

PERSPEKTIF UNDANG-UNDANG TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK TERHADAP *CYBER CRIME* DALAM BENTUK *PHISING*

Anggun Juniamalia Sholikhah, Aryo Fadlian

Fakultas Hukum Universitas Singaperbangsa Karawang

anggunjuniamalias@gmail.com, deni.ramdhani.2811@gmail.com,

aryo.fadlian@fh.unsika.ac.id

ABSTRAK

Perkembangan sistem informasi memicu terjadinya perubahan kebiasaan, dimana masyarakat pada saat ini cenderung lebih sering menggunakan internet dalam melakukan interaksi sosial dan bahkan dalam melakukan proses jual beli yang biasanya di lakukan di pasar. Hal demikian menjadi latar belakang di bentuknya UU ITE. Di dalam UU ITE terdapat pasal yang membahas mengenai perlindungan terhadap korban dari tindak pidana cyber crime. Tidak dapat di pungkiri bahwasanya perkembangan informasi juga mengakibatkan banyak terjadinya kasus tindak pidana cyber crime dan yang sering terjadi ialah tindakan phising dimana pelaku mencuri informasi korban dengan menggunakan teknik penipuan. Hal demikian kerap terjadi di media sosial whatsapp, dimana pelaku akan mengirimkan link pada korban melalui nomor yang tidak di ketahui ke nomor korbannya, dengan motip memberikan hadiah berupa uang dari salah satu lembaga online shop. Hal demikian tentunya menjadi salah satu tujuan penulis membuat artikel ini.

Kata Kunci : informasi, sosial, cyber crime, media sosial, phising

ABSTRACT

The development of information systems triggers changes in habits, where people nowadays tend to use the internet more often in carrying out social interactions and even in carrying out the buying and selling process which is usually carried out in the market. This is the background in the formation of the ITE Law. In the ITE Law there is an article that discusses the protection of victims from cyber crime. It cannot be denied that the development of information has also resulted in many cases of cybercrime and what often occurs is phishing where the perpetrator steals the victim's information using fraudulent techniques. This often happens on WhatsApp social media, where the perpetrator will send a link to the victim via an unknown number to the victim's number, with the motive of giving a prize in the form of money from one of the online shop institutions. This, of course, is one of the goals of the author in writing this article.

Keyword : information, social, cyber crime, social media, phishing

Perspektif Undang-Undang Tentang Informasi ...

A. PENDAHULUAN

Pada era saat ini internet menjadi kebutuhan pokok semua kalangan masyarakat di dunia khususnya di Indonesia. Karena dengan menggunakan internet masyarakat lebih mudah dalam mengakses informasi, bersosial dan melakukan kegiatan jual beli. Dalam prosesnya tersebut tak jarang pula mereka menggunakan media sosial dan situs online shop, seperti whatsapp, instagram, twitter, shopee, tokopedia dsb.

Ketika seseorang mendaftar akun media sosial dan online shop biasanya pengguna akan di minta memberikan data pribadi berupa nama, alamat, tgl lahir dsb. Hal demikian memicu terjadinya tindak pidana phising dimana pelaku akan mencuri data korban. Phising termasuk kedalam cyber crime yang dapat di artikan bahwa hal demikian dapat membahayakan hak dari korban dari tindakan phising.

Phising adalah tindakan penipuan dengan cara mengelabui target atau korban dengan maksud mencuri informasi penting dari user yang menggunakan internet. Istilah ini berasal dari kata “fishing” atau memancing target agar terperangkap dijebakkannya. Pelaku phishing akan mengklaim dirinya sebagai pihak institusi yang berwenang lalu mereka akan mengirimkan link pada korbannya yang di muat dalam narasi berupa pesan. Di kutip dari blog master ada 4 jenis tindakan cyber crime phishing di antaranya¹:

Spear Phising

Spear phishing merupakan tindakan mengirim email pada korban dengan spesifik dan mengaku sebagai pengirim terpercaya. Isi email tersebut biasanya berisi tautan yang mengarahkan penerima ke situs web palsu yang penuh dengan malware. Upaya ini ditargetkan untuk mencuri informasi sensitif seperti kredensial akun atau informasi keuangan dari korban tertentu. Meskipun sering dimaksudkan untuk mencuri data untuk tujuan jahat, penjahat cyber mungkin juga berniat untuk menginstal malware di komputer pengguna yang ditargetkan. Ini adalah bentuk paling sukses untuk memperoleh informasi rahasia di internet, mencakup 91% serangan.

