**HERMENEUTIKA** p-ISSN 2337-6368 | e-ISSN 2615-4439
Vol. 6, No. 1, Februari 2022 http://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

# ANALISIS YURIDIS CYBERCRIME TERHADAP PENANGANAN KASUS PHISING KREDIVO

Andrew Christian Banjarnahor[1], Puti Priyana[2]

[1]Universitas Singaperbangsa Karawang, Fakultas Hukum, christianandrew172@gmail.com
[2]Universitas Singaperbangsa Karawang, Fakultas Hukum, puti.priyana@fh.unsika.ac.id

DOI: http://dx.doi.org/10.33603/hermeneutika.v3i2
Diterima: 21 Oktober 2021; Direvisi: 10 Februari 2022; Dipublikasikan: 01 Maret 2022

**Abstrak**: *Seiring dengan perkembangan teknologi internet, menyebabkan munculnya kejahatan, adanya cybercrime membuka peluang bagi para pelaku kejahatan yang beraksi dalam dunia maya yang melakukan kejahatan dengan tersembunyi, terorganisasi, dan lebih rapi serta menembus ruang waktu dengan jangkauan yang sangat luas seperti kejahatan phising yang terjadi pada perusahaan kredivo yang menyebabkan kerugian pada korban pengguna kredivo. Tujuan penulisan ini adalah untuk mengkaji mengenai pengaturan hukum bagi pelaku phising bersumber pada Undang-Undang ITE. Penelitian ini menggunakan metode pendekatan yuridis normatif. Hasil penelitian ini menunjukkan bahwa kebijakan Hukum terhadap tindakan phising berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik pelaku dikenakan Pasal 35 jo Pasal 51 ayat(1), pasal 28 ayat(1) jo Pasal 45A ayat(1), dan dijerat Pasal 30 ayat(3) jo.Pasal 46 ayat(3) atas tindakan penipuan, manipulasi, menyebarkan berita palsu, dan penerobosan.*

**Kata kunci:** *Cybercrime; Hukum; Phising.*

## I. PENDAHULUAN

Sejarah internet berawal pada suatu departemen pertahanan yang dibuat Amerika Serikat pada tahun 1970 yang dinamakan dengan sebutan ARPA*net*, yang dibuat oleh ARPA(*Advanced Research Projects Agency*) berfungsi dalam menghubungi berbagai lokasi baik lokasi milter maupun lokasi riset. Tujuan dari dibuatnya ARPAnet sendiri untuk membangun suatu sistem jaringan yang baik. [1] Akhirnya jaringan tersebut digunakan juga dalam kepentingan Pendidikan tinggi.

Teknologi informatika dan komunikasi telah berkembang demikian pesat. Komputer(*Cyber*) telah memunculkan internet yang menjadikan perubahan baru di bidang media masa. [2] Internet merupakan sebagai jaringan komunikasi digital yang telah menghubungkan jaringan dari hampir seluruh bagian dunia yang sampai sekarang masih digunakan oleh setiap negara.

Perkembangan teknologi di bidang media, informasi, dan komunikasi yang menyebabkan perubahan pada perilaku masyarakat maupun secara global. Berkembangnya teknologi terhadap media, informasi, dan komunikasi menyebabkan perubahan sehingga dapat terhubung dengan dunia luar dengan tanpa adanya batasan sehingga perubahan terjadi secara cepat mengenai ekonomi, budaya serta sarana yang memudahkan masyarakat dalam kehidupan sehari-hari hingga perubahan sosial bagