PAMPAS: *Journal Of Criminal*
Volume 1 Nomor 2, 2020
(ISSN 2721-8325)

Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik

Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi

Fakultas Hukum, Universitas Jambi
Author email correspondence:ardisaputra.gulo98@gmail.com

ABSTRAK
Artikel ini membahas cyber crime dalam bentuk phising berdasarkan Undang-Undang tentang Informasi dan Transaksi Elektronik. Penelitian yang digunakan yakni penelitian hukum normatif. Hasil penelitian yang telah dilakukan menunjukan: 1) Pengaturan hukum terhadap cyber crime dalam bentuk phising berdasarkan Undang-Undang tentang Informasi dan Transaksi Elektronik tidak dapat dikenakan Pasal 35 jo Pasal 51 Ayat (1) dan Pasal 28 Ayat (1) jo Pasal 45A Ayat (1). 2) Kebijakan hukum terhadap cyber crime dalam bentuk phising berdasarkan Undang-Undang tentang Informasi dan Transaksi Elektronik adalah dilakukannya perubahan terhadap Undang-Undang tentang ITE dengan merumuskan konsep phising dan merubah isi Pasal 35.

Kata Kunci : *Cyber Crime*; kebijakan hukum pidana; *phising*

ARTICLE HISTORY
Submission: 2020-06-09
Accepted: 2020-10-07
Publish: 2020-10-10

KEYWORDS: *Cyber Crime*; The Criminal Law Policy; *Phising*

ABSTRACT
This article discusses cyber crime in the form of phishing based on the Law on Electronic Information and Transactions. The research used is normative legal research. The results of the research that have been conducted demonstrated that: 1) Legal regulations on cyber crime in the form of phishing based on the Law on Electronic Information and Transactions cannot be subject to Article 35 in conjunction with Article 51 Paragraph (1) and Article 28 Paragraph (1) in conjunction with Article 45A Paragraph (1). 2) the criminal law policy against cyber crime in the form of phishing based on the Law on Electronic Information and Transactions is the amendment of the Law on ITE by formulating the concept of phishing and amending the contents of Article 35.

A. PENDAHULUAN

Dewasa ini teknologi informasi dan komunikasi telah mengalami perkembangan yang begitu pesat didunia, terutama di Indonesia yang tidak mau ketinggalan dalam hal penggunaan dan pemanfaatan kemajuan di bidang teknologi informasi dan komunikasi, hal ini dapat dilihat dari banyaknya masyarakat yang telah menggunakan alat komunikasi dan teknologi seperti komputer atau laptop, handphone, dan internet. Kemajuan teknologi ini telah membantu masyarakat dalam hal berkomunikasi lebih efektif dan memudahkan pekerjaan yang sulit menjadi

lebih sederhana, sehingga penggunaan dan pemanfaatan teknologi informasi dan komunikasi hampir seluruh bidang kehidupan manusia telah menggunakan teknologi.

> Peranan teknologi informasi dan komunikasi di era globalisasi telah menempatkan pada posisi yang amat strategis karena menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu, yang berdampak pada peningkatan produktivitas dan efisiensi. Pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat, dan berkembang dalam tatanan kehidupan baru dan mendorong terjadinya perubahan sosial, ekonomi, budaya, pertahanan, keamanan, dan penegakan hukum.[1]

Satu hal yang menarik adalah bahwa proses globalisasi telah dimulai ketika terjadinya kemajuan dan perkembangan teknologi komunikasi dan informasi. Memang awalnya kehidupan kita adalah komunikasi antar makhluk hidup, khususnya kita sebagai manusia yang tidak sanggup bertahan hidup tanpa komunikasi satu dengan yang lain, sehingga dengan kemajuan dan perkembangan teknologi komunikasi dan informasi tersebut haruslah kita manfaatkan dengan sebaik-baiknya.

> Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan tindak kejahatan-kejahatan baru (cyber crime) sehingga diperlukan upaya proteksi. Dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.[2]

Kejahatan baru pada saat ini yang perlu diperhatikan oleh semua orang, khususnya pemerintah untuk dapat melakukan upaya preventif dan/atau refresif terhadap kejahatan baru ini, yang mana kejahatan tersebut dilakukan didunia maya dan istilah lainnya adalah cyber crime. "Cyber Crime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai the new form of anti-social behavior."[3]

> Cyber Crime (selanjutnya disingkat CC) merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Kekhawatiran demikian terungkap pula dalam makalah Cyber Crime yang disampaikan oleh ITAC (Information Technology Association of Canada) pada International Information Industry Congress (IIIC) 2000 Millenium Congress di Quebec pada tanggal 19 September 2000, yang menyatakan bahwa cyber crime is a real and growing threat to economic and social development around the world. Information

---

1 Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari*, PT. Rineka Cipta, Jakarta, 2009, hlm. 39.

