JUSTITIA : Jurnal Ilmu Hukum dan Humaniora
ISSNCetak :2354-9033 |ISSN Online :2579-9398
http://jurnal.um-tapsel.ac.id/index.php/Justitia| Vol. 9 No. 2 Tahun 2022

PERTANGGUNGJAWABAN HUKUM PLATFORM MEDIA SOSIAL TERHADAP KORBAN *PHISING* MELALUI *MASS TAGGING* PORNOGRAFI

Nawawi Muslim, Oci Senjaya
Fakultas Hukum, Universitas Singaperbangsa Karawang

ABSTRAK

Di era milenial ini, media sosial seperti sudah menjadi kebutuhan primer. Namun, media sosial juga rentan terhadap kejahatan, salah satunya adalah phising melalui mass tagging pornografi yang berujung pada peretasan akun. Tindakan ini termasuk perbuatan pidana dan diatur dalam Pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Penelitian ini membahas mengenai sanksi apakah yang dapat dijatuhkan bagi pelaku tindak pidana phising ditinjau dari hukum positif Indonesia dan bagaimana bentuk pertanggungjawaban hukum platform media sosial terhadap korban phising melalui mass tagging pornografi.Penelitian ini menggunakan metode yuridis normatif serta menggunakan pendekatan undang-undang dan konseptual. Dari hasil penelitian ini dapat disimpulkan bahwa sampai saat ini belum ada undang-undang yang secara khusus mengatur mengenai phising. Namun demikian, pelaku dapat dijerat dengan ketentuan KUHP dan UU ITE, sesuai dengan tindak pidana pelaku. Dan pengguna bisa mengajukan gugatan perdata untuk menuntut ganti kerugian jika kelalaian berasal dari pemilik platform sesuai dengan Pasal 15 UU ITE.

Kata Kunci : **Mass Tagging; Milenial; Phising; Platform; Pornografi**

PENDAHULUAN

Berselancar di media sosial sudah menjadi bagian dari gaya hidup masyarakat di era milenial. Hanya dengan bermodalkan *smartphone*, orang bisa terhubung di banyak *platform* media sosial. Konten-konten yang terdapat dalam berbagai media sosial pun cukup beragam, namun ada juga pengguna yang hanya sekadar mencari informasi dan hiburan di dunia maya.

Di era milenial ini, media sosial seperti sudah menjadi kebutuhan primer, seperti untuk memposting momen keseharian atau momen spesial sesorang dan juga mungkin hanya sekadar untuk mencari informasi atau hiburan semata. Namun, media sosial juga rentan terhadap kejahatan seperti penipuan hingga peretasan. Salah satunya adalah *phising* (pengelabuan) yang tengah ramai diperbincangkan karena adanya *mass tagging* (penandaan massal) pornografi yang berujung pada peretasan akun.

E-Mail : nawawimuslim2@gmail.com
DOI : www. dx.doi.org 10.31604/justitia.v9i2. 955-963

Phising merupakan suatu upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran *phising* adalah data pribadi (nama, usia, alamat), data akun (*username* dan kata sandi), dan data finansial (informasi kartu kredit, rekening).[2]

Phising juga dapat diartikan sebagai suatu bentuk tindakan penipuan yang biasanya digambarkan dengan percobaan untuk mendapatkan informasi peka, misalnya informasi mengenai kata sandi dan kartu kredit, dengan menyamar sebagai orang atau lembaga yang sah.[3]

Ketua Umum Indonesia *Cyber Law Community* (ICLC), Teguh Arifiyadi, mengatakan bahwa setiap orang bisa melakukan *tagging* secara massal pada *platform* media sosial. Oknum menyebarkan link *phising* menggunakan konten-konten pornografi untuk menarik pengguna masuk ke dalam konten tersebut. Hal semacam ini dilakukan secara otomatis dengan teknik menyebarkan link ke banyak pengguna media sosial.[4]

Tak hanya di Indonesia, *mass tagging* ini juga terjadi di berbagai negara. Meski pihak *platform* media sosial sudah melakukan investigasi dan memblokir link-link pornografi tersebut dari *platform*, namun tak ada jaminan keamanan sepenuhnya bahwa *platform* tersebut aman.

Dari sisi teknologi, tidak ada jaminan suatu *platform* itu aman. Tapi *platform* harus memiliki langkah-langkah yang memberi solusi bagaimana mengatasi modus seperti ini. Setiap *platform* pasti melakukan pengamanan secara optimal, namun tetap ada celah, dan bagaimana platform merespons kemudian melakukan investigasi terhadap modus-modus ini.