¹ Ridho Nastainullah "*Ciri-Ciri Phising dan Cara Mengatasinya*" [Apa Itu Phising, Ciri-Ciri dan Cara Mengatasinya - Masterweb Blog \(ampproject.org\)](#) di akses pada 17 desember 2022

Perspektif Undang-Undang Tentang Informasi ...

Deceptive Phising

Deceptive Phising adalah jenis penipuan phishing yang paling umum. Penipuan ini terjadi ketika sumber yang dikenal atau perusahaan yang Anda kenal mengirim email kepada Anda untuk mengkompromikan informasi. Biasanya, email-email ini meminta Anda:

- Verifikasi informasi akun
- Masukkan kembali informasi, seperti login atau kata sandi
- Minta Anda mengubah kata sandi Anda
- Melakukan pembayaran

Setelah informasi ini dimasukkan, peretas akhirnya mendapatkan informasi dan dapat mengakses akun Anda lalu menggunakan informasi sensitif untuk mencuri informasi kartu pembayaran, menjual informasi pribadi Anda atau memanfaatkan informasi sensitif Anda untuk mendapatkan keuntungan.

Ada 2 cara yang bisa dilakukan oleh pelaku untuk melakukan tindakan phising ini, cara pertama yaitu pelaku mengklaim atau menyamar sebagai perwakilan dari sebuah instansi/perusahaan resmi dan meminta korbannya tersebut untuk memberikan informasi tertentu. Cara kedua, pelaku ini menyisipkan situs berbahaya di tautan yang korban klik.

Smishing

Smishing merupakan jenis phishing yang dalam prosesnya pesan teks. Sering kali, bentuk phishing ini melibatkan pesan teks dalam SMS atau nomor telepon. Smishing sangat menakutkan karena kadang-kadang orang cenderung lebih mempercayai pesan teks daripada email. Sebagian besar orang menyadari risiko keamanan yang terlibat dengan mengklik tautan di email. Namun lain hal jika melalui pesan teks.

Biasanya pelaku kejahatan menggunakan cara atau trik agar korban mengklik tautan yang diberikan, menelpon nomor yang tertera, atau membalas pesan tersebut dengan informasi yang pelaku butuhkan. Contohnya yang sering ada di Indonesia yaitu menang undian atau hadiah dari perusahaan besar dan mengatasnamakan diri mereka bagian dari perusahaan tersebut.

Perspektif Undang-Undang Tentang Informasi ...

Whale Phising

Whale phishing adalah istilah yang digunakan untuk menggambarkan serangan phishing yang secara khusus ditujukan untuk individu yang kaya, berkuasa, atau terkemuka. Karena status mereka, jika pengguna seperti itu menjadi korban serangan phishing, ia dapat dianggap sebagai big pish (ikan besar) atau whale (ikan paus). Whale phishing ini pelaku menggunakan taktik yang sama seperti spear phishing.

Data yang terekam di blog Databoks menunjukkan bahwa phishing telah menyebar terutama ke lembaga keuangan. Porsinya naik menjadi 41 persen. Selanjutnya, hingga 32 persen serangan phishing menargetkan e-commerce. Kemudian, hingga 21% serangan phishing menargetkan media sosial. Sementara itu, hanya 6% serangan phishing yang menargetkan pencurian data di game online dan akun cryptocurrency. Banyaknya laporan phishing juga dipengaruhi oleh rendahnya tingkat kesadaran masyarakat. Faktor lainnya adalah pelaku phishing saat ini dapat menggunakan lebih dari satu domain, sehingga menghasilkan lebih banyak laporan.²

Berdasarkan permasalahan diatas, guna menunjang penelitian agar dapat mengkaji permasalahan dengan baik, maka penelitian ini difokuskan kepada beberapa masalah yang akan dikaji, sebagai berikut:

1. Bagaimana bentuk pemidanaan terhadap pelaku tindak pidana cyber crime dalam bentuk phishing di indonesia?
2. Bagaimana perlindungan hukum bagi pelaku tindak pidana cyber crime dalam bentuk phishing?