2 *Ibid*., hlm. 39-40.

3 Barda *Nawawi*, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, PT. RajaGrafindo Persada, Jakarta, 2005, hlm. 1.

> technology touches every aspect of human life and so can electronically enabled crime. Sehubungan dengan kekhawatiran akan ancaman/bahaya cyber crime ini karena berkaitan erat dengan economic crimes dan organized crime (terutama untuk tujuan money laundering), Kongress PBB mengenai The Prevention of Crime and the Treatment of Offenders (yang diselenggarakan tiap lima tahun) telah pula membahas masalah ini. Sudah dua kali masalah cyber crime ini diagendakan, yaitu pada Kongres VIII/1990 di Havana dan pada Kongress X/2000 di Wina.[4]

Perbuatan melawan hukum di dunia maya (cyber crime) merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan carding, hacking, penipuan, terorisme, dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas pelaku kejahatan di dunia maya.[5] Perbuatan melawan hukum yang terjadi di dunia maya pasti memiliki suatu hal kenapa seseorang melakukan kejahatan siber, karena patut diketahui bahwa kejahatan siber yang dilakukan tersebut pasti menimbulkan kerugian bagi pihak lain.

> Terdapat dua hal yang menyebabkan timbulnya cyber crime (tindak pidana dunia maya) yaitu teknis dan sosio ekonomi (kemasyarakatan). Pertama, dalam hal teknis. Tidak dapat dipungkiri bahwa kemajuan teknologi(teknologi informasi) dapat berdampak negatif bagi perkembangan masyarakat. Berhasilnya teknologi tersebut menghilangkan batas wilayah negara menjadikan dunia ini begitu sempit. Keterhubungan antara jaringan yang satu dengan jaringan yang lain memudahkan pelaku tindak pidana untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat daripada yang lain. Kelemahan tersebut dimanfaatkan oleh mereka yang tidak bertanggung jawab untuk melakukan tindak pidana. Kedua, dalam hal sosio ekonomi. Tindak pidana dunia maya merupakan produk ekonomi. Isu global yang kemudia dihubungkan dengan tindak pidana tersebut adalah kemananan jaringan (security network).Keamanan jaringan merupakan isu global yang digulirkan berbarengan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Tindak pidana dunia maya berada dalam skenario besar dari kegiatan ekonomi dunia.[6]

Hal yang perlu diperhatikan bahwa cyber crime ini selain dikenal dengan istilah hacking maupun hacker, ada juga istilah lainnya ialah cracking maupun cracker yang mana hal ini mempunyai persamaan dan perbedaan antara hacking dengan cracking. Kejahatan yang dilakukan oleh cracking ataupun cracker salah satunya ialah Phising karena kejahatan ini tujuannya untuk menguntungkan diri sendiri dan tentunya merugikan pihak lain jika menjadi korban dari cyber crime dalam bentuk phising ini.

> Dalam ruang lingkup keamanan komputer, phising adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud

---

4 *Ibid*., hlm. 1-2.

5 Siswanto Sunarso, *Loc.Cit*.

6 Sahuri Lasmadi, "*Tindak Pidana Dunia Maya Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*," Jurnal Ilmu Hukum, 2012, hlm. 40-41.

> untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/*legitimate organization* dan biasanya berkomunikasi secara elektronik.[7]

Phising ini juga biasanya ditujukan kepada pengguna online banking, karena menggunakan isian data (ID) pengguna dan kata sandi, dan tidak menutup kemungkinan untuk ditujukan ke pengguna online lainnya. Ketika pengguna memasukkan isian data pengguna miliknya dan kata sandinya ke form login yang merupakan fake form login maka akan diketahui oleh pelaku cyber crime dalam bentuk phising tersebut.

> Aksi phising ini semakin marak terjadi. Tercatat secara global, jumlah penipuan bermodus phising 42% dari modus selain phising yang dinyatakan dalam website *Anti-Phising Working Group* (*APWG*) dalam laporan bulannya, mencatat ada 12.845 e-mail baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana phising.[8]

Hasil dari laporan mengemukakan jumlah laporan phising yang dikirimkan ke APWG selama kuartal pertama tahun 2018 sekitar 263.538 kasus serangan. Serangan tersebut mengalami peningkatan sekitar 46% dibanding kuartal keempat tahun 2017.[9] Hal ini dapat disimpulkan bahwa cyber crime dalam bentuk phising tersebut sangat banyak terjadi bahkan di seluruh dunia.