Pada dasarnya, pengguna media sosial bisa mengantisipasi *mass tagging* di akun pribadinya. Salah satunya dengan cara tidak menampilkan nomor seluler dan tidak asal membuka link tautan dari siapapun jika tidak yakin atau tidak bisa diidentifikasi dengan baik, apalagi yang berisi ajakan-ajakan yang isinya *clickbait*, yang bisa saja terdapat *phising* dan *malware* didalamnya. Di berbagai *platform* media sosial pun juga telah menyediakan *setting*-an untuk menampilkan atau tidak konten *mass tagging* tersebut. Selain itu terdapat fitur keamanan untuk melindungi akun yang bisa digunakan oleh pengguna media sosial.

Peretasan akun, salah satunya melalui *mass tagging* yang berisi konten pornografi ini cukup berbahaya karena bisa digunakan sebagai sarana penipuan dengan mengatasnamakan pemilik akun, akun diperjualbelikan untuk iklan atau sarana promosi satu produk. Biasanya akun-akun dengan banyak *follower* menjadi sasaran para peretas. Tindakan ini termasuk perbuatan pidana dan diatur dalam Pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Di sisi lain, banyak oknum yang melakukan peretasan akun hanya untuk iseng dan tidak melakukan pencurian data. Namun demikian, perbuatan mengambil alih akun milik

---

[2] Suryadi Kurniawan, 'Phising: Pengertian, Cara Kerja Dan Langkah Mengatasinya' (2020) <https://www.niagahoster.co.id/blog/mengatasi-phishing/> diakses 22 Mei 2021.

[3] Fitri Novia Heriani, 'Jadi Korban Phising Lewat Mass Tagging Pornografi? Pengguna Bisa Tuntut Platform' (2021) <https://jurnal.hukumonline.com/berita/baca/lt608845a8dcbc1/jadi-korban-phising-lewat-i-mass-tagging-i-pornografi-pengguna-bisa-tuntut-platform?page=all> diakses 22 Mei 2021.

[4] *Ibid.*

orang lain tanpa persetujuan pemilik adalah tindakan ilegal. Perbuatan ini bisa diancam pidana penjara sebagaimana diatur dalam UU ITE.

Perbuatan meretas meskipun tidak untuk mencuri data, termasuk dalam perbuatan mengambil alih merupakan ilegal akses, yang melanggar Pasal 30 ayat (1), (2) dan (3), dengan maksimal pidana penjara 3 tahun. Sejauh ini instrumen hukum untuk mengatasi kasus tersebut sudah cukup lengkap, namun memang tidak mudah menemukan pelaku dengan modus spesifik, butuh investigasi lama dan mendalam.

Mekanisme pengawasan terutama untuk menyamakan persepsi saat terjadinya kebocoran data sangatlah penting. Pengawasan harus memiliki standar yang jelas, misal bagaimana tanggung jawab *platform* jika terjadi kebocoran data, apa yang harus dilakukan pemilik data saat terjadi kebocoran data sehingga dari setiap insiden bisa didapat gambaran yang jelas.

Sebagai langkah antisipasi, pemerintah memiliki peran untuk melakukan sosialisasi dan edukasi ke banyak *stakeholder* seperti *platform*, untuk memberikan pendidikan dan pemahaman terkait *security awareness* kepada pengguna pemula. Selanjutnya, penegakan hukum harus dipublikasikan dan diproses untuk memberikan efek jera kepada pelaku dan calon pelaku kejahatan.

Jika peretasan terhadap akun media sosial menimbulkan kerugian bagi pemilik akun, maka *platform* adalah pihak yang paling bertanggung jawab. Jika kelalaian dari *platform*, maka *platform* wajib bertanggung jawab, dan pengguna harus bisa membuktikan ada kelemahan dan celah dari *platform* yang bisa memberikan akses bagi peretas untuk masuk. Pengguna bisa mengajukan gugatan perdata untuk menuntut ganti kerugian jika kelalaian berasal dari pemilik *platform* sesuai dengan Pasal 15 UU ITE.

Namun, Pasal 15 ayat (3) memberikan pengecualian, di mana *platform* tidak bertanggung jawab atas kerugian yang dialami pemilik akun jika adanya kelalaian dari sisi pengguna.

