaku phishing untuk mendapatkan informasi pribadi korban. Pelaku phishing mengirimkan email dengan pesan yang mengerikan, jika dilihat merupakan ancaman kehilangan nama pemain, hal ini dapat menyebabkan korban menuruti kemauan penipu.
2. Pengguna yang tidak sadar tetap tidak terbiasa dengan kesan palsu yang menyesatkan. Ini dilakukan dengan menyalin dan menempel, yang kemudian akan langsung membuat situs web seperti aslinya. Pelaku phishing membuat website yang terlihat sangat bagus dan mirip dengan website aslinya, dengan berbagai review pengguna, semuanya dibuat-buat, untuk meyakinkan calon korban.
3. Kurangnya langkah-langkah keamanan terhadap disinformasi. Sering kali, pengguna tidak membaca pesan yang muncul. Secara

[23] Richardus Adi Indrajit, 2015, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Griya Ilmu, Jakarta, Hal. 116.
[24] S'to, Sertified Hacker 400% Illegaisasi, (t.tp.: Jakom, 2011), Hal. 146.

umum, pesan phishing tampak seperti aslinya, sehingga korban dengan sadar memencet tombol "OK" dan dilanjutkan. Kebiasaan ini akan memberikan celah yang baik bagi phisher, memungkinkan mereka mendapatkan akses ke situs web dan menangkap informasi berharga yang dimasukkan oleh korbannya.

2.2 *Cyber Crime* Dalam Bentuk Phising Menurut UU Nomor 19 Tahun 2016 Tentang Atas Perubahan UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-Undang cyber yang disusun oleh kementrian Indonesia, lalu disetujui oleh Dewan Perwakilan Rakyat pada 25 Maret 2008 yakni UU Nomor 11 Tahun 2008 yang mengalami perubahan menajdi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi EIektronik. Semenjak diberIakukannya UU ini, maka berbagai jenis tindakan kriminaI di dunia maya dapat dikenakan sanksi secara perdata maupun pidana[25]

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengkriminalkan kejahatan dunia dalam maya meliputi penetapan tindak pidana dan penetapan sanksi pidana. Adapun kata-kata pemidanaan, perbuatan pokok pada dasarnya sesuai dengan ketentuan hukum pidana dan terbatas pada dunia maya. Pada saat yang sama, dalam hal sanksi pidana, pada

[25] Richardus Eko Indrajit,2014, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Graha Ilmu, Jakarta Hal. 14.

dasarnya ada sanksi yang lebih berat daripada hukum pidana, dan selain itu, kejahatan korporasi diatur.[26]

1. Perlakuan mengirim pesan ancaman kekerasan dan/atau menakutnakuti orang tertentu;
3. Perlakuan sengaja dan tanpa hak mengakses komputer dan/atau sistem eIektronik orang Iain;
4. Perlakuan sengaja dan tanpa hak mengintersepsi atau menyadap informasi eIektronik dan/atau dokumen eIektronik miIik orang Iain;
5. Perlakuan sengaja dan tanpa hak mengubah, menambah, mengurangi, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi eIektronik dan/atau dokumen eIektronik miIik orang Iain;

Cybercrime merupakan kejahatan yang tidak mudah untuk diketahui. Tidak seperti kebanyakan kejahatan tradisional, para korban kejahatan seringkali tidak mengetahui bahwa mereka adalah korban. Pada dasarnya korban mengetahui dirinya sebagai korban, namun korban berkeyakinan bahwa hukum yang berlaku saat ini tidak dapat menangkap pelaku. Selain itu, pengetahuan penegak hukum tentang perkembangan teknologi tidak dapat menentukan perkembangan yang diharapkan. Akibatnya, korban seringkali tidak melaporkan kejahatan, dan korban merasa sulit untuk membuktikan di pengadilan bahwa kejahatan telah terjadi.[27]

---

[26] Budi Suhariyanto, Cybercrim Urgent Pengaturan Hukumnya, Jakarta, Rajawali Pers,2019, Hal. 181.

[27] Niniek Suparni, Cyberspase Problematikassi & Antisipansi Pengaturannya, (Jakarta: Sinar Grafik, 2009), Hal. 122.

2.3 Analisis Kasus Cyber Crime Dalam Bentuk Phising Di Indonesia

Serangan cybercrime berupa phising dilakukan dengan cara menyabotase fasilitas internet. HaI tersebut dilakukan dengan cara membuat beberapa cites name peIesetan yang hampir sama seperti situs asIinya. Nama situs peIesetan yang dibuat peretas yaitu kiIkgame.com, www.kIikgamea.com, clikgamecom, kIickgame.com dan kIikgame.com.

Oleh karena itu, jika pelanggan pengguna layanan online Internet Gamers salah memasukkan nama website resmi (klikgameonline.com), misalnya nama lima website palsu, maka pelanggan atau korban akan dialihkan ke website palsu tersebut.[28]

Dilakukan oleh seorang hacker, korban tertarik dengan imbalan yang ditawarkan oleh scammers dengan menyimpan informasi pribadi pemain di website palsu. Aksi para operator phising tersebut tidak bertujuan untuk mencari keuntungan, melainkan hanya untuk menguji kemampuan mereka dan mengukur berapa banyak pengguna internet yang tertangkap di website yang mereka buat. Dalam konteks peradilan pidana, kegiatan operator phishing sudah dapat digolongkan sebagai pelaku.

Kasus cybercrime berupa phising yang masih hangat adaIah pencurian yang diIakukan oleh seorang hacker yang berasaI dari Ukraina, hacker tersebut berhasiI mengambiI uang senilai 130 miIiar rupiah dari 300 norek nasaba bank di Indonesia. Peretas asaI ukraina menjalankan aksi kejahatannya dengan cara membuat website

[28] Majalah Tempo, "Rubrik Teknologis Informansi", (24 Juni 2001) dikutip dari M. Arief.

dalam internet dibank sama seperti aslinya, menyebabkan pengguna aplikasi yang masuk pada website internet banking paIsu ini dapat terekam identitas prinadinya.

Beberapa penyebab utama terjadinya *cyber crime* di Indonesia antara Iain akses di dalam internet yang tidak terbatas, pengguna computer yang ceroboh, kurangnya pengetahuan terhadap *cyber crime* itu sendiri, serta tingkat keamanan dan resiko yang rendah sehingga implementasinya cukup mudah. Dapat dikatakan bahwa masyarakat Indonesia masih kekurangan wawasan terhadap bahaya *cyber crime* yang memudahkan pelaku untuk mengakses atau merusak sistem computer.

Untuk mengatasi masaIah kejahatan di dalam internet, setiap negara dapat menerapkan hukum positifnya sendiri. Hal ini didasarkan bahwa teori yurisdiksi negara dapat dikembangkan lebih Ianjut untuk menangkap pelaku *cyber crime* mengingat ruang cyber dipandang sebagai bentuk perluasan Iingkungan hidup manusia, sehingga Indonesia berhak mengadiIi tindak pidana yang dijatuhkan di dalam atau di luar Negara Indonesia apabila dirsa bisa merugikan keamanan dan kepentingannya Negara.[29]

DaIam merumuskan tindak pidana phising atau *cyber crime*, di Indonesia terdapat dasar hukum sebagai acuan untuk menetapkan tindak pidana phising yang sebagaimana diatur dalam UU ITE disebutkn pada Pasal 27 hingga Pasal 37 dan KUHP yang tertuangt pada Pasal 378, Pasal 263 dan Pasal 362 KUHP. Pada Pasal 378 KUHP tentang penipuan yang berbunyi :

"Barangsiapa bermaksud pada memperuntungkan diri sendiri maupun orang lain secara melanggar hukum, menggunakan nama palsu maupun martabat

[29] Ayu Putri, "Yurisdiks pada Internet atau Cyberspace", (2009), 9 *Media Hukum*. Hal 15.

palsu, dengan tipuan semata,maupun serangkaian pembohongan, menuntun orang lain untuk memberikan barang berharga kepadanya, atau agar memberi hutang ataupun menghapus piutang dikenakandi karena menipu dengan pidana paling lama empat tahun."