Phising ini juga biasanya dilakukan melalui media-media sosial yang terhubung ke jaringan internet seperti melalui email/sms dan website. Modus perbuatannya yang melalui email/sms mengirimkan pesan seperti: Pertama, saya membutuhkan pertolongan anda sekarang, maksud pesannya adalah seseorang mengaku sebagai salah satu kerabat atau teman dan mengatakan membutuhkan pertolongan karena sedang dalam masalah. Kedua, selamat, Anda menang, maksud pesannya adalah seperti anda telah memenangkan lotre dan harus mengklaimnya, tetapi biasanya selalu ada pancingan didalamnya, seperti memasukkan data pribadi ke sebuah website tertentu atau yang sudah dideface untuk mendapatkan hadiah tersebut.

> Banyak informasi diperoleh dari majalah, televisi, atau surat kabar yang memberitakan terjadinya berbagai tindak pidana dengan mempergunakan internet sebagai sarana pendukungnya, sebagai contoh, dalam suatu majalah mingguan diberitakan bahwa fasilitas internet banking Bank Central Asia (BCA) lewat situs www.klikbca.com telah dirusak oleh seorang hacker dengan cara melahirkan lima nama situs plesetan yang mirip situs aslinya. Akibatnya, bila nasabah BCA menggunakan fasilitas internet banking BCA tetapi salah mengetik nama situsnya (www.klikbca.com) ia akan masuk ke situs tiruan. Si nasabah pun tak bisa bertransaksi, sementara Personal Identification

---

[7] Dian Rachmawati, "*Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber*," Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211.

[8] Suhardi Rustam, "*Analisa Clustering Phising dengan K-Means dalam Meningkatkan Keamanan Komputer*," Ilkom Jurnal Ilimiah, Vol. 10 No. 2, 2018, hlm. 175.

[9] Aseh Ginanjar et al., "*Analisis Serangan Web Phising pada Layanan E-commerce dengan Metode Network Forensic Process*," Jutei Edisi, Vol. 2 No. 2, 2018, hlm. 147.

> Number (PIN) miliknya terekam di situs gadungan tadi. Adapun situs tiruan yang dibuat hacker itu adalah: kilkbca.com, wwwklikbca.com, clickbca.com, klickbca.com dan klikbac.com. Di Amerika Serikat, kasus typosite atau situs tiruan telah menimpa *washingtonpost.com*, yang alamat tiruannya menjadi washintonpos.com (tanpa huruf "t") dan situs [10]*Microsoft.com* menjadi micosoft.com (tanpa "r")

Pengetahuan pengguna yang minim terhadap alat teknologi yang digunakan merupakan faktor penyebab terjadinya phising, sehingga pengguna teknologi harus dibekali oleh beberapa pengetahuan tentang pengoperasian sebuah teknologi karena seperti yang dijelaskan diatas bahwa pengetahuan pengguna yang minim menjadi salah satu faktor penyebab terjadinya cyber crime khsususnya dalam karya ilmiah ini adalah phising. Ada sebuah teori yang menyatakan, *crime is product of society its self* artinya bahwa masyarakat itu sendirilah yang menghasilkan kejahatan.[11]

Dewasa ini diperlukannya Peraturan Perundang-Undangan yang mengatur tentang kejahatan didunia maya terutama pada penulisan karya ilmiah ini membahas tentang *cyber crime* dalam bentuk phising tersebut. *Cyber Crime* dalam bentuk phising saat ini di Indonesia dimungkinkan dapat dikenakan Pasal 35 jo Pasal 51 ayat (1) karena phising merupakan kejahatan siber yang membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu. *Cyber crime* dalam bentuk phising ini juga dapat dikenakan Pasal 28 ayat (1) jo Pasal 45A ayat (1) karena phising juga melakukan kebohongan untuk menyesatkan orang lain dimana mengarahkan orang yang dibohongi untuk mengakses sebuah link yang dimana link tersebut ditujukan ke situs palsu dan memberikan suatu perintah untuk memperbarui informasi pribadinya yang rahasia ke dalam situs palsu yang telah dibuat oleh pelaku phising, sehingga informasi pribadinya yang rahasia tersebut diketahui oleh pelaku phising dan menyebabkan orang tersebut mengalami kerugian.

Pasal 35 dan Pasal 28 berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang dirumuskan sebagai berikut:

> Pasal 35
> Setiap Orang dengan sengaja, dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

> Pasal 28

[10] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, PT. Refika Aditama, Bandung, 2010, hlm.

[11] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Bandung, 2010, hlm. 39.

> Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Cyber crime dalam bentuk phising ini merupakan kejahatan siber yang tidak hanya melakukan pemalsuan data pada sebuah website palsu yang tampilannya menyerupai website aslinya, tetapi memiliki suatu tujuan untuk mendapatkan identitas milik orang lain untuk digunakan secara ilegal tanpa diketahui oleh pemilik asli identitas tersebut dan dalam pasal 35 hanya memuat unsur pemalsuan data pada sebuah website yang membuat seolah-olah website tersebut asli namun telah dideface seperti website aslinya dan tidak memuat unsur maksud dan tujuan.