Selalu ada batasan dan regulasi dalam penggunaan informasi dan transaksi elektronik. Diperlukan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi dalam regulasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik. Dan juga untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu lingkungan masyarakat. Undang-Undang Informasi dan Transaksi Elektronik dibuat untuk mewujudkan keadilan, ketertiban umum, dan kepastian hukum bagi masyarakat.

Kementerian Komunikasi dan Informatika (Kominfo) Republik Indonesia menanggapi kejadian *mass tagging* dari link tautan yang bermuatan pornografi di media sosial, yang terjadi beberapa waktu terakhir. Pihak Kominfo telah melakukan upaya dengan memblokir link tautan yang mencurigakan agar kasus *phising* dapat diminimalisir.

Agar terhindar dari upaya *phishing*, Kominfo mengimbau masyarakat untuk tidak mengakses tautan atau pesan yang mencurigakan, serta menjaga keamanan akun dengan memastikan kembali *setting* keamanan dan privasi di semua akun media sosial, aplikasi percakapan dan email.

Seiring dengan berkembangnya kemajuan teknologi dan internet mampu mengubah berbagai pola-pola yang sudah mapan dalam suatu tindak pidana dengan kata lain modus operandi yang umumnya dilakukan dalam kejahatan umum (konvesional) melalui teknologi

internet telah diubah menjadi modus operandi yang sifatnya baru, sehingga hal ini mengakibatkan perlunya upaya-upaya penanganan yang baru pula.[5]

Bertitik tolak dari latar belakang yang telah diuraikan di atas, penulis tertarik untuk meneliti mengenai sanksi apakah yang dapat dijatuhkan bagi pelaku tindak pidana *phising* ditinjau dari hukum positif Indonesia dan bagaimana bentuk pertanggungjawaban hukum *platform* media sosial terhadap korban *phising* melalui *mass tagging* pornografi.

Jenis kajian dalam penelitian ini lebih bersifat deskriptif, karena bermaksud memaparkan secara jelas tentang hal-hal yang terkait dengan objek yang diteliti. Penelitian ini menggunakan metode yuridis normatif, yang merupakan penelitian yang mengacu kepada norma-norma hukum yang terdapat dalam peraturan perundang-undangan, sejarah, kasus dan putusan pengadilan sebagaimana sifat Ilmu Hukum yang "*Sui Generis*". Data yang digunakan dalam penelitian ini diperoleh melalui penelitian kepustakaan dan teknik pengumpulan dan inventarisasi peraturan perundang-undangan, buku-buku, karya ilmiah, artikel-artikel yang ada hubungannya dengan tindak pidana *phising*. Dalam penelitian ini juga menggunakan beberapa pendekatan masalah berupa pendekatan perundang-undangan *(statue approach),* dalam hal ini perundang-undangan yang dimaksud adalah perundang-undangan mengenai tindak pidana *phising*. Serta pendekatan konseptual *(conceptual approach).*

Data yang digunakan dalam penelitian ini adalah data hukum sekunder yang menggunakan sumber bahan hukum primer yang berupa Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) dan Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta bahan hukum sekunder yang berupa artikel, jurnal, dan literatur yang relevan dengan permasalahan mengenai pertanggungjawaban hukum *platform* media sosial terhadap korban *phising* melalui *mass tagging* pornografi. Teknik pengumpulan data dalam penelitian ini menggunakan studi kepustakaan, serta menggunakan analisis terhadap bahan hukum yang dilakukan secara kualitatif normatif.

PEMBAHASAN

Sanksi Yang Dapat Dijatuhkan Bagi Pelaku Tindak Pidana *Phising* Menurut Hukum Positif Indonesia

Phising dalam terjemahan bebas didefinisikan sebagai suatu tindak kejahatan mayantara (*cybercrime*) di mana seseorang menyamar sebagai lembaga yang sah menghubungi korban/target melalui email, telepon, atau pesan singkat, agar korban memberikan data sensitif misalnya informasi identitas pribadi, detail perbankan dan kartu kredit, serta kata sandi. Selanjutnya, dari informasi yang didapat tersebut kemudian digunakan untuk mengakses akun korban yang bisa mengakibatkan peretasan akun, pencurian identitas dan kerugian finansial.[6]

---

[5] Dikdik M. Arief Mansyur dan Elisatris Gultom, *CYBER LAW Aspek Hukum Teknologi Informasi* (PT Reflika Aditama 2009) 89.