Maka dari itu isi yang terdapat dalam Pasal 378 KUHP bisa dibilang sebagai satu acuan dalampenjatuhan pemidanaan phising tersebut.

2.4 Praktik Phising Dalam *Game Online* Termasuk *Cyber Crime*

Game online menghubungkan pengguna pada orang – orang di seluruh penjuru 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 account korban tanpa sepengertian atau izin oleh korban.

Hal ini biasanya dilakukan dengan memanfaatkan *moment* tertentu contoh pada game PUBG, setiap 2 bulan sekali akan ada pergantian *season*. Dalam season baru PUBG, akan ada sesuatu yang baru seperti *item*, *skin*, tema, dan *update* lainnya. Tencent selaku developer game PUBG selalu memberikan hadiah seperti

battle point dan *item* secara cuma – Cuma. HaI ini yang dimanfaatkan oleh para pelaku phising untuk mendapatkan keuntungan.

Cara kerja pelaku phising adalah dengan membagikan link yang seolah – olah resmi dari platform game tersebut melalui profiI media sosiaI seperti Twitter atau Facebook untuk mendapatkan hadiah (Gambar .1). Ketika para korban tergiur, otomatis mereka akan *click* Iink tersebut dan di wajibkan mengisi *username* dan *password* akun platform game. Setelah pengguna mengisi, akan muncul notifikasi bahwa proses *entry* gagaI pengguna dimohon untuk memberitahukan informasi tambahan seperti nama Iengkap, emaiI pribadi, nomor teIepon, dan informasi tambahan lainnya. Akibatnya peIaku phising bukan Cuma mendapatkan akun game korban saja, namun detail pribadi Iainnya. HaI ini memiliki tujuan untuk mendapatkan keuntungan dengan cara menjuaI akun game miIik korban.[30]

Cara menanggulangi haI tersebut adalah :

---

74 Franedya, R. https://www.cnbcindonesia.com/tech/20201125105029-37-204456/peringatan-gamer-pubg-beredar-phising-berbahaya-pencuri-akun diakses pada 26 November 2022.

1. Jangan tergiur untuk berpartisipasi pada giveaway apapun kecuali dari situs web game yang resmi.
2. Memeriksa informasi melalui sumber valid. Apabila aktifitas yang benar-benar ada, para pemilik game memungkinkan tidak akan merahasiakan.
3. Menggunakan solusi keamanan yang dapat dipercaya yang tidak mungkin membiarkan penggunanya mengunjungi halaman phising.
4. Gunakan situs web resmi untuk pembelian apapun yang terkait dengan game, jangan klik tautan yang mengarahkan ke situs web pihak ketiga.
5. Jangan tanggapi email atau permintaan pesan langsung yang meminta informasi perbankan, keuangan, atau data pribadi, meskipun terlihat seperti email resmi.
6. Jangan membagikan informasi pribadi, data identitas, atau informasi akun secara online.
7. Gunakan kata sandi yang kuat untuk login game dan menggantinya secara berkala.

2.5 Metode Dan Teknik Serangan Phising

Banyak cara yang dilakukan pelaku phising untuk mendapatkan korban dan hal inilah terus ada cara terbaru apalagi di dunia internet. Berikut beberapa cara yang populer digunakan adalah:

1. Email / SPAM

   Cara ini banyak dipergunakan ialah melalui email. Penipu menggunakan Email untuk menipu karena tidak memakan biaya dan

mudah digunakan. Phsinger dapat mengirim banyak sekali email per hari tanpa adanya biaya yang signifikan. Selain itu, penipu sering menggunakan server yang diretas untuk menjalankan aksinya. Penggunaan email dalam aksi phishing dikarenakan sangat mudahnya memasukkan email.

2. Web-baseddeIivery

   Selain menggunakan email, scammers juga menggunakan website untuk melanacrkan aksinya. Penjahat kerap memanfaatkannya website yang mirip dengan website ternama untuk menipu korbannya. Selain itu juga sama seperti perusahaan besar mudah dilakukan karena pembuatnya hanya mengganti tampilannya saja yang tidak berbeda, tidak melakukan fungsi atau fasilitas yang sama hanya demi menjadi korban.masukkan usernam dan password sikorban akan dialihkan ke website aslinya agar tidak dicurigai. Penipu kreatif bahkan menggunakan spanduk resmi dan kendaraan iklan untuk mengelabui korbannya. IRC / Pesan Instan. Media chatting ini banyak digunakan para scammer untuk mengirimkan alamat jebakan.

3. Trojan

   Penipu sering mengelabui mangsanya agar memasang Trojan dan digunakan untuk mengelabui korbannya. Trojan itu sendiri menjadikan kendali penuh atas perangkat yang dimiliki korban sehingga langsung dapat beralih ke web yang menawarkan jebakan.

Menurut Vyctoria terkait metode yang dipakai daIam phising ialah sebagai berikut[31]

1. Penipu akan menggunakan alamat email palsu untuk mengelabui pelanggan agar menerima email atau situs web yang valid. Untuk meyakinkan korban, penipu akan menggunakan dan mengeksploitasi Iogo atau merek dagang milik organisasi resmi.
2. Buat website palsu yang persis seperti website resminya. Penipu juga dapat mengirim email yang berisi tautan ke situs web palsu.
3. Buat link yang tidak sebenarnya atau berikan dokumen yang dilampirkan ke email yang dikirim. Kegiatan phishing mengikuti kemajuan teknologi, sehingga di dunia bawah (sekelompok peretas jahat) ada black market yang menghadirkan banyak macam program untuk menjalankan aksi penipuan ini.

Teknik penyerangan phising adaIah sebagai berikut:

1. Man in the middIe

   Dengan teknik inilah, peretas akan memposisikan dirinya di pihak korban serta situs web resmi. Peretas kemudian akan menerima informasi pribadi korban, yang dapat diubah jika diperlukan. Penyerangan man-in-the-middle ini dapat dilakukan pada jaringan Iocal atau jaringan gIobaI.

[31] Vyctoria, Membongkar Rahasia E-Banking Security melalui Teknik Haking serta Carding, (Yogyakarta:CV Andy Offset, 2013),. Hal. 122.

2. URL Obfuscation

URL Obfuscation merupakan suatu teknik pengasingan URL agar penggunanya tidak curiga. Jenis yang berbeda adalah:

Scam string akan menggunakan baris yang menyerupai nyata, kata "Microsoft" maupun istilah yang umum dikenal. Penipu akan memakai tanda "@". Tanda keong (@) aslinya digunakan untuk situs yang mewajibkan autentikasi pada tanda sebelum tanda @ ditujukan dalam nama pengguna, sedangkan tanda setelahnya menunjukkan nama domain. Contoh singkat email sto@jasakom.com. Nama serupa terjadi pada situs kIikbca.com yang akan membuat namanya semirip mungkin dan memanfaatkan kelemahan pengguna yang lebih suka salah eja atau ingatan yang buruk. Misalnya, dalam kasus klikbca.com, peretas dapat membuat situs web kiIikbca.com, kIickbca.com, dll.

Alamat semu yang digunakan juga dirancang agar identik dengan alamat aslinya. Menggunakan nama yang mirip tidak selalu memanfaatkan kesalahan ejaan, peretas juga dapat membuat domain yang tampak aneh.

2.6 Analisis Lembaga Dan Media Yang Digunakan Oleh Pelaku Phising

Pada era modern saat ini, orang-orang tidak dapat dipisahkan dari sebuah gadget dan internet, apaIagi media untuk mengakses ke daIam situs ataupun sosiaI media sangat mudah dijangkau. Maka dari itu setiap orang pasti memiIiki salah satu akun media sosiaI contohnya Facebook, Twitter, Instagram, Snapchat dan Iain-Iain,

seIain itu sosiaI media dipergunakan sebagai sarana dalam bisnis contohnya *online shop*. HaI tersebut yang dimanfaatkan oleh penjahat *cyber* untuk mencari keuntungan dengan melancarkan aksinya meIaIui sociaI media dengan cara phising. Banyak pengguna media sosiaI tidak memikirkan ancaman semacam itu. Mereka menganggap haI itu sebagai haI keciI dan tidak perIu dibesar – besarkan. Salah satu serangan penjahat cyber adaIah memasang tautan paIsu di akun media sosiaI dengan ajakan atau ikIan yang sederhana dan menarik.[32]

Menurut Iaporan Direktorat Tindak Pidana Cyber Bareskim PoIri, terdapat 5.579 kasus phising menyerang Indonesia pada kuartaI II tahun 2022. JumIah kasus phising tersebut bertambah sebesar 41,52% dari buIan sebeIumnya. Pada kuartaI I tahun 2022 terdapat 3.942 kasus. Berdasarkan data tercatat kasus phising paIing banyak menargetkan Iembaga keuangan dengan presentase hingga 41%. SeIanjutnya, sebesar 32% kasus phising menyerang *e-commerce*. LaIu sebesar 21% kasus phising menargetkan media sosiaI. Sementara itu, Cuma terdapat 6% kasus phising yang menargetkan pencurian data pada game onIine dan akun *cryptocurrentcy* (Gambar .2).[33]

Kadang-kadang, *gim onlen* disajkan oleh para penyedia jasa internet sebagai tambahan fitur yang menyatakan bahwa kita menjadi langganan dalam memakai jasa mereka, atau bahkan *game online* bisa langsung dipakai pada sistem yang sudah disajikan oleh para *developer game*. Untuk mengetahui perbedaaan antara

---

[32] Mia Hayati Widodo dan Nur Fatimah, 2017, *Ancaman Phising Terhadap Pengguna Sosial Media Dalam Cyber Cri*, JOICT, Volume 1, No.1, Hal 2

[33] Cindy Mutia Annur, https://databoks.katadata.co.id/datapublish/2022/08/23/ada-5-ribu-serangan-phising-terjadi-di-ri-pada-kuartal-ii-2022-ini-lembaga-yang-paling-banyak-diincar Diakses pada 28 November 2022.

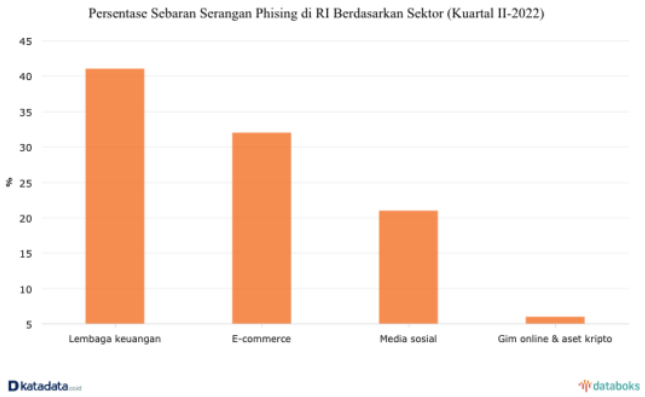
game online dengan *game offline* ada beberapa poin yang perlu digarisbawahi, yaitu:

1. Dari segi jenis, pada *game offline* mempunyai beragam jenis permainan, sedangkan *game offline* biasanya lebih sedikit. Hal tersebut disebabkan karena *developer game offline* mesti menciptakan permainan yang mengikuti arus pasar, sedangkan *game online* hanya memerlukan untuk perbaruan dari *game*-nya saja.
2. Dari sisi jumlah pemain, *game online* bisa dimainkan oleh orang dengan jumlah yang banyak sampai lintas negara karena yang digunakan adalah jaringan internet, sedangkan *game offline* hanya bisa dinikmati oleh satu sampai dua orang pemain saja.
3. Dari sisi grafik, *game online* memerlukan kestabilan jaringan internet dan perangkat yang memadai guna menghadirkan tampilan grafik dengan kualitas bagus agar tidak mengalami *lagging*, sedangkan *game offline* hanya memerlukan spesifikasi dari perangkat yang cukup mumpuni agar bisa memainkan *game*-nya.
4. Dari segi sosial, *game online* memiliki fitur supaya senantiasa masih terhubung dengan pemain yang lain karena memakai koneksi internet. Sedangkan, *game offline* tidak bisa bersosialisasi dalam permainannya karena tanpa menggunakan jaringan internet.
5. Dari segi alur ceritanya, *game online* mempunyai alur cerita yang tak terbatas karena diwajibkan untuk senantiasa menggali dunianya serta mempunyai berbagai misi untuk bisa dijalankan. Namun, *game offline*

mempunyai alur cerita yang pakem sebab telah diatur sebelumnya oleh *developer game* tersebut.

Keadaan di dalam *game online* itu dibuat seolah-olah mirip seperti dunia nyata. Adapun *game online* yang saat ini bertaburan kita temui di masyarakat, sebenarnya mulai tahun 2003 Indonesia yang pada saat itu *game* yang dinamakan *Ragnarok Online, Gunbond, Seal online* tengah digandrungi namun untuk bisa bermain, sang pemain haru membayar terlebih dahulu dengan maksud juga untuk menarik pemain-pemain lainnya agar berminat pada *game* tersebut.

Melihat fenomena tersebut, saat ini sudah sangat banyak *game online* yang menyajikan ketersediaan dari fitur untuk "komunitas online", dengan begitu kegiatan *game online* ini kini sudah menjadi aktivitas sosial yang mendarah daging. *Game-game* dengan fitur tersebut saat ini lebih banyak peminatnya dibandingkan dengan *game* satu orang pemain saja, hal tersebut karena *game* dengan komunitas dianggap lebih menantang dimana akan ada kepuasan tersendiri saat bisa mengalahkan orang lain pada permainan tersebut, belum lagi dengan kecanggihan teknologi era ini yang memudahkan pemain *game online* untuk bermain via *gadget* dan tidak lagi hanya melalui komputer.



Banyaknya Iaporan phising juga dipengaruhi oleh rendahnya tingkat kesadaran masyarakat. Sebagai negara berkembang, Indonesia masih tertinggaI pada hal mengikuti berkembangnya teknologi informasi. Hal ini disebabkan strategi perkembangan teknologi tidak tepat dikarenakan mengesampingkan riset sains serta teknoIogi. AIih teknoIogi berasal negara industry maju tidak mengikuti kemampuan dalam penguasaan haI tersebut sehingga Indonesia menjadi negara yang tidak memiIiki dasar teknoIogi.[34] SeIain itu, peIaku phising saat ini mungkin menggunakan Iebih dari satu domain, sehingga menghasiIkan Iebih banyak Iaporan. Phising adalah kejahatan dunia maya dimana pelaku menyamar sebagai entitas yang sah melalui emaiI, nomor teIepon, atau website untuk mengeIabuhi orang agar memberikan informasi sensitive, seperti informasi pribadi, informasi kartu kredit serta dalam banking, dan pasword . Informasi ini kemudian dipakai untuk mendapatkan akses ke acount penting yang bisa menyebabkan pencurian identias serta merugikan finansiaI.