Dapat disimpulkan phising adalah perbuatan yang dilakukan oleh seseorang untuk memancing orang lain untuk memasukkan informasi pribadi rahasia pengguna milik orang itu ke dalam sebuah website yang telah dideface atau diubah mirip dengan yang asli resminya dengan cara menggunakan email yang mengarahkan ke situs web palsu guna mendapatkan informasi pribadi rahasia pengguna orang lain, sehingga muncul sebuah pertanyaan, apakah dalam menangani cyber crime dalam bentuk Phising di Indonesia tidak hanya dikenakan Pasal 35 jo Pasal 51 ayat (1) dan Pasal 28 ayat (1) jo Pasal 45A ayat (1) saja atau dapat berkaitan dengan pasal-pasal yang lain di dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan juga mungkin dapat dikenakan dengan pasal-pasal diluar Undang-Undang Informasi dan Transaksi Elektronik seperti KUHP.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini selain membuat aturan tentang phising, Undang-Undang ini juga membuat aturan terhadap perbuatan-perbuatan kejahatan yang merugikan orang lain yang terjadi didunia maya melalui transaksi elektronik yang dapat diketahui bahwa perkembangan teknologi informasi semakin pesat[12]

Berdasarkan uraian di atas, artikel ini membahas mengenai bagaimana pengaturan hukum terhadap pelaku cyber crime dalam bentuk phising berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan bagaimana kebijakan hukum terhadap cyber crime dalam bentuk phising berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

B. METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif, yakni jenis penelitian hukum yang diperoleh dari studi kepustakaan, dengan menganalisis suatu permasalahan hukum melalui peraturan perundang-undangan, literatur-literatur dan bahan-bahan referensi lainnya.

[12] Sahuri Lasmadi, "Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya," *Jurnal Ilmu Hukum*, 2014, hlm. 3.

C. PEMBAHASAN

1. Pengaturan Hukum Terhadap *Cyber Crime* dalam Bentuk *Phising*

Pengaturan hukum terhadap cyber crime dalam bentuk phising sebelumnya diatur di dalam Pasal 378 KUHP tentang penipuan sebagaimana yang diketahui bahwa phising secara umum merupakan tindakan penipuan. Penipuan yang dirumuskan didalam Pasal 378 KUHP adalah:

> 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 empat tahun.

Beberapa unsur-unsur yang terdapat didalam Pasal 378 KUHP tersebut, yaitu:

1. Barangsiapa
2. Dengan maksud untuk menguntungkan diri sendiri atau orang lain
3. Secara melawan hukum
4. Dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun dengan rangkaian kebohongan
5. Menggerakan orang lain
6. Untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi untang maupun menghapuskan piutang

Berdasarkan unsur-unsur yang telah diuraikan dalam Pasal 378 KUHP tersebut, maka dapat disimpulkan bahwa barangsiapa adalah subjek maksudnya ialah pelaku yang melakukan tindak pidana penipuan. Ada maksud untuk menguntungkan diri sendiri atau orang lain, artinya bahwa ada suatu kesengajaan yang dilakukan sebagai maksud (oogmerk). Selanjutnya perbuatan tersebut dilakukan secara melawan hukum, yang berarti pelaku penipuan itu tidak mempunyai hak sama sekali untuk menikmati keuntungan itu yaitu hasil penipuan tersebut.[13]

Unsur selanjutnya memakai nama palsu seperti mengaku suatu nama yang tentunya dikenal baik oleh orang yang ditipu yaitu si korban. Martabat palsu seperti pelaku penipuan mengaku sebagai seorang kiai, dengan tipu muslihat seperti mengaku akan membelikan suatu barang yang harganya sangat murah kepada yang ditipu yaitu si korban, dan rangkaian kebohongan yang dimaksud adalah segala upaya penipuan seperti menceritakan bahwa pelaku penipuan kenal baik dengan seseorang yang dimana orang yang ditipu mempunyai urusan dengan orang tersebut, lalu meminta uang untuk diserahkan kepada orang yang akan ditemui oleh orang yang ditipu yaitu si korban dengan memberikan uang tersebut kepada pelaku penipuan agar pelaku penipuan tersebut menyerahkan uang itu kepada orang yang mempunyai urusan dengan si korban yaitu orang yang ditipu.[14]

Menggerakan orang lain yang dapat diartikan bahwa dengan cara-cara tersebut pelaku penipuan menghendaki orang yang ditipu tergerak untuk melakukan apa yang

---

[13] Andi Hamzah, *Delik-Delik Tertentu (Speciale Delicten) Didalam KUHP Edisi Kedua*, Sinar Grafika, Jakarta, 2015, hlm. 100.