[6] Phising.org, 'What is Phising?' <https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords> diakses pada 24 Mei 2021.

Pelaku *phising* dalam melakukan perbuatannya menggunakan berbagai macam cara atau modus di antaranya:[7]

a. Mengirimkan Email Palsu
   Pelaku mengirimkan pesan palsu melalui email, di mana ia menyamar sebagai petugas atau admin *website* suatu perusahaan yang sah. Isinya biasanya mengenai pemberitahuan yang ditujukan kepada pemilik akun tentang suatu hal tertentu yang sifatnya penting, mendesak, dan membutuhkan respon yang cepat dan segera. Dalam pesan tersebut juga dicantumkan suatu tautan/*link* yang apabila diklik oleh korban, maka korban akan diarahkan menuju ke suatu *website* yang dibuat oleh pelaku.
b. *Web Forgery* (Pemalsuan Web)
   Web forgery yaitu suatu upaya pemalsuan web yang dirancang untuk menipu pengunjungnya. Tampilan *website* tersebut dibuat mirip dengan *platform* resminya. Selanjutnya, korban diarahkan untuk menginput identitasnya dalam suatu formulir yang sudah disiapkan pelaku. Setelah korban menginput *username* dan kata sandinya, data akan tersimpan dalam *database* situs web tersebut, sehingga pelaku bisa mencuri data-data yang sudah diinput oleh korban.
c. *Phone Phising*
   Pelaku menghubungi korban melalui telepon dengan mengatasnamakan suatu pihak/lembaga tertentu. Selanjutnya, pelaku menanyakan dan meminta hal tertentu, misalnya meminta *username* dan kata sandi korban, dan meminta kode *one-time password* (OTP) yang masuk ke telepon seluler korban.
d. SMS *Phising*
   Pelaku akan mengirimkan SMS yang isinya pemberitahuan bahwa korban telah memenangkan hadiah undian berupa uang. Untuk bisa mengklaim hadiahnya, korban diarahkan untuk mengkonfirmasi dengan memberikan *username* dan kata sandi *internet banking* kepada pelaku.
e. *Chat Phising*
   Pelaku akan berpura-pura seolah-olah menjadi *customer service online* dengan merekayasa bahwa tampilan web sedang terputus, dan kemudian mengarahkan korban untuk *log in* ulang dengan memasukan *username* dan kata sandi pada tautan yang dikirim oleh pelaku.

Sampai saat ini belum ada regulasi yang secara *lex specialis* mengatur mengenai tindak pidana *phising*. Namun, pelaku dapat dijerat sesuai 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 Elektronik (ITE), sesuai dengan tindak pidana yang dilakukan oleh pelaku.[8]

---

[7] Ki Jagad Tomara, '[Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs *Phising*]' (Skripsi, Fakultas Hukum Universitas Brawijaya 2011) 54-66.

[8] Erizka Permatasari. 'Jerat Hukum Pelaku Phising Dan Modusnya' (2021) <https://new.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-iphising-i-dan-modusnya/> diakses pada 24 Mei 2021.

Berikut pasal-pasal yang dapat dijatuhkan terhadap pelaku *phising*, diantaranya yaitu:[9]

a. Penipuan

   Terdapat dalam KUHP Pasal 378, yang berbunyi:

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

b. Manipulasi

   Terdapat dalam UU ITE Pasal 35 jo. Pasal 51, yang berbunyi:

   "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik dipidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp. 12 miliar."

c. Penerobosan

   Terdapat dalam UU ITE Pasal 30 ayat (3) jo. Pasal 46 ayat (3), yang berbunyi:

   "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp. 800 juta."

d. Memindahkan atau Mentransfer

   Terdapat dalam UU ITE Pasal 32 ayat (2) jo. Pasal 48 ayat (2), yang berbunyi:

   "*Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak dipidana penjara paling lama 9 tahun dan/atau denda paling banyak Rp. 3 miliar*."

Pertanggungjawaban Hukum *Platform* Media Sosial Terhadap Korban *Phising* Melalui *Mass Tagging* Pornografi

Di era milenial ini, media sosial seperti sudah menjadi kebutuhan primer, seperti untuk memposting momen keseharian atau momen spesial sesorang dan juga mungkin hanya sekadar untuk mencari informasi atau hiburan semata. Namun, media sosial juga rentan terhadap kejahatan seperti penipuan hingga peretasan. Salah satunya adalah *phising* (pengelabuan) yang tengah ramai diperbincangkan karena adanya *mass tagging* (penandaan massal) pornografi yang berujung pada peretasan akun.

Phising dapat diartikan sebagai suatu bentuk tindakan penipuan yang biasanya digambarkan dengan percobaan untuk mendapatkan informasi peka, misalnya informasi mengenai kata sandi dan kartu kredit, dengan menyamar sebagai orang atau lembaga yang sah.

Ketua Umum Indonesia *Cyber Law Community* (ICLC), Teguh Arifiyadi, mengatakan bahwa setiap orang bisa melakukan *tagging* secara massal pada *platform* media sosial. Oknum menyebarkan link *phising* menggunakan konten-konten pornografi untuk menarik

[9] *Ibid.*

pengguna masuk ke dalam konten tersebut. Hal semacam ini dilakukan secara otomatis dengan teknik menyebarkan link ke banyak pengguna media sosial.[10]

Jika peretasan terhadap akun media sosial menimbulkan kerugian bagi pemilik akun, maka *platform* adalah pihak yang paling bertanggung jawab. Jika kelalaian dari *platform*, maka *platform* wajib bertanggung jawab, dan pengguna harus bisa membuktikan ada kelemahan dan celah dari *platform* yang bisa memberikan akses bagi peretas untuk masuk. Pengguna dapat mengajukan gugatan perdata untuk menuntut ganti kerugian jika kelalaian berasal dari pemilik *platform* sesuai dengan Pasal 15 UU ITE. Namun, Pasal 15 ayat (3) UU ITE memberikan pengecualian, di mana *platform* tidak bertanggung jawab atas kerugian yang dialami pemilik akun jika adanya kelalaian dari sisi pengguna.

Tetapi, apabila *platform* media sosial bekerja sama dengan pihak lain dari luar perusahaan tersebut yang terindikasi tindak pidana, maka perbuatannya masuk ke dalam ranah pidana penyertaan. Pidana penyertaan merupakan perbuatan pidana yang melibatkan lebih dari satu orang. Penyertaan merupakan bentuk keterlibatan atau turut serta seseorang atau lebih, baik itu secara fisik maupun secara psikis melakukan suatu tindakan yang mengakibatkan suatu tindak pidana.[11] Karena dalam penyertaan melibatkan lebih dari satu peserta, maka tentu saja pembebanan pertanggungjawabannya pun berbeda. Terdapat dua macam bentuk pembebanan tanggung jawab dalam doktrin hukum pidana, yaitu:

1. Setiap orang yang terlibat atau turut serta dalam tindak pidana dianggap dan dibebankan tanggung jawab secara sama dengan pembuat tindak pidana, tanpa terkecuali baik atas tindakan yang dilakukannya atau yang ada dalam niatnya.
2. Setiap orang yang terlibat atau turut serta dalam tindak pidana dianggap dan dibebankan tanggung jawab secara berbeda, sesuai dengan perbuatannya masing-masing.

Apabila *Platform* media sosial terbukti bersalah, baik bertindak sebagai pelaku tunggal, bersama-sama dengan pihak lain (penyertaan), maupun berlaku sebagai pembantu, jelas dapat dikenai sanksi pidana. Ketentuan yang mengatur mengenai sanksi pidana bagi *platform* media sosial selaku penyedia dan penyelenggara sistem informasi apabila terbukti bersalah adalah Pasal 52 ayat (4) UU ITE, yang berbunyi:

"Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga."

Ketentuan tersebut berlaku bagi semua macam jenis penyertaan. Khusus untuk pembantuan, maka dikenakan ketentuan dalam Pasal 57 ayat (1) KUHP. Dalam hal pembantuan, maksimum pidana pokok terhadap kejahatan dikurangi sepertiga.

Selalu ada batasan dan regulasi dalam penggunaan informasi dan transaksi elektronik. Diperlukan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi dalam regulasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik. Dan juga untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu lingkungan

[10] Fitri Novia Heriani, *Loc. Cit.*
[11] Adami Chazawi, *Pelajaran Hukum Pidana Bagian 3* (PT Raja Grafindo Persada 2005) 73.

masyarakat. Undang-Undang Informasi dan Transaksi Elektronik dibuat untuk mewujudkan keadilan, ketertiban umum, dan kepastian hukum bagi masyarakat.

PENUTUP

Phising merupakan suatu tindak kejahatan mayantara (*cybercrime*) di mana seseorang menyamar sebagai lembaga yang sah, kemudian menghubungi korban/target melalui email, telepon, atau pesan singkat, agar korban memberikan data sensitif misalnya informasi identitas pribadi, detail perbankan dan kartu kredit, serta kata sandi. Selanjutnya, dari informasi yang didapat tersebut kemudian digunakan untuk mengakses akun korban yang dapat mengakibatkan peretasan, pencurian identitas dan kerugian finansial. Pelaku *phising* dalam melakukan perbuatannya menggunakan berbagai macam cara atau modus di antaranya: Mengirimkan email palsu; *Web Forgery*; *Phone Phising*; SMS *Phising*; dan *Chat Phising*. Sampai saat ini belum ada regulasi yang secara *lex specialis* mengatur mengenai tindak pidana *phising*. Namun, pelaku dapat dijerat sesuai 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 Elektronik (ITE), sesuai dengan tindak pidana yang dilakukan oleh pelaku, di antaranya: Pasal 378 KUHP; Pasal 35 jo. Pasal 51; Pasal 30 ayat (3) jo. Pasal 46 ayat (3); Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE.

Jika peretasan terhadap akun media sosial menimbulkan kerugian bagi pemilik akun, maka *platform* adalah pihak yang paling bertanggung jawab. Jika kelalaian dari *platform*, maka *platform* wajib bertanggung jawab, dan pengguna harus bisa membuktikan ada kelemahan dan celah dari *platform* yang bisa memberikan akses bagi peretas untuk masuk. Pengguna dapat mengajukan gugatan perdata untuk menuntut ganti kerugian jika kelalaian berasal dari pemilik *platform* sesuai dengan Pasal 15 UU ITE. Namun, Pasal 15 ayat (3) memberikan pengecualian, di mana *platform* tidak bertanggung jawab atas kerugian yang dialami pemilik akun jika adanya kelalaian dari sisi pengguna. Tetapi, apabila *platform* media sosial bekerja sama dengan pihak lain dari luar perusahaan tersebut yang terindikasi tindak pidana, maka perbuatannya masuk ke dalam ranah pidana penyertaan. Apabila *Platform* media sosial terbukti bersalah, baik bertindak sebagai pelaku tunggal, bersama-sama dengan pihak lain (penyertaan), maupun berlaku sebagai pembantu, jelas dapat dikenai sanksi pidana. Ketentuan yang mengatur mengenai sanksi pidana bagi *platform* media sosial selaku penyedia dan penyelenggara sistem informasi apabila terbukti bersalah adalah Pasal 52 ayat (4) UU ITE, ketentuan tersebut berlaku bagi semua macam jenis penyertaan. Khusus untuk pembantuan, maka dikenakan ketentuan dalam Pasal 57 ayat (1) KUHP. Selalu ada batasan dan regulasi dalam penggunaan informasi dan transaksi elektronik. Diperlukan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi dalam regulasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik.

DAFTAR BACAAN

Buku:

Chazawi, Adami, *Pelajaran Hukum Pidana Bagian 3* (PT RajaGrafindo Persada 2005).

Mansyur, Dikdik M. Arief dan Gultom, Elisatris, *CYBER LAW Aspek Hukum Teknologi Informasi*, (PT Reflika Aditama 2009).

Skripsi:

Tomara, Ki Jagad, 'Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs *Phising*' (Skripsi, Fakultas Hukum Universitas Brawijaya 2011).

Peraturan Perundang-Undangan:

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Internet:

Heriani, Fitri Novia, 'Jadi Korban Phising Lewat Mass Tagging Pornografi? Pengguna Bisa Tuntut Platform' <https://jurnal.hukumonline.com/berita/baca/lt608845a8dcbc1/jadi-korban-phising-lewat-i-mass-tagging-i-pornografi-pengguna-bisa-tuntut-platform?page=all> diakses pada 22 Mei 2021.

Kurniawan, Suryadi, 'Phising: Pengertian, Cara Kerja Dan Langkah Mengatasinya' <https://www.niagahoster.co.id/blog/mengatasi-phishing/> diakses pada 22 Mei 2021.

Permatasari, Erizka, 'Jerat Hukum Pelaku Phising Dan Modusnya' (2021) <https://new.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-iphising-i-dan-modusnya/> diakses pada 24 Mei 2021.

Phising.org, 'What is Phising?' <https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords> diakses pada 24 Mei 2021.