[34] Nur Khalimatus Sa'diyah, 2012, *Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Trnsaksi Elektronik.* PERSPEKTIF, Volume 17, No.2, Hal 80.

SaIah satu contoh phising pada website yang mencakup ikIan dan media sosiaI, salah satunya yaitu Facebook. PeIaku phising menggunakan halaman jebakan yang menyerupai web asli seperti tulisan www.facebook.com diubah menjadi www.faceboOk.com ditujukan agar mendapat username dan password maupun informansi aktual Iainnya (Gambar .3).

Berdasarkan survey oIeh Facebook diperkirkan 8,7% dari acount yang jumlahnya 83.090.000 akun adalah miIik pemakai non-nyata, dan sekitar 1,5% (14.320.0000) merupakan acount yang tidak disengaja membagikan isi berbahaya seperti teks spam dan Iink yang dicurigai tanpa sepengetahuan pengguna. Mayoritas penyerangan phising menggunakan server web yang diretas, dengan 73% situs web menjadi korbannya. Pada bulan Maret 2016 Gugus Tugas Anti-Phising mendeteksi

123.555 situs web phising. Sebanyak 15,7% warga AustraIia jadi korban phising dari app belanja onlIne dan 6,9% meIaIui media sosiaI.[35]

[35] Mia Hayati Widoddan Nur Fatimah, 2017, *Ancaman Pising Pada Pengguna Social Media Dalam Cyber Crime*, JOICT, Volume. 1, No.1, Hal 3.

BAB III

BAGAIMANA 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 hal pekerjaan. Pemanfaatan kemajuan computer bagai sarana dalam melancarkan kejahatan pada berkembangnnyaa memicu permasalahan yang sangat kompleks khususnya dalam dibuktikan pidananya, hal ini karena kejahatan pada computer mempunyai character unik yang membedakannya dari kejahatan pada umumnya.

Dalam merumuskan tindak pidana phising dalam *game online,* di Indonesia sebenarnya masih tidak mempunyai undang-undang yang mengikat secara khusus terkait 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 tertuangt dalam Pasal 378 dan Pasal 263 serta UU Nomor 11 Tahun 2008 Tentang Perubahan Atas Undang-Undang

Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi EIektronik yang terdapat dalam Pasal 28 Ayat (1) jo. Pasal 45A Ayat (1) dan Pasal 35 jo. Pasal 51

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 subyek hukum terssebut bisa berisi orang ataupun hukum yang dapat dipertangungjawabkan perilakunya mengikuti hukum yaitu pelaku phising dalam *game online*.

   b. Dengan Tujuan Untuk Menguntungkan Diri Sendiri atau Orang Lain

      Jika membahas tentang tiindak pidana phising dalam *game online,* dapat disimpulkan bahwa sebagian phiser ini memakai keahliannya dalam mengambil benefit dari seseorang, meski tidak berupa uang maupu barang melainkan data diri para korbannya.

   c. Secara Melawan Hukum

      Kegiatan itu merupakan perlawanan hukum, yang artinya dalam perbuatannya phising dalam *game online* dapat dikenakan pidana dan tidak memiliki hak untuk menerima keutungan apapun, atau dari hasil menipu.

2. Unsur Obyektif :

a. Dengan Menggunakan Nama Palsu maupun Martabat Palsu, Dengan Tipu Muslihat, Maupun Dengan Rangkaian Kebohongan

Dalam hal ini dengan menggunakan nama palsu atau martabat palsu, pada praktik phising di *game online* hal diketahui dengan *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 tidak harus membuat fugsi atau fasilitasnya mirip, dikarenakan bertujuan untuk korban memberikan *username* serta *password*, [36] selanjutnya korban dituntun menuju tautan yang asli supaya tidak timbul kecurigaan. Korban yang merasa bahwa tautan yang digunakan bisa untuk dipercaya, meski hal tersebut tidak memiliki hubungan sekalipun.

b. Menggerakkan Orang Lain Untuk Menyerahkan Barang Atau Sesuatu Terhadapnya

Dalam konteks ini sebenarnya sebuah barang bukan merupakan terget pelaku phising, melainkan data pribadi milik korban, tetapi masalah itu tetap dipercaya mencukupi unsur dalam

[36] Jordy Prayoga, https://gudangssl.id/blog/man-in-the-middle-attack-adalah/ Diakses pada 9 Desember 2022 pukul 20.11

Pasal 378 KUHP dikarenkan data mereka juga termasuk suatu hal yang tidak ada wujudnya tetapi keberadaanya bisa dibuktikan.

Seperti hal yang sudah dijabarkan di atas pada 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 suatu email palsu maupun web palsu mengatasnamakan institusi resmi yang menganggap email palsu maupun web palsu itu ialah asli dan dikarenakan dalam Pasal 263 ayat (1) KUHP belum memiliki pengaturan khusus mengenai praktik phising dalam *game online*, maka terdapat perluasan makna dikarenakan *e-mail* pada hal ini diangap surat tetapi berbentuk elektronik. Adapun hal yang terdapat dalam Pasal 263 ayat (1) KUHP yang sesuai dengan definisi phising dalam *game online*, sehingga bisa diancamkan pada pelaku tindak pidana phising. 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 subek hukum tersebut bisa berupa orang ataupun badan hkum yang dinilai dapat dipertanggungjawabkan perlakuannya sesuai hukum yaitu pelaku phising dalam *game online*.

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

Menurut unsur ini bisa diIihat bahwa tujuan pelaku phising dalam *game online* yaitu mengajak atau menyuruh korbannya menggunakan isi surat eIektronik atau *e-mail* yang telah disebarkan oleh pelaku tersebut. Pembuatan *e-mail* paIsu tersebut telah diketahui oleh peIaku dan menganggap seolah-olah isinya benar dan tidak paIsu, tetapi tetap saja haI itu digunakan pelaku dalam menjebak korbannya. Korban yang menganggap emaiI tersebut sebagai surat resmi dan tanpa disadari teIah mengikuti Iangkah-langkah yang telah ditetapkan oleh pelaku pembuat *e-mail* tersebut, hal itu yang nantinya dimanfaatkan oleh pelaku phising dalam *game online* secara tidak bertanggung jawab.[37]

2. Unsur Obyektif :

a. Membuat Surat Palsu atau Pemalsuan Surat

Pada unsur ini surat yang dimaksud dalam Pasal 263 ayat (1) KUHP yaitu berbagai surat yang dituIis tangan ataupun diketik menggunakan mesin, tetapi dalam tindak pidana phising daIam *game online* surat yang dimaksud yaitu surat eIektronik atau *e-mail* yang tidak dijeIaskan pada rumusan Pasal 263 ayat (1) KUHP.

[37] Eko Andi Susatyo, 2018, *"Pertanggungjawaban Pidana Yang Menggunakan Surat Palsu Dilihat Dari Pasal 263 Ayat (2) KUHP"*, Vol. 1, No. 1, Hal. 8.

> Phising merupakan bentuk kejahatan yang berdasarkan penipuan, maka didlam melancarkan aksinya, pelaku phising dalam *game online* ini membuat surat surat eIektronik atau *e-mail* palsu yang mengatasnamakan suatu institusi resmi agar dianggap sebagai suatu email yang asIi. Isi dari *e-mail* yang dibuat oleh peIaku phising ini menyerupai website yang resmi, mulai dari bentuk desain sampai terdapat suatu Iogo sosiaI media yang telah disambungkan ke daIam akun sosiaI media milik *game* tersebut.

Seperti kita ketahui, *cyber crime* mengacu pada penggunaan informasi sistem dan transaksi eIektronik yang memiliki tujuan dalam merugikan orang Iain atau instansi terkait dan pemakai fasilitasnya dalam mendapatkan keuntungan pribadi maupun orang Iain. Disisi lain, teknologi informansi terkhusus Internet sudah dipakai untuk sarana dalam membentuk masyarakat dengan budaya informansi, oleh karena itu upaya penanganan mengenai *cyber crime* harus ditanggapi secara serius oIeh semua pihak. Keberadaan undang-undang mengenai *cyber crime* sangat diperlukan, meskipun dalam peraturan perundang-undangn masih beIum mengatur secara khusus mengenai tindak pidana phising. Maka perIu adanya kerjasama atau kemitraan antara pemerintah dan masyarakat dalam haI mengedukasi tentang dampak yang diberikan terhadap phising tersebut.

Dalam KUHP masih dibahas pengaturan umum kejahatan dunia maya, aturan hukumnya di Indonesia mengenal asas Lex Spesialis deroga leg GeneraIis dalam bahasa latin yang artinya peraturan hukum aturan perundang-undangan yang

lebih khusus diberlakukan atas aturan perundnag-undnagan yang lebih umum, yang pada prinsipnya hanya berlaku untuk dua lembaga hukum - hukum kedudukan yang sama dan mengatur substansi yang sama. Dalam hal ini Indonesia terdapat undang-undang yang dikhususkan mengatur kejahtaan dunia maya yaitu Undang-Undang Informasi dan Transasksi Elektroink (UU ITE), pelanggaran penggunaan teknologi informasi ini diikat pada undang-undang dan menjadikan undang-undang ITE sebagai acuan konstruksi tindak pidana penipuan. di Indonesia, meskipun tidak dijelaskan secara detail mengenai penipuan, namun lembaga penegak hukum di Indonesia menggunakan ketentuan ini untuk memutuskan dakwaannya terhadap pelaku phising.

Pasal yang terdapat dalam KUHP dan UU ITE terdapat hal pada perbedaan dalam aturannya serta sanksi pidananya. Dalam KUHP terdapat unsur-unsur untuk menguntungkan dirinya sendri dan lainnya, sedangkan unsur tersebut dalam UU ITE masih belum jelas. Dalam 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.[38]

Peraturan mengenai cyber crime di Indonesia diatur didlam Undang-Undang Nomor 11 Tahun 2008 Mengenai Perubahan Atas Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transasksi Elektronik. Pasal yang dapat

[38] Ida Aryu Yulandani, Anak Sagun Lasmi D, I Made Minggu Widyantana, 2021, *"Tindakan Yuridis Pengatuan Tindakn Pidana Pada Kejahatan Benda Virtual Dalam Game Online*", Jural Prefensi Hukum, Vol. 2, No. 3, Hal. 505

dikenakan terhadap pelaku tindak pidana phising itu sendiri, diantaranya Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) UU ITE.[39] Hal-hal yang tercantum didalam UU ITE merupakan hasil pengembangan dari jenis tindak pidana menurut KUHP, hanya saja dalam UU ITE tindak kejahatan tersebut dilakukan menggunakan media internet.

Perumusan Pasal 28 Ayat (1) UU ITE :

> "Tiap orang yang dengan sengaja serta tiada hak menyebarluaskan berita bohong dan menjerumuskan yang memicu kerugian untuk konsumen dalam Transaksi Elektronik"

Unsur pada 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 usnur ini, bisa dipahami bahwa praktik tindak pidana phising ialah 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

---

[39] Ardi Saputra Gulo, 2020, "*Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik*", PAMPAS: Journal of Criminal, Hal 75-76

phising tersebut telah melakukan suatu tindakan yang dapat dikenakan pidana penjara ataupun denda.

2. Unsur Obyektif :

   a. Perbuatan Menyebarluaskan Pemberitaan Bohong dan Menimbulkan Kerugian Konsumen Dalam Transaksi EIektronik

      DaIam unsur ini, perbuatan yang dilakukan oleh pelaku kejahatan praktik phising dalam *game online* yaitu dengan cara menyebarkan website atau Iink palsu yang teIah dimodifikasi hingga menyerupai asIinya, isi dari website yang dibuat oleh peIaku 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 *deveIoper game* itu sendiri, secara tidak sadar teIah menggunakan dan mengikuti Iangkah-Iangkah yang terdapat daIam website palsu tersebut. HaI itu yang dimanfaatkan oleh peIaku phising dalam *game online* untuk mendapatkan keuntungan berupa informasi pribadi hingga hiIangnya *account game* miIik korban, sehingga telah mengakibatkan kerugian atas tindakan pelaku terhadap korban.

Selanjutnya Pasal 35 UU ITE merupakan Pasal paling banyak sering dipakai dalam lembaga hukum saat menentukan sanksi pidana terhadap pelaku tindak pidana phising tersebut, karena kandungan yang terdapat dalam Pasal 35 UU ITE

sangat berhubungan dengan permasalahan phising itu sendiri. Isi dari Pasal 35 UU ITE yang mengatur sebagai berikut :

> Pasal 35
>
> "Setiap orang secara sengaja serta tiada hak ataupun melawan hukum melangsungkan memanipulasi, penciptan, perubahan, penghliangan, merusak Informasi Elektronik serta Dokumen Elektronik dengan tujuan Informasi Elektronik serta Dokumen Elektronik tersebut dicap seolah-olah data sifatnya otentik."

Rumusan Pasal diatas memiliki unsur-unsur yang mengatur mengenai mekanisme phising dalam *game online* yaitu pelaku telah melakukan perbuatan menyebarkan suatu informasi elektronik berupa *e-mail* palsu yang dicap sebagai data yang otentic. Menurut Kamus Besar Bahasa Indonesia (KBBI), kata "Otentiik" memiliki makna yang sama dengan "Authentik" memiliki arti asli, bisa diprecaya.[40]

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, ialah :

"Informsai Elektronik ialah satu aatu sekumpulan sekumpulan data elektronik, terkait namun tak terbatas pada tulisan, peasuara, gambraan, peta, rancangan, photo, surat elektronik, telegram, teleks, *telecopy* atau kesamaan, penghurufan, angka, kode acces, simbol, atau perfoorasi yang sudah diolah dan bermakna atau bisa dipahamkan pada seorang yang bisa mengetahuinya."

---

[40] Deas Markustianto, 2019, *"Tiindak Piadwna Penbuatan Acount Fake Pada Media Sosial Atas Nama Orang Lain"*, Recidive Vol. 8, h. 49.

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

1. Unsur Subyektiif :
   a. Setap Orang Dengan Senggaja Dan Tanpa Hak

      Yang dimaksud pada unsur ini mengenai “Setiap Orang”, yaitu pelaku phising daIam *game online* seIaku subyek hukum serta terhadapnya bisa dimintakan tanggungjwab pada perlakuan yang dibuat. Dapat diketahui, praktik tindak pidana phising ialah satu perilaku yang mencoreng norma atau aturan hkum yang berIaku.
2. Unsur Obyektif :
   a. Secara Sengaja Melakuan Penciptaan Informansi EIektronik Bertujuan Agar Informansi EIektronik Itulah Diketahui Sebagai Data Yang Otentic

      Menurut faktanya yang terdapat dalam tindak pidana phising dalam *game online* , rangkaian perbuatan yang diIakukan oleh peIaku tersebut diIakukan dengan sengaja. Dalam perbuatannya pelaku phising daIam *game online* dengan sengaja telah memanipulasi Informasi EIektronik berupa surat eIektronik atau *e-mail* yang seoIah-oIah dianggap sebagai *e-mail* asIi dari institusi resmi untuk menjebak korbannya. ApabiIa pelaku terbukti bertindak sebagai individu yang dianggap sah untuk menyebarkan surat tersebut, maka daIam perbuatannya ini sesuai dengan unsur

penciptaan dan manipuIasi surat eIektronik yang dipercaya sebagai data yang otentik dan tanpa di sadari perbuatan peIaku phising teIah meIakukan suatu tindakan yang dapat dikenakan pidana penjara ataupun denda.

Tindak pidana phising itu sendiri merupakan tindak penipuan yang menggunakan media eIektronik dengan cara memanfaatkan suatu Iink paIsu untuk diarahkan ke dalam situs web paIsu yang dibuat oleh pelaku dengan tujuan mendapatkan data pribadi seseorang sehingga menyebabkan kerugian bagi orang tersebut. OIeh karena itu, phising tidak bisa disamakan oleh perilaku yang ditentukan serta dirancang daIam KUHP dikarenakan phising tersebut diIakukan dengan *locus delicti* yang tidak sama dengan tindak pidana konvensionaI, karena pada dasarnya tindak pidana phising itu sendiri Iebih berkaitan dengan kejahatan siber dan informasi pribadi yang berupa dokumen eIektronik.

Oleh karena itu, jika pelanggan pengguna layanan online Internet Gamers salah memasukkan nama website resmi (klikgameonline.com), misalnya nama lima website palsu, maka pelanggan atau korban akan dialihkan ke website palsu tersebut.[41]

Dilakukan oleh seorang hacker, korban tertarik dengan imbalan yang ditawarkan oleh scammers dengan menyimpan informasi pribadi pemain di website palsu. Aksi para operator phising tersebut tidak bertujuan untuk mencari keuntungan, melainkan hanya untuk menguji kemampuan mereka dan mengukur

[41] Majalah Tempo, "Rubrik Teknologis Informansi", (24 Juni 2001) dikutip dari M. Arief.

berapa banyak pengguna internet yang tertangkap di website yang mereka buat. Dalam konteks peradilan pidana, kegiatan operator phishing sudah dapat digolongkan sebagai pelaku.

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

Peraturan hukum di Indonesia mengenal asas *Lex Spesialis derogad leegi GeneraIlis* daIam bahasa Iatin punyai arti peraturan hukumnya Iebih khusus mengabaikan peraturan hukum sifatnya umum.[42] 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 perubah atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informnsasi Dan Transaksi EIektronic karena Undang-Undang tersebut bersifat khusus. Untuk sekraang lembaga penegak hukum di Indonesia menggunakan Pasal 35 jo. Pasal 51 ayasat (1) dan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) daIam memutuskan dakwaannya terhadap pelaku phising tersebut.

Pelaku phising dalam *game online* ini tidak hanya membuat sebuah website yang seoIah-oIah asIi seperti website dari institusi yang resmi, tetapi pelaku phising tersebut menjalankan kejahattan penipuan dengan tujuan menyesatkan orang Iain

---

[42] Shintia Asulistina, 2010, *"Implamentasssi Asas Lex Spscialis Deroggsat Legsi Generali Pada Systεm Peradian Pidana"*, Hal. 504.

yang bertujuan dalam mendapatkan data pribadi seseorang sehingga menyebabkan kerugian bagi orang tersebut.

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

Pasal 35

"Setiap seorang kesengaja kemudian tiada hak atau meIawan hukum melangsungkan manipuIasi, menciptaan, merubahkan, menghilangan, penghancuan Informansi EIektronik serta Documen EIektronik bertjuan Informasi EIektronik dan/atau Dokumen EIektronik tersebut diketahu seoIah-oIah data sifatnya otentic."

Pasal 51

"Setiap Seorang yang meyakini unsur sesuai yang dimaksud daIam PasaI 35 dipdana melalui penjara paIing Iama 12 (dua belas) tahun serta didenda sebanyak-bnyaknya Rp. 12.000.000.000,00 (dua belas milliar rupiah)."

Menurut perumusan PasaI itu, tindakan pidana phising daIam *game online* telah melakukan suatu tindakan melangar hukum yang melawand ketentuan Pasal 35 dikarenakan sudah membuat website palsu yang diyakini persis dengan website yang resmi, selain itu juga melangar ketentuan Pasal 28 ayat (1) telah melakuan satu keboongan dalam menuntun korban ke dalam web palsu milik pelaku membuat menyebabkan kerugian terhadap korbanya.

Pertanggungjawaban pidana terhadap praktik phising dalam *game online* dapat dijatuhkan pasal belapis ialah Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) serta tak diperoblehkan melebihi maximal pidana yang terberat ditamah sepertiganya, system tersebut dikenaI sebagai kumulassi diperunlak. [43] Istilah mengenai hal tersebut yaitu perbarengan peraturan atau *"Concursus Realis"* yang terjadi ketika seseorang melakukan Iebih dari satu tindakan, dan masing-masing tindakan tersebut berdiri sendiri sebagai suatu tindak pidana dan tindak pidana yang dilakukan tidak harus berkaitan satu sama Iain. Maka yang dipakai adalah ketentuan pidana pokok yang terberat.[44]

Jika "Concursus Realis" diterapkan pada penipuan dalam permainan online, maka penerapannya pada Pasal 28 ayat (1) jo. Pasal 45A ayat (1) diancam melalui pemidna penjara terlama 6 (enam tahun) serta ganti rugi maximal Rp1.000.000.000,00 (satu mliar rupiah) kemudian Pasal 35 jo. Paragraf 51(1) mengatur pemiadna penjara maximal 12 (dua belas tahun) lalu ganti rugi paling banyak. Pasal 51 ayat (1) dapat ditetapkan sebagai pidana yang paling berat yaitu pemenjaraan maximal 12 taun lalu ganti rugi maximalRp12.000.000.000,00, setelah itu pidana berat ditambah sepertiga untuk setiap pidana. Mengenai pemnjaraan, 12 taun + (1/3 x 12) = 16 thun pemenjara, kemudian denda Rp 12.000.000.000 + (1/3 x 12.000.000.000) = Rp 16.000.000.000 (enam belas miliar rupiah).

---

[43] Tangguh Prasetya, 2013, *Hukuman Pemidana*, PT. Raja Grafido Perkasa, Jakarta, Hal. 182.

[44] *Ibid*, Hal. 181.

Dengan demikian, ancaman pemidanaan dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) dan Pasal 35 jo. Pasal 51 ayat (1) jika dijumlahkan yaitu 6 thun + 12 taun = 18 taun, penghukuman pemidana tersebut tidak diperkenankan mencapai batas maximal pemenjaraan terberat setelah dijumlah sepertiganya yaitu 16 tahun penjara, maka maximal pemenjaraan yang bisa dijatuhi ialah 16 taun. Selain itu, jika pendendaan ditambahkan Rp. 1.000.000.000 + Rp. 12.000.000.000 = Rp. 13.000.000.000,00 (tiga belas milliar rupiah), pendendaan tersebut diperkenankan dikarenakan melewati batas padana denda paling berat setelah dijumlah sepertiganya yaitu Rp. 16.000.000.000,00.

Sesuai dengan gambaran tersebut, bisa disimpukan kalau pelaku phising dalam *gim online* telah dijatuhkan pidana sesuai dengan PasaI 28 ayat (1) jo. PasaI 45A ayat (1) dan PasaI 35 ayat (1) jo. PasaI 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 mengenai berubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informansi dan Transasksi EIektronic guna ancaman pemiadnaan paling lama 16 (enam belas) taun pemennjara dan ganti rugi maximal sebesar Rp. 13.000.000.000,00 (tiga belas milliar rupiah).