[14] *Ibid*.

dikehendaki pelaku penipuan dengan menyerahkan suatu barang kepadanya. Untuk memberi utang ataupun menghapus piutang itu adalah bagian inti delik yang bermakna pada delik penipuan, objeknya bisa berupa hak yaitu membuat utang atau menghapus piutang. Menurut Nico Keijzer, delik yang paling tepat untuk orang yang mengutakatik komputer untuk mendapatkan keuntungan ialah Pasal 378 karena meliputi hak. Tetapi, tidak memenuhi unsur mengenai informasi elektronik dan/atau dokumen elektronik salah, oleh karena itu Pasal 378 sebenarnya tidak tepat untuk dikenakan terhadap cyber crime dalam bentuk phising.[15]

Telah disahkannya dan diberlakukannya Undang-Undang ITE yang pada awalnya dibentuk Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan kemudian dibentuk lagi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang telah berlaku sampai saat ini.

Kita mengenal dan menganut asas "*Lex Specialis Derogat Legi Generali*". Berdasarkan asas *lex specialis derogat legi generali*, berarti aturan-aturan hukum yang bersifat khusus dianggap berlaku meskipun bertentangan dengan aturan-aturan hukum yang umum. Dapat disimpulkan bahwa yang berlaku saat ini untuk mengatur tentang bagaimana pengaturan hukum *cyber crime* dalam bentuk phising tersebut saat ini diatur oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena Undang-Undang ini bersifat khusus. Pada saat ini perbuatan phising tersebut diatur pada Pasal 35 jo Pasal 51 ayat (1), yang dirumuskan sebagai berikut:

> Pasal 35
>
> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
>
> Pasal 51
>
> Setiap Orang yang memenuhi unsur sebagaimana dimaksdu dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).
>
> Unsur-unsur yang terdapat di dalam Pasal 35, yaitu:
>
> - 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

Perbuatan phising ini juga tidak hanya membuat sebuah situs yang seolah-olah mirip dengan situs asli yang resmi, namun juga perbuatan phising ini melakukan sebuah tindakan kebohongan untuk menipu atau menyesatkan orang lain sehingga menyebabkan orang tersebut mengalami kerugian karena informasi pribadi rahasia orang itu diketahui oleh pelaku *cyber crime* dalam bentuk phising

[15] *Ibid*., hlm. 101.

tersebut. Oleh sebab itu, perbuatan phising dapat dikenakan Pasal 28 ayat (1) jo Pasal 45A ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah melakukan tindakan kebohongan. Pasal 28 ayat (1) jo Pasal 45A ayat (1) dirumuskan sebagai berikut:

> Pasal 28 ayat (1)
> Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
>
> Pasal 45A ayat (1)
> Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

Berdasarkan uraian unsur-unsur tersebut di atas, jika dikaitkan dengan kasus *phising* yang pernah terjadi yang dilakukan oleh seorang laki-laki bernama Steven Haryanto yaitu seorang *hacker* dan jurnalis. Lelaki asal bandung tersebut dengan sengaja membuat situs asli tapi palsu sebuah layanan internet banking Bank Central Asia (BCA). Steven Haryanto membeli domain-domain dengan nama yang hampir mirip dengan situs asli Internet Banking BCA yaitu "*www.klikbca.com*". Nama-nama domain yang dibelinya adalah dengan nama domain wwwklik-bca.com, klikbca.com, clickbca.com, klickca.com, dan klikbac.com. Tampilan dan isi situs-situs tersebut hampir mirip dengan situs aslinya. Jika nasabah BCA salah mengetik nama domain situs BCA yang asli, maka nasabah tersebut dapat masuk perangkap situs palsu yang telah dibuat oleh Steven Haryanto apalagi nasabah memasukkan informasi pribadinya seperti username dan passwordnya, nomor kartu kredit, Pin, nomor rekening, tanggal lahir, atau nama ibu kandung sehingga Steven Haryanto mengetahui informasi pribadi nasabah tersebut.[16]

Kasus selanjutnya yaitu dialami oleh Amirah, karyawan swasta asal Jakarta, memperoleh sebuah pesan dari Go-Jek, isinya "*Don't share this with anyone (not even Go-Jek). Your verification code for account login*: 11234" Lalu, ada seseorang menghubungi amirah mengatasnamakan Go-Jek dan meminta amirah memberi tahu kode verifikasi tersebut agar akunnya tidak terblokir dan akhirnya amirah memberikan kode tersebut. Kemudian amirah menyesali perbuatannya itu yang menyebabkan saldo G-Pay, dompet digital yang terhubung dalam akun Go-Jek miliknya terkuras. Namun kasus tersebut hampir mirip seperti phising namun modusnya lebih seperti vishing karena menggunakan menggunakan media suara karena pelaku menghubungi si korban.[17]

---

[16] Muh. Alfian, "*Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan*," Jurnal Kosmik Hukum, Vol. 17 No. 2, 2017, hlm. 149-150.

[17] https://www.google.com/amp/s/amp.tirto.id/phising-penipuan-yang-mengancam-semua-akun-digital-dmcS Di akses pada tanggal 28-02-2020, Pukul 14.40.

Berdasarkan kasus diatas, Steven Haryanto dapat dikenakan dengan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena Steven Haryanto memenuhi unsur-unsur didalam Pasal 35 tersebut dengan membuat situs palsu seolah-olah situs aslinya.

Apabila Steven Haryanto setelah membuat situs phising tersebut lalu mengirimkan sebuah email dengan isi sebuah Link URL yang mengarahkan ke website palsunya. Dimana didalam isi email tersebut, si calon korban diperintahkan untuk memperbarui informasi pribadinya. Dan si korban mengikuti arahan isi email tersebut untuk memperbarui Informasi Pribadinya di website phising yang telah ia buat dan Informasi Pribadi Korban diketahui oleh Steven Haryanto, maka Steven Haryanto dapat dikenakan Pasal 28 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah memenuhi unsur-unsur didalam Pasal 28 ayat (1) karena dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Pidana yang dijatuhkan terhadap *cyber crime* dalam bentuk phising adalah dikenakan Pasal yang berlapis yaitu Pasal 28 ayat (1) jo Pasal 45A ayat (1) atau Pasal 35 jo Pasal 51 ayat (1) dan tidak boleh lebih dari maksimum pidana yang terberat ditambah sepertiga, sistem ini dinamakan sistem kumulasi diperlunak[18]. Hal ini dinamakan dengan istilah "*Concursus Realis*". *Concursus Realis* terjadi apabila seseorang melakukan beberapa perbuatan, dan masing-masing perbuatan itu berdiri sendiri sebagai suatu tindak pidana dan tindak pidana yang dilakukan tersebut tidak perlu sejenis bahkan tidak perlu berhubungan satu dengan yang lainnya.[19]

Seperti halnya dengan *cyber crime* dalam bentuk phising melakukan perbuatan melawan hukum yang melanggar Pasal 35 karena telah membuat situs yang seolah-olah mirip dengan situs asli resminya namun situs yang dibuat tersebut situs palsu, namun juga melanggar Pasal 28 ayat (1) dengan melakukan suatu kebohongan untuk mengarahkan korban ke website palsu nya sehingga merugikan orang lain.

Berdasarkan uraian di atas, maka didalam Pasal 28 Ayat (1) jo Pasal 45A Ayat (1) dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah) dan Pasal 35 jo Pasal 51 ayat (1) dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah), dapat ditentukan bahwa pidana yang terberat ada di Pasal 35 jo Pasal 51 ayat (1) yaitu dengan pidana penjara paling lama 12 tahun dan pidana denda paling banyak Rp 12.000.000.000,00, lalu pidana terberat tersebut ditambahkan sepertiga dari masing-masing pidana terberat. Pertama, pidana penjara 12 tahun + (1/3 x 12) = 16 Tahun. Kedua, pidana denda Rp 12.000.000.000,00 + (1/3 x 12.000.000.000) = Rp 16.000.000.000,00 (enam belas miliar rupiah).

Jadi, jika dijumlahkan pidana penjara 6 tahun + 12 tahun = 18 tahun maka penjatuhan pidana penjara tidak diperbolehkan karena melebihi maksimum pidana penjara terberat ditambah sepertiga, oleh sebab itu pidana penjara yang akan dijatuhkan paling lama adalah 16 tahun. Dan pidana denda jika dijumlahkan Rp 1.000.000.000,00 + 12.000.000.000,00 = 13.000.000.000,00 (tiga belas miliar rupiah)

[18] Teguh Prasetyo, *Op.Cit*., hlm. 182.
[19] *Ibid*., hlm. 181.

maka penjatuhan pidana denda tersebut diperbolehkan karena tidak melebihi maksimum pidana denda terberat ditambah sepertiga.

Berdasarkan penjabaran tersebut di atas dapat diambil kesimpulan bahwa pidana yang akan dijatuhkan kepada pelaku phising yang telah melanggar Pasal 28 ayat (1) jo Pasal 45A ayat (1) dan Pasal 35 jo Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah dengan pidana penjara paling lama 16 (enam belas) tahun dan/atau pidana denda paling banyak Rp 13.000.000.000,00 (tiga belas miliar rupiah).

Namun, dapat diketahui bahwa *cyber crime* dalam bentuk phising itu sendiri satu kesatuan antara membuat situs yang seolah-olah dengan situs asli resminya dengan melakukan tindakan kebohongan mengirimkan sebuah email yang isi nya mengarahkan ke situs palsu tersebut, dimana orang yang mengaksesnya diperintahkan untuk memperbarui informasi pribadi rahasianya, dan kemudian informasi pribadi rahasianya diketahui oleh pelaku phising tersebut.

Phising merupakan perbuatan yang melawan hukum, karena telah melakukan suatu tindak pidana yang merugikan orang lain. *Cyber crime* dalam bentuk *phising* ini juga merupakan suatu delik materiil, Mengapa ? Karena dapat dikatakan *phising* merupakan suatu tindak pidana ketika *cyber crime* dalam bentuk *phising* ini perbuatan nya telah merugikan orang lain yaitu informasi rahasia pribadi orang tersebut atau si korban diketahui oleh pelaku *phising*.

Tetapi, dari semuanya yang telah diuraikan di atas. Pasal 35 jo Pasal 51 ayat (1) tidak memuat unsur kebohongan yang merugikan orang lain dan Pasal 28 ayat (1) jo Pasal 45A ayat (1) tidak memuat unsur manipulasi, penciptaan, dan perubahan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, maksudnya tidak memuat unsur seseorang membuat situs yang seolah-olah mirip situs asli resminya.

Oleh sebab itu, telah terjadinya kekaburan hukum mengenai pengaturan hukum terhadap *cyber crime* dalam bentuk *phising* berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

2. Kebijakan Hukum Terhadap *Cyber Crime* Dalam Bentuk *Phising*

Berdasarkan penjelasan di atas, bahwa definisi itu sendiri adalah tindakan penipuan yang menggunakan sebuah email palsu untuk mengarahkan ke sebuah situs website palsu yang tujuannya untuk mengelabui seseorang yang menjadi target sehingga pelaku bisa mendapatkan data pribadi rahasia orang itu yang menyebabkan kerugian pada orang tersebut.

Diketahui bahwa didalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik belum merumuskaan dan/atau menjelaskan konsep tentang *phising* sehingga menyebabkan permasalahan apabila ada seseorang yang melakukan *cyber crime* dalam bentuk *phising* namun belum ada penjelasan mengenai konsep phising tersebut.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik harus

dilakukannya kebijakan hukum terhadap Undang-Undang Tentang ITE tersebut untuk dilakukannya tindakan represif apabila terjadinya cyber crime dalam bentuk phising.

Kebijakan Hukum yang harus dilakukan terhadap Undang-Undang tentang ITE tersebut dengan merumuskan konsep phising serta merubah Pasal 35, Mengapa perlu merubah Pasal 35? Karena Pasal 35 mendekati dengan konsep phising, hanya saja ada beberapa unsur yang tidak dirumuskan didalam Pasal 35 sehingga menyebabkan Pasal tersebut mengalami kekaburan norma.

Hukum tidak dapat dikenakan apabila hukumnya mengalami kekaburan seperti Pasalnya memiliki penafsiran yang bermacam-macam dan/atau konsepnya belum ada. Bagaimana dapat diterapkan suatu aturan terhadap pelaku tindak pidana jika hukumnya tidak tegas dan jelas.

Berdasarkan uraian yang telah dijelaskan di atas, maka Kebijakan Hukum yang dilakukan terhadap Konsep Phising dan Pasal 35 berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah:

1. Konsep *Phising*

   Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan dan perubahan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik. Menggunakan media yang terhubung ke jaringan internet yang berisikan Nama Domain dari Informasi Elektronik dan/atau Dokumen Elektronik yang menggerakkan orang lain untuk mengakses Informasi Elektronik dan/atau Dokumen Elektronik tersebut untuk memasukkan identitas pribadi rahasia ke dalam Informasi Elektronik dan/atau Dokumen Elektronik, sehingga menyebabkan orang tersebut mengalami kerugian.
2. Pasal 35

   Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan Phising mengakibatkan kerugian bagi orang lain.

   Berdasarkan Kebijakan Hukum diatas maka dapat diketahui apa yang dimaksud dengan phising dan bagaimana pengaturannya terhadap cyber crime dalam bentuk phising. Lalu, kita dapat menentukan syarat dapat dikriminalisasikan pelaku *phising* yaitu apabila telah melanggar ketentuan hukum Pasal 35 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena telah dilakukannya kebijakan hukum terhadap Pasal 35 dan kemudian tidak terjadi kembali kekaburan norma didalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Cyber crime* dalam bentuk *Phising* ini juga tidak dirumuskan didalam Rancangan Kitab Undang-Undang Hukum Pidana, mungkin dikarenakan terkait teknologi informasi sehingga tidak diaturnya mengenai *phising*.

D. SIMPULAN

Pengaturan hukum terhadap *cyber crime* dalam bentuk phising berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah tidak dapat

dikenakan sanksi pidana karena di dalam Pasal 35 jo Pasal 51 ayat (1) tidak memuat unsur kebohongan yang merugikan orang lain dan Pasal 28 ayat (1) jo Pasal 45A ayat (1) tidak memuat unsur manipulasi, penciptaan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, maksudnya tidak memuat unsur seseorang membuat situs yang seolah-olah mirip situs asli resminya. Karena phising itu sendiri perbuatan satu kesatuan antara membuat situs yang seolah-olah mirip situs aslinya tetapi situs tersebut palsu dan juga melakukan tindakan kebohongan untuk mengarahkan orang lain mengakses ke situs palsu tersebut untuk memasukkan informasi pribadi rahasia dan kemudian diketahui oleh pelaku phising. Oleh sebab itu, telah terjadinya kekosongan hukum mengenai pengaturan hukum terhadap cyber crime dalam bentuk phising berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Kebijakan Hukum terhadap *cyber crime* dalam bentuk phising berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah dilakukannya perubahan terhadap Undang-Undang tentang ITE tersebut dengan merumuskan konsep phising dengan jelas dan tegas serta merubah isi dan unsur pada Pasal 35 agar kemudian Pasal 35 tersebut dapat diterapkan dan/atau dikenakan terhadap pelaku *cyber crime* dalam bentuk *phising*.

DAFTAR PUSTAKA

Dokumen Hukum

Kitab Undang-Undang Hukum Pidana

Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. LNRI TAHUN 2016 Nomor 251. TLNRI Nomor 5952.

Buku

A'an Efendi et al, *Teori Hukum*, Sinar Grafika, Jakarta, 2016.

Andi Hamzah, *Delik-Delik Tertentu (Speciale Delicten) Didalam KUHP Edisi Kedua*, Sinar Grafika, Jakarta, 2015.

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Bandung, 2010.

Bahder Johan Nasution, *Metode Penelitian Ilmu Hukum*, Cet. 2, CV. Mandar Maju, Bandung, 2016.

Barda Nawawi, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, PT. RajaGrafindo Persada, Jakarta, 2005.

Budi Suhariyatno, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, PT. RajaGrafindo Persada, Jakarta, 2013.

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, PT. Refika Aditama, Bandung, 2010.

Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Kencana, Jakarta, 2014.

Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi*, Cet. 9 Kencana, Jakarta, 2014.

Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, PT. Rineka Cipta, Jakarta, 2009.

Teguh Prasetyo, *Hukum Pidana*, PT. RajaGrafindo Persada, Jakarta, 2013.

Vyctoria, "*Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*," CV. Andi Offset, Yogyakarta, 2013.

Jurnal/Majalah Hukum

Aseh Ginanjar et al., "*Analisis Serangan Web Phising pada Layanan E-commerce dengan Metode Network Forensic Process*," Jutei Edisi, Vol. 2 No. 2, 2018.

Dian Rachmawati, "*Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber*," Jurnal Saintkom, Vol. 13, No. 3, 2014.

Dista Amalia Arifah, "*Kasus Cubercrime di Indonesia*," Jurnal Bisnis dan Ekonomi (JBE), Vol. 18 No. 2, 2011.

Eliasta Ketaren, "*Cybercrime, Cyber Space, dan Cyber Law*," Jurnal Times, Vol. V No. 2, 2016.

Maulvie Yazid A et al., "*Cyber Crime Dengan Metode Phising*," Makalah Stikom Surabaya, 2015.

Mia Haryati Wibowo dan Nur Fatimah, "*Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime*," JOEICT, Vol. 1, No. 1, 2017.

Michael Enrick, "*Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dengan Pengajuan Restitusi*," Jurist-Diction, Vol. 2, No. 2, 2019.

Muh. Alfian, "*Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan*," Jurnal Kosmik Hukum, Vol. 17 No. 2, 2017.

Suhardi Rustam, "*Analisa Clustering Phising Dengan K-Means dalam Meningkatkan Keamanan Komputer*," Ilkom Jurnal Ilimiah, Vol. 10 No. 2, 2018.

Sahuri Lasmadi, "*Tindak Pidana Dunia Maya Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*," Jurnal Ilmu Hukum, Vol. 2 No. 4, 2010.

----------, "*Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya*," Jurnal Ilmu Hukum, 2014.

Internet

http://www.beritabebas.com/definisi/vishing/

https://www.google.com/amp/s/amp.tirto.id/phising-penipuan-yang-mengancam-semua-akun-digital-dmcS

https://amp.hitekno.com/internet/2020/01/14/103000/terkena-email-phising-sekolah-ini-kehilangan-rp-31-miliar