² Cindy Mutia Nur "Ada 5 Ribu Serangan Phising Terjadi di RI pada Kuartal II-2022, Ini Lembaga yang Paling Banyak Diincar" [Ada 5 Ribu Serangan Phising Terjadi di RI pada Kuartal II-2022, Ini Lembaga yang Paling Banyak Diincar \(katadata.co.id\)](https://katadata.co.id) di akses pada 17 desember 2022

B. METODE PENELITIAN

Untuk mendapatkan data yang diperlukan dalam penelitian ini, maka penulis menggunakan metode pengumpulan data, yakni: Penelitian Kepustakaan (library research). Sehubungan dengan permasalahan dalam penelitian ini maka pengumpulan data akan dilakukan melalui Penelitian Kepustakaan, dikumpulkan melalui penelitian literatur, yakni dengan mempelajari ketentuan Perundang-undangan tentang izin edar kosmetik dan Peraturan Perundang-undangan lain yang relevan dengan materi penelitian.

C. PEMBAHASAN

1. Bentuk Pidana Terhadap Pelaku Tindak Pidana Cyber Crime Berbentuk Phishing di Indonesia

Sebelum masuk ke inti pembahasan, phishing merupakan kejahatan dimana pelaku yang menyamar sebagai organisasi yang sah, menghubungi korban atau target melalui email, telepon, atau pesan singkat, di mana korban memberikan data pribadi seperti identitas diri, data perbankan, dan nomor kredit yaitu seperti detail kartu dan kata sandi. Setelah target memberikan informasi yang diminta, informasi tersebut digunakan untuk mendapatkan akses ke akun penting yang dapat menyebabkan pencurian identitas dan kerugian finansial.

Phishing sendiri berasal dari kata fishing yaitu menangkap ikan. Layaknya kegiatan memancing, phishing merupakan kejahatan dengan cara berburu atau menggunakan umpan. Umpan yang ditargetkan dengan baik adalah faktor penentu keberhasilan phishing. Memiliki akun phishing adalah kuncinya, karena mirip dengan akun resmi. Dalam hal ini, umpan yang digunakan biasanya adalah umpan palsu yang dibuat menyerupai aslinya. Pesan ini biasanya dikirim oleh orang yang tampaknya berwenang, seperti administrator sistem, pegawai bank, atau pegawai pemerintah. Isi informasinya bermacam-macam, namun biasanya berupa permintaan untuk memperbarui informasi akun yang dimaksud³.

³ Erizka Permatasari "Jerat Hukum Pelaku Phising dan Modusnya" di akses pada desember 2021, <https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnya-cl5050>

Perspektif Undang-Undang Tentang Informasi ...

Indonesia adalah negara hukum sebagaimana yang tertuang dalam pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia. Salah satu pilar terpenting dalam negara hukum adalah perlindungan dan penghormatan terhadap hak asasi manusia. Setiap manusia sejak kelahirannya memiliki hak dan kewajiban yang bebas dan mendasar. Tidak boleh menghilangkan arti atau makna kebebasan dalam pembentukan negara dan pelaksanaan kekuasaan suatu negara. Bahkan saat ini, salah satu ciri dari apa yang disebut sebagai negara gagal adalah ketika negara gagal melindungi dan menegakkan hak-hak rakyatnya.

Menurut Andi Hamzah, pemidanaan sama halnya dengan penjatuhan pidana. Pidana macam bagaimanakah yang akan dijatuhkan oleh hakim kepada orang yang melanggar nilai-nilai itu. Bagaimanakah pelaksanaan pidana itu kepada terpidana dan bagaimanakah membina narapidana sehingga dapat diubah menjadi manusia yang berguna dalam masyarakat Pancasila ini⁴.

Pemidaan terhadap pelaku kejahatan tentunya merupakan hal yang harus dilakukan agar selain memberikan efek jera bagi pelakunya juga merupakan bagian dari upaya negara untuk menegakkan keadilan di negaranya. Suatu perbuatan dapat disebut sebagai kejahatan apabila perbuatan tersebut dilarang dan diancam dengan undang-undang menurut peraturan perundang-undangan yang berlaku, dan suatu perbuatan pidana dapat dipidana apabila perbuatan tersebut mengandung unsur kesalahan sehingga pelakunya dapat dimintai pertanggungjawaban. perbuatannya dengan memberikan hukuman atau hukuman.

Kasus kejahatan dunia maya di Indonesia sebelum adanya UU ITE diadili dengan pasal-pasal yang sesuai dengan unsur-unsur hukum pidana sehingga kriminalisasi terhadap pelaku kejahatan dunia internet akan menggunakan hukum pidana. Dalam hukum pidana, ketentuan pidana dalam perkara kejahatan dunia maya dapat digunakan dalam bentuk phishing berdasarkan Pasal 378 KUHP yang berbunyi: “Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan menggunakan nama atau status palsu, dengan cara Penipuan, atau serangkaian kebohongan, membujuk

⁴ Andi Hamzah, Sistem Pidana dan Sistem Pemidanaan Indonesia, Pradnya Paramita, Jakarta, 1993, h. 9

Perspektif Undang-Undang Tentang Informasi ...

orang lain untuk menyerahkan sesuatu kepadanya, diancam dengan penipuan dan diancam dengan pidana penjara paling lama empat tahun”. Pembentukan peraturan perundang-undangan di dunia cyber pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan, dan kepastian hukum. Sebagai norma hukum cyber atau cyber law akan bersifat mengikat bagi tiap-tiap individu-individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya.

Setelah di sah kan nya UU ITE, Ditinjau dari sistem lamanya ancaman pidana (strafmaat), dalam UU ITE menggunakan stelsel ancaman pidana maksimum sebagaimana digunakan dalam KUHP. Buktinya dalam semua pasal dalam UU ITE yang mengatur ancaman pidana, hanya menyebutkan ancaman pidana penjara dalam jangka waktu paling lama, dan/atau jumlah pidana denda paling banyak. UU ITE tidak menganut sistem ancaman pidana minimum khusus. Berdasarkan pengkajian secara ilmiah alasan pembenar secara filosofis, teoritis, yuridis, dan empiris bahwa dalam bentuk cybercrime kategori tertentu, dan terhadap pelaku dengan karakteristik tertentu dapat dijatuhi pidana sosial (sebagai pengganti pidana penjara) bersamaan dengan pidana denda belum terakomodasi secara tersurat dalam UU ITE⁵.

Seiring dengan perkembangan zaman, ketika internet masuk ke dalam jaringan komputer, maka perbuatan hukum yang berkembang di dalamnya menjadi suatu pengelompokan penanganan menggunakan hukum tersebut, salah satunya adalah phishing. Berdasarkan unsur-unsur phishing dan dalam putusan pengadilan, pengaturan mengenai kejahatan dunia maya berupa phishing tercantum dalam Undang-Undang Republik Indonesia No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam beberapa pasal yang dapat dikenakan antara lain :

1. Pasal 28 ayat (1) menyebutkan bahwa “Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan

⁵ Andri Winjaya Laksana “Pidana Cyber Crime dalam Perspektif Hukum Pidana Positif” JURNAL HUKUM UNISSULA VOL.35 NO.1 (2019) Hlm 12-13.

Perspektif Undang-Undang Tentang Informasi ...

kerugian konsumen dalam Transaksi Elektronik.” jo. Pasal 45 ayat (2) sebagai ketentuan pidananya bahwa “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)”.

2. Pasal 35 menyebutkan bahwa “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” jo. Pasal 51 sebagai ketentuan pidananya bahwa “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)”.

Dari ketentuan diatas dapat dilihat bahwa jenis hukuman yang diberikan adalah pidana pokok berupa pidana penjara dan pidana denda dengan menggunakan stelsel straf maksimum, seperti yang digunakan dalam KUHP. Hakim menentukan hukuman yang akan dikenakan (berapa tahun lamanya pidana penjara dan jumlah banyaknya denda) dengan berdasarkan apa yang tercantum dalam UU ITE. Ketentuan dalam pemidanaan ini juga dilakukan dengan cara menggabungkan sistem alternatif dan sistem kumulatif, dimana hakim mempunyai pilihan apakah dapat dijatuhkan pidana penjara atau pidana denda ataupun keduanya. Terhadap pidana penjara bagi pelaku tindak pidana cyber crime berbentuk phising dilakukan dengan memberikan pembatasan kebebasan bergerak seperti pelaku tindak pidana lainnya yang selanjutnya ditampung dalam lembaga pemasyarakatan dengan diwajibkan menaati segala peraturan yang berlaku di dalamnya dikaitkan dengan tata tertib bagi para narapidana jika melanggar peraturan. Sebagaimana yang tercantum dalam Pasal 1 angka 3 Undang-Undang Negara Republik Indonesia Nomor 12 Tahun 1995 tentang Pemasyarakatan menyatakan bahwa “Lembaga Pemasyarakatan yang selanjutnya

Perspektif Undang-Undang Tentang Informasi ...

disebut lapas adalah tempat untuk melaksanakan pembinaan narapidana dan anak didik pemasyarakatan”.

Jika ditinjau dari sudut filosofis maka akan ada hal-hal yang saling ambivalen (keadaan yang bertentangan) antara lain:

1. Pidana penjara memiliki tujuan untuk menjamin pengamanan terhadap para narapidana, serta memberikan kesempatan bagi para narapidana untuk direhabilitasi.
2. Hakikat fungsi dari penjara seringkali mengakibatkan dehumanisasi pelaku tindak pidana dan akhirnya menimbulkan kerugian-kerugian tersendiri bagi narapidana dikarenakan terlalu lama berdiam di dalam lapas, misalnya ketidakmampuan untuk melanjutkan kehidupan dalam bermasyarakat.

Pemidanaan selanjutnya bagi pelaku tindak pidana cyber crime berbentuk phising, yaitu pidana denda. Pidana denda juga termasuk salah satu pidana pokok yang tercantum dalam Pasal 10 KUHP, dan merupakan urutan pidana paling terakhir dari jenis-jenis pidana pokok yang berarti pidana denda yaitu jenis pidana pokok yang paling ringan diantara yang lain. Pidana denda berbeda dengan jenis pidana penjara yang mempunyai tujuan untuk penghilangan kemerdekaan, sedangkan pidana denda tujuannya yaitu harta benda dari pelaku tindak pidana. Karena, denda merupakan aturan dengan menitikberatkan pada keharusan untuk membayar sesuatu dalam bentuk uang karena melanggar suatu aturan yang berlaku dalam masyarakat.²¹ Pidana denda sebagaimana menjadi bagian dari pemidanaan atau penghukuman bagi pelaku agar dapat membayar sejumlah uang yang telah ditetapkan dalam peraturan perundang-undangan dan dalam putusan pengadilan, disebutkan bahwa ada langkah lain yang dapat ditempuh jika pelaku tidak mampu untuk membayar denda yang dimaksud. Hal tersebut tercatat pada Pasal dalam KUHP sebagai berikut, yaitu:

1. Pasal 30 ayat (2) KUHP menyebutkan bahwa, “Jika pidana denda tidak dibayar, ia diganti dengan pidana kurungan”.

Perspektif Undang-Undang Tentang Informasi ...

2. Pasal 30 ayat (3) menyebutkan bahwa, “Lama pidana kurungan pengganti paling sedikit satu hari dan paling lama enam bulan”.
3. Pasal 30 ayat (6) yaitu “Pidana kurungan pengganti sekali-kali tidak boleh lebih dari delapan bulan”.

Tindak pidana cyber crime berupa phising menggunakan UU ITE, serta pemidanaan menurut UU ITE menggunakan kombinasi sistem kumulatif dan alternatif sehingga hakim harus menentukan pemidanaan antara hanya pidana penjara, denda saja atau kedua-duanya. waktu yang sama. Namun lebih lanjut, dalam ketentuan RUU KUHP Pasal 80 ayat (1) disebutkan bahwa, “Dalam menjatuhkan pidana denda, hakim harus mempertimbangkan kemampuan terdakwa dengan memperhatikan pendapatan dan pengeluaran yang sebenarnya dari terdakwa.” Karena subjek hukum yang wajib memenuhi denda dalam suatu tindak pidana tidak dijelaskan secara tegas dalam peraturan perundang-undangan, maka dapat disimpulkan bahwa pembayaran denda dapat dilakukan oleh orang lain atau pihak ketiga dari pelaku. Ketika denda yang seharusnya diberikan kepada pelaku agar dapat menimbulkan efek jera tidak sepenuhnya dilakukan oleh pelaku sendiri, maka dapat membuat tujuan kriminalisasi cybercrime berupa phising menjadi kurang maksimal⁶.

2. Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Dalam Bentuk Phising

Saat ini kejahatan berkembang dari berbagai bentuk dan bisa terjadi kapan saja bahkan dalam keadaan yang dilihat sudah aman pun pasti ada saja celah masalahnya. Penggunaan teknologi berbasis internet memiliki dampak dari perkembangan teknologi saat ini, seperti pedang bermata dua selain membantu kemajuan masyarakat masuk ke era baru, era 4.0 ini memiliki dampak berbahaya. Seperti yang disebutkan oleh Internet World Stats, sebuah situs web internasional untuk data pengguna internet, populasi negara/regional serta data riset pasar internet bahwa pengguna internet yang berada di Indonesia mencapai urutan ketiga terbanyak dari 34 negara di Asia dengan jumlah 212 juta

⁶ Leticia M. Malunsenge, Cornelis Dj. Massie, Ronald E. Rorie “Penegakan Hukum Terhadap Pelaku dan Korban Tindak Pidana Cyber Crime Berbentuk Phising di Indonesia” Jurnal Leticia . Hlm 2-6.

Perspektif Undang-Undang Tentang Informasi ...

pengguna dari populasi jumlah penduduk yang berjumlah kurang lebih sekitar 276 juta jiwa tercatat pada Juni 2021⁷. Dengan begitu, akhirnya menjadi bukti bahwa semakin lama, masyarakat semakin tidak terlepas dari kemanfaatan internet serta menjadi langkah utama keterikatan pengguna internet dengan ancaman kejahatan di internet yang berpeluang pada peningkatan korban tindak pidana, terlebih pada kasus phising yang jarang mudah dibedakan mengenai keasliannya.

Phising merupakan kejahatan dunia maya di mana seseorang menyamar sebagai lembaga yang sah dan menghubungi korban atau target melalui email, telepon, atau pesan teks, agar ia memberikan data sensitif seperti informasi identitas pribadi, detail perbankan, dan kartu kredit, serta kata sandi. Setelah korban atau target memberikan informasi yang diminta, informasi tersebut kemudian digunakan untuk mengakses akun penting yang dapat mengakibatkan pencurian identitas dan kerugian finansial. Dari definisi Phising, jika dilihat dari cara bekerjanya, phising dilakukan untuk memancing korban ke dalam jebakan phiser. Phiser menggunakan e-mail, spanduk, atau pop-up untuk mengelabui pengguna agar dialihkan ke halaman web palsu tempat pengguna diminta memberikan informasi pribadi. Di sinilah para phiser memanfaatkan ketidakpedulian dan ketidakpedulian pengguna jaringan palsu untuk mendapatkan informasi⁸.

Untuk peraturan perundang-undangan mengenai phising masih belum ada, namun pelaku tindak pidana cyber crime dalam bentuk phising dapat dijerat ketentuan dalam Kitab Undang-Undang hukum Pidana (KUHP) serta UU ITE dan perubahannya. Selain itu penting untuk diketahui bahwa pelaku phising dapat dijerat dengan beberapa tindak pidana, seperti penipuan, manipulasi, penerobosan, dan meindahkan atau mentransfer. Bentuk perlindungan masyarakat merupakan wujud dari pertanggungjawaban negara kepada seluruh masyarakat Indonesia sebagai negara hukum. Untuk perlindungan dari kerugian yang dialami korban, telah disebutkan secara yuridis dimana tercantum dalam:

⁷ Internet World Stats, (<https://internetworldstats.com/asia.htm>, diakses pada 02 Februari 2022, pukul 16.15)

⁸ Muftiadi, Amin. Agustina, Tri Putri Mulyani. Evi, Margaretha. "Studi Kasus Keamanan Jaringan Komputer : Analisis Ancaman Phising terhadap layanan online banking", Jurnal Ilmiah Teknik, Vol. 1, No. 2 tahun 2002: hlm.62.

Perspektif Undang-Undang Tentang Informasi ...

1. Pasal 28 D ayat (1) Undnag-undang 1945 menyebutkan “Setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama.
2. Selanjutnya, dicantumkan lagi dalam Pasal 3 ayat (2) Undang-Undang No. 39 Tahun 1999 Tentang Hak Asasi Manusia yang menyebutkan, “Setiap orang berhak atas pengakuan, jaminan, perlindungan dan perlakuan hukum yang adil serta mendapat kepastian hukum dan perlakuan yang sama di depan hukum.”
3. Pasal 40 ayat (2) UU ITE bahwa “Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan peraturan perundang-undangan.”
4. Pasal 1 angka 8 Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 tahun 2006 tentang Perlindungan Saksi dan Korban, yang menyebutkan “Perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban yang wajib dilaksanakan oleh LPSK atau lembaga lainnya sesuai dengan ketentuan Undang-Undang ini.”

Korban yang dirugikan oleh pelaku tindak pidana phising dapat menuntut ganti rugi. Aturan ganti rugi untuk korban tindak pidana dapat melalui cara penggabungan perkara ganti kerugian, melalui gugatan perbuatan melawan hukum, melalui permohonan restitusi. Adapun perlindungan hukum terhadap korban yang disebutkan oleh Barda Nawawi Arief, bahwa pengertiannya terbagi atas 2 (dua) makna, yaitu:

- 1) Dapat diartikan, sebagai pelindungan hukum supaya tidak menjadi seorang korban tindak pidana.
- 2) Dapat diartikan, sebagai perlindungan agar korban dapat memperoleh jaminan atau santunan hukum dari kerugian yang dialami korban, seperti

Perspektif Undang-Undang Tentang Informasi ...

rehabilitasi, pemulihan keseimbangan batin (seperti: pemaafan), pemberian ganti rugi (seperti: restitusi), kompensasi atau jaminan kesejahteraan sosial⁹.

Korban phising yang pada dasarnya memiliki kebutuhan terhadap pemenuhan kerugian material yang dialaminya, dalam UU Perlindungan Saksi dan Korban atau disebut dengan UUPSK menyebutkan terdapat adanya perlindungan korban dan/atau saksi tindak pidana yaitu dalam bentuk Kompensasi, Restitusi dan Bantuan. Terhadap kerugian materiil bagi korban tindak pidana cyber crime berbentuk phising ini, Restitusi adalah metode yang tepat. Seperti dalam Pasal 1 Angka 11 yang menyebutkan bahwa “Restitusi adalah ganti kerugian yang diberikan kepada Korban atau Keluarganya oleh pelaku atau pihak ketiga.” Pada hakikatnya pengajuan permohonan Restitusi kepada LPSK dapat diajukan sebelum perkara didakwakan, dan setelah perkara memperoleh putusan pengadilan. Dengan ditangani oleh LPSK, untuk mengajukan permohonan Restitusi dari pemohon ke pihak terkait. Untuk perkara yang belum didakwakan, permohonan diajukan kepada penuntut umum agar dapat memuat permohonan kedalam tuntutananya sekaligus, dan untuk perkara yang telah memperoleh putusan pengadilan diajukan kepada pengadilan agar dapat diberikan penetapan¹⁰.

Korban tindak pidana berhak memperoleh restitusi berupa:

1. Ganti kerugian atas kehilangan kekayaan atau penghasilan.
2. Ganti kerugian yang ditimbulkan akibat penderitaan yang berkaitan langsung sebagai akibat tindak pidana; dan/atau
3. Penggantian biaya perawatan medis dan/atau psikologis.

Dilanjutkan dalam Pasal 7A ayat (2) yang menyebutkan bahwa “Tindak pidana sebagaimana dimaksud pada ayat (1) ditetapkan dengan keputusan LPSK”. Keputusan LPSK yang dimaksud yaitu keputusan berdasarkan rapat paripurna LPSK untuk

⁹ Mahesa J. Kusuma, “Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank terhadap Tindak Kejahatan ITE di Bidang Perbankan, Cet 2”, (Bandung: Nusa Media, 2019), hlm.36.

¹⁰ Penetapan pengadilan yaitu ketetapan yang diberikan oleh hakim terhadap suatu permasalahan hukum yang diajukan kepadanya agar dapat diberi ketetapan, yang hanya dihadiri oleh pihak pemohon I dan pemohon II.

Perspektif Undang-Undang Tentang Informasi ...

menyatakan penolakan atau diterimanya permohonan perlindungan bagi korban tindak pidana yang diajukan oleh pemohon. Jika dinyatakan diterima dapat dilimpahkan ke bidang perlindungan untuk masuk ke tahap pemberian perlindungan sebagaimana yang dimaksud dalam permohonan tersebut. Namun, apabila permohonan ditolak LPSK tetap menyampaikan pemberitahuan tersebut kepada pihak pemohon secara tertulis. Akan tetapi, perlindungan hukum yang dimaksud menurut UUPSK ini ialah siapa saja yang mengajukan permohonan perlindungan yang dapat dilindungi ditinjau dari kerugian yang benar-benar dialami oleh korban.

D. PENUTUP

Dari pembahasan yang terdapat dalam artikel ini, kami mengambil kesimpulan bahwa:

1. Bentuk pidana terhadap pelaku phising berupa pidana penjara dan pidana denda. Pidana terhadap pelaku kejahatan merupakan hal yang harus dilakukan agar selain memberikan efek jera bagi pelakunya juga merupakan bagian dari upaya negara untuk menegakkan keadilan di negaranya. Berdasarkan unsur-unsur phishing dan dalam putusan pengadilan, pengaturan mengenai kejahatan dunia maya berupa phishing tercantum dalam Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Perubahan atas Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, beberapa pasal yang dapat dikenakan antara lain:
 - a. Pasal 28 ayat (1) menyebutkan bahwa “Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.” jo. Pasal 45 ayat (2) sebagai ketentuan pidananya bahwa “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)”.
 - b. Pasal 35 menyebutkan bahwa “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan,

Perspektif Undang-Undang Tentang Informasi ...

penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik” jo. Pasal 51 sebagai ketentuan pidananya bahwa “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)”.

2. Sebagai negara hukum, Indonesia wajib melindungi warga negaranya dari berbagai kejahatan, tertama kejahatan siber yang marak akhir-akhir ini serta semakin beragam bentuknya, salah satunya adalah Phising. Pelaku tindak pidana cybercrime dalam bentuk phising dapat dijerat dengan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) serta Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya. Karena, kejahatan phising ini memuat berbagai macam tindak pidana, seperti penipuan, manipulasi, penerobosan, dan memindahkan atau mentransfer. Maka dari itu, terdapat beberapa aturan terkait perlindungan korban yang tertera di bawah ini.
 - a. Pasal 28 D ayat (1) Undnag-undang 1945 menyebutkan “Setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama”.
 - b. Selanjutnya, dicantumkan lagi dalam Pasal 3 ayat (2) Undang-Undang No. 39 Tahun 1999 Tentang Hak Asasi Manusia yang menyebutkan, “Setiap orang berhak atas pengakuan, jaminan, perlindungan dan perlakuan hukum yang adil serta mendapat kepastian hukum dan perlakuan yang sama di depan hukum”.
 - c. Pasal 40 ayat (2) UU ITE bahwa “Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi

Perspektif Undang-Undang Tentang Informasi ...

Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan peraturan perundang-undangan”.

- d. Pasal 1 angka 8 Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 tahun 2006 tentang Perlindungan Saksi dan Korban, yang menyebutkan “Perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban yang wajib dilaksanakan oleh LPSK atau lembaga lainnya sesuai dengan ketentuan Undang-Undang ini”.

DAFTAR PUSTAKA

Jurnal:

- Muftiadi, Amin. Agustina, Tri Putri Mulyani. Evi, Margaretha. (2002). Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising terhadap layanan online banking. *Jurnal Ilmiah Teknik*, Vol. 1, No. 2. Di unduh dari <https://jurnal.arkainstitute.co.id/index.php/hexatech/index>
- Laksana, Andri Winjaya. (2019). Pemidanaan Cyber Crime dalam Perspektif Hukum Pidana Positif. *Jurnal Hukum Unissula* Vol.35 No.1.
- Malunsenge, Leticia M. Massie, Cornelis Dj. Rorie, Ronald E. Penegakan Hukum Terhadap Pelaku dan Korban Tindak Pidana Cyber Crime Berbentuk Phising di Indonesia. *Jurnal Leticia*.
- Fadlian, A. (2022). The Influence of Social Media in Era 4.0 in Criminal Law Study and Implementation of Criminal Sanctions. *IJCLS (Indonesian Journal of Criminal Law Studies)*, 7(2).

Buku:

- Mahesa J. Kusuma, (2019). *Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank terhadap Tindak Kejahatan ITE di Bidang Perbankan*, Cet 2. Bandung: Nusa Media.
- Hamzah, Andi. (1993) *Sistem Pidana dan Sistem Pemidanaan Indonesia*. Jakarta: Pradnya Paramita.

Internet:

- Nastainullah, Ridho. (2022). Ciri-Ciri Phising dan Cara Mengatasinya. (Online).
- Nur, Cindy Mutia. (2022). Ada 5 Ribu Serangan Phising Terjadi di RI pada Kuartal II-2022, Ini Lembaga yang Paling Banyak Diincar. (Online).
- Internet World Stats. Di akses di <https://internetworldstats.com/asia.htm>
- Permatasari, Erizka. (2021) Jerat Hukum Pelaku Phising dan Modusnya. (Online) di akses <https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnya-cl5050>

Peraturan Perundang-Undangan:

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
- Kitab Undang-Undang Hukum Pidana (KUHP)
- Undang-Undang No. 39 Tahun 1999 Tentang Hak Asasi Manusia
- Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) tentang Perubahan atas Undang-Undang Republik Indonesia No. 11 Tahun 2008
- Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 tahun 2006 tentang Perlindungan Saksi dan Korban.