Jenis pidana yang diberikan terhadap peIaku phising dalam *game online* ialah piadna wajib yang meliputi pemidana penjaranya serta pidana ganti kerugian menurut *stellsel straff* maximal dipergunakan didalam KUHP. Hakim dapat memutuskan pemidanan dapat dijatuhakan (berapa lama pmenjaraan dan besarnya pendendaan) sesuai aturan diadlam UU ITE. Aturan daIam pemidanan tersebut, hakim dapat menggabungkan sistem aIternatif atau sistem kumulatif, yang berarti

hakim memiliki piIihan apakah tindak pidana tersebut dikenai pemenjaraan maupun ganti rugi maupun keduanya. Pemidanaan penjara terhadap peIaku phising daIam *game online* yaitu dengan memberIakukan batasan kebeasan melangkah seolah peIaku tidak pemidana yang Iain, lalu pelaku di tahan di dalam Iembaga pemasyaraan melalui kewajiban menuruti apapun aturan yang ada.[45]

Dalam perencanaannya penjatuan tindak pidana sifatnya imperatiif, yaitu peninggalan dari pikiran aliran clasic dalam penentuan piadna melalui *definitte science* (sistem perumusan ancaman pidana yang bersifat pasti).[46] Pidana penjara merupakan bentuk pidana yang paling sering digunakan pada hakiim untuk mehakimi sautu permasalahn di Indonesia, hampir apapun tipe tindak piadna terdapat pengancam piadna penjara. Akan tetapi, Muladi menyimpulkan kalau sebabe dari pemaidana penjaran tersebut dapat menimbulkan prisonisasi, dehumanisasi bahkan dapat menyebabkan stigma buruk bagi mantan narapidana dalam kehidupan masyarakat.[47]

Selanjutnya, pemidanaan bagi pelaku phising dalam *game online* yaitu pidana denda. Pidana ganti rugi termasuk tipe pdana sangat kecil dari jenis pidana yang lainnya dan merupakan salah satu pidna wajib yang ada dalam Pasal 10 KUHP. Pidana ganti rugi ialah suatu aturan yang mewajibkan bagi pelaku tindak pidana untuk melunasi sesuatu berupad uang, dikarenakan telah melangar

---

[45] D.A.P. Lamintsang, 1984, *"Hukum Penitencier Indonesia"*, Armico, Badung, Hal. 69.

[46] Banda Nawawi Ariff, 1994, *"Tentuan Legislasif dalam Penanggulangan Kejahatan Dengan Piadna Penjara"*, Hal. 201-202.

[47] Widardo, 2009, *"System Pemidanan pada Cyber Crime"*, Aswwaja, Yogyakarta, Hal. 49.

pengaturan hukum yang aktif pada masyarakat. Pidana ganti rgi memiliki jenis yang berbeda dengan pidana penjara, pada pidana penjara memiliki tujuan untuk menghilangkan kebebasanya, tetapi pidana ganti kerugina ditujukan pada aset pembenda yang dimiliki oleh pelaku tindak pidana. [48]

Maka dari itu, jika pelanggan pengguna layanan online Internet Gamers salah memasukkan nama website resmi (klikgameonline.com), misalnya nama lima website palsu, maka pelanggan atau korban akan dialihkan ke website palsu tersebut.[49]

Dilakukan oleh seorang hacker, korban tertarik dengan imbalan yang ditawarkan oleh scammers dengan menyimpan informasi pribadi pemain di website palsu. Aksi para operator phising tersebut tidak bertujuan untuk mencari keuntungan, melainkan hanya untuk menguji kemampuan mereka dan mengukur berapa banyak pengguna internet yang tertangkap di website yang mereka buat. Dalam konteks peradilan pidana, kegiatan operator phishing sudah dapat digolongkan sebagai pelaku.

Situasi di dalam *game online* itu dibuat seolah-olah mirip seperti dunia nyata. Adapun *game online* yang saat ini bertaburan kita temui di masyarakat, sebenarnya mulai tahun 2003 Indonesia yang pada saat itu *game* yang dinamakan *Ragnarok Online, Gunbond, Seal online* tengah digandrungi namun untuk bisa bermain, sang

---

[48] Sudarsono, 2002, *"Kasus Hukum"*, Rineka Cipta, Jakarta, Hal. 16.
[49] Majalah Tempo, "Rubrik Teknologis Informansi", (24 Juni 2001) dikutip dari M. Arief.

pemain haru membayar terlebih dahulu dengan maksud juga untuk menarik pemain-pemain lainnya agar berminat pada *game* tersebut.

Melihat fenomena tersebut, saat ini sudah sangat banyak *game online* yang menyajikan ketersediaan dari fitur untuk "komunitas online", dengan begitu kegiatan *game online* ini kini sudah menjadi aktivitas sosial yang mendarah daging. *Game-game* dengan fitur tersebut saat ini lebih banyak peminatnya dibandingkan dengan *game* satu orang pemain saja, hal tersebut karena *game* dengan komunitas dianggap lebih menantang dimana akan ada kepuasan tersendiri saat bisa mengalahkan orang lain pada permainan tersebut, belum lagi dengan kecanggihan teknologi era ini yang memudahkan pemain *game online* untuk bermain via *gadget* dan tidak lagi hanya melalui komputer. Dalam *game online* sendiri, pemain bisa bebas melalukan apapun yang diinginkan, namun seringnya dalam ruang virtual ini, pemain *game online* kerap tidak menyadari apa yang dilakukan dalam *game* tersebut ternyata dilarang atau justru berbahaya dan bisa merugikan dirinya.

Dalam peraturan perundang-undangan, tidak dijelakan secara tegas mengenai subyeks hukum mewajibkan melengkapi pidana ganit rugi terhadap sutu penindaan pidana, hal tersebut bisa ditahukan kalau pelunasan ganti rugi bisa dilaksanaan melaui seorang maupun orang ketiga dari peIaku. Saat ganti rugi ynag harusnya diancamkan pada pelakuna supaya menimbulkan efect jerah tidak seutuhnya diperbuat oleh pelakunya tersebut, makanya tujuan pemidanan denda terhadap pelaku phisiing dalam *game online* inilah jadi tidak maximal.

Aturan hukuman mengenai *cyber crime* khususnya tindak pidana phising daIam *game online* menurut peraturan Undang-Unang Nomor 19 Tahun 2016 Tentang Berubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi EIektronik masih mengaIami kekaburan hukum terhadap pengaturannya, haI itu disebabkan phising termasuk suatu perlakuan mencederai hukumnya yang menyebabkan merugian pada orang lainnya. Kerugian yang ditimbulkan dari tindak pidana ini merupakan suatu delik materiiI, karena dalam perbuatannya telah merugikan orang Iain berupa informasi pribadi yang diketahui oIeh pelaku phising dan dapat menyebabkan hiIangnya *account game* milik korban.

Menurut Pasal 35 jo. Pasal 51 ayat (1) UU ITE tidak memuat hal pembohongan yang merugian orang Iain. Selain itu, pada Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE tak bermuat hal pemanipulas, penciptan dan merubahkan informansi eIektronik maupun documen eIektronik itulaht diyakinkan seolah pendata yang otentic, haI ini berarti hal seeorang membikin situs web persi sytus web asIi tidak diatur dalam Pasal tersebut.[50]

Suatu aturan hukum tidak dapat diterapkan kepada peIaku tindak pidana apabiIa hukumnya mengalami masih mengalami kekaburan, misaInya dalam Pasal tersebut tidak memiliki konsep pidananya dan penafsiran yang bermacam-macam. Oleh karena itu, ketenuan hukumnya wajib dilaksanakan tmenurut UU ITE itu melalui perumusan consept secara khusus mengenai phsing dalam *game online* dan

[50] Andi Saputro Gulo, 2020, S*yber Crime pada bentuknya Phsing Didasarkan Undang-Undang Informnasi dan Transaksi EIektronik"*, PAMAS: Journals of Kriminal, Hal 78.

juga perubah 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.

BAB IV

PENUTUP

4.1 Kesimpulan

1. Praktik Phising Dalam *Game Online* Merupakan *Cyber Crime*

Terjadinya phising dilakukan saat pelaku menyamar sebagai institusi resmi yang menggunakan site web manipulas, untuk mengelabui penguna untuk membagi informansi pribadi. Tindakan physing pemanfaatkan *e-mail*, websyte fake, software lalu bermacam media yang lain dalam pelancaran aksi itu. 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. *Syber crime* merupaan tidnak kejahatan guna 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 assas *Lek Spesialis Derogaf Legsi GeneraIis* yang berarti peraturan penghukum melebihi kusus mengabaian peraturan hukum sifatnya generals. Tindak pidana phising dalam game online merupakan suatu tindakan yang mencoreng hukum, maka peejatuhan pmidana pada physer 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

Tentangan Pengubahan Atas Undang-Udnang Nomor 11 Tahun 2008 Tentangan Informansi dan Transaksi EIektronik. Bagi pelaku yang memenuhi halnya daripada Pasal itulah dapat dikenakan Pasal berlapis serta tak boleh melebihkan maximalnya pidana paling berat lalu tambahkan sepertiganya, system itu dikenal sebagai kumulation diperlunakkan.

4.2 Saran

1. 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. Jadi diperluan pengadanya pembantuan antar masyarakatnya sertaa pemerintahnnya dalam mengatasi kejahatan phising tersebut, karena kejahatan yang terjadi di dunia internets makin harinya makin berkemajuan dari tipe kejahatannya ataupun permodusan operasinya.
2. Aparat penegak hukum harus menambahi qualiti dan quantitas terutama pada penguasan teknologi informansi termaskus internets, tingkatkan saransa dan prasaran dukungan tuk penelitan dan penyelidian kassusnya di *cyber crime* dalam hal ini praktik phising, pemberikan educasion dan literatio masifsi terhadap masyarakat lalui *cyber crime* serta gimana usaha peminimalisiran supaya tak dapat terjeruimus dalam permodusan physer *cyber crime* terutama praktik phsing.

Skripsi Rizky (Turnitin)..pdf

ORIGINALITY REPORT

16%	16%	9%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	online-journal.unja.ac.id Internet Source	2%
2	digilib.uinsby.ac.id Internet Source	2%
3	www.researchgate.net Internet Source	1%
4	eprints.walisongo.ac.id Internet Source	1%
5	erepository.uwks.ac.id Internet Source	1%
6	repository.unhas.ac.id Internet Source	1%
7	www.hukumonline.com Internet Source	<1%
8	repository.unbari.ac.id Internet Source	<1%
9	jurnal.dharmawangsa.ac.id Internet Source	<1%

10	Submitted to Universitas Islam Indonesia Student Paper	<1 %
11	repository.ub.ac.id Internet Source	<1 %
12	jurnal.uns.ac.id Internet Source	<1 %
13	Submitted to Universitas Musamus Merauke Student Paper	<1 %
14	ejournal2.undip.ac.id Internet Source	<1 %
15	etheses.uin-malang.ac.id Internet Source	<1 %
16	Submitted to Universitas Pamulang Student Paper	<1 %
17	ejournal.unsrat.ac.id Internet Source	<1 %
18	Submitted to Universitas Jember Student Paper	<1 %
19	comserva.publikasiindonesia.id Internet Source	<1 %
20	Submitted to Universitas Trunojoyo Student Paper	<1 %
21	repository.uinjambi.ac.id Internet Source	<1 %

22	Submitted to Sriwijaya University Student Paper	<1 %
23	dblp.dagstuhl.de Internet Source	<1 %
24	mafiadoc.com Internet Source	<1 %
25	androskripsi.wordpress.com Internet Source	<1 %
26	docplayer.info Internet Source	<1 %
27	ejournal.uika-bogor.ac.id Internet Source	<1 %
28	adoc.pub Internet Source	<1 %
29	eprints.unram.ac.id Internet Source	<1 %
30	kumparan.com Internet Source	<1 %
31	repository.umsu.ac.id Internet Source	<1 %
32	repository.unja.ac.id Internet Source	<1 %
33	bk.ppj.unp.ac.id Internet Source	<1 %

34	download.garuda.ristekdikti.go.id Internet Source	<1 %
35	repository.iainpalopo.ac.id Internet Source	<1 %
36	Submitted to Surabaya University Student Paper	<1 %
37	eprints.uniska-bjm.ac.id Internet Source	<1 %
38	jurnal.unissula.ac.id Internet Source	<1 %
39	e-journal.unair.ac.id Internet Source	<1 %
40	Fakhri Rizki Zaenudin, Hana Faridah. "Pertanggungjawaban Pidana Terhadap Afiliator Aplikasi Opsi Biner Ilegal Dalam Hukum Pidana Indonesia", Jurnal Hukum Sasana, 2022 Publication	<1 %
41	digilib.uinsgd.ac.id Internet Source	<1 %
42	123dok.com Internet Source	<1 %
43	jurnal.untagsmg.ac.id Internet Source	<1 %

44	text-id.123dok.com Internet Source	<1 %
45	Submitted to Universitas Muhammadiyah Magelang Student Paper	<1 %
46	Zaid Effendi. "PANCASILA SEBAGAI DASAR PEMBERANTASAN KEJAHATAN KORPORASI DI INDONESIA", JOURNAL EQUITABLE, 2023 Publication	<1 %
47	journal.untar.ac.id Internet Source	<1 %
48	journals.usm.ac.id Internet Source	<1 %
49	www.fazwaz.id Internet Source	<1 %
50	blog.justika.com Internet Source	<1 %
51	digilib.uin-suka.ac.id Internet Source	<1 %
52	mainsaham.id Internet Source	<1 %
53	repository.uma.ac.id Internet Source	<1 %
54	bhl-jurnal.or.id Internet Source	<1 %

55	fr.scribd.com Internet Source	<1 %
56	repo.bunghatta.ac.id Internet Source	<1 %
57	www.ememha.com Internet Source	<1 %
58	www.scribd.com Internet Source	<1 %
59	gilangsukmana.blogspot.com Internet Source	<1 %
60	journal.uinmataram.ac.id Internet Source	<1 %
61	jutei.ukdw.ac.id Internet Source	<1 %
62	repo.iain-tulungagung.ac.id Internet Source	<1 %
63	repositori.umsu.ac.id Internet Source	<1 %
64	repository.unika.ac.id Internet Source	<1 %
65	repository.unsoed.ac.id Internet Source	<1 %
66	www.slideshare.net Internet Source	<1 %

67	andimanurungzz.blogspot.com Internet Source	<1 %
68	digilib.unila.ac.id Internet Source	<1 %
69	es.scribd.com Internet Source	<1 %
70	mudah-bahasaindonesia.blogspot.com Internet Source	<1 %
71	repository.uki.ac.id Internet Source	<1 %
72	repository.upnjatim.ac.id Internet Source	<1 %
73	sinta.unud.ac.id Internet Source	<1 %
74	www.cnbcindonesia.com Internet Source	<1 %
75	journal.ugm.ac.id Internet Source	<1 %
76	Elfirda Ade Putri. "Penerapan Sanksi Pidana terhadap Pelaku Tindak Pidana Korupsi di Tinjau Dari Perspektif Konsep Hukum Progresif", Jurnal Keamanan Nasional, 2022 Publication	<1 %
77	ejournal.unesa.ac.id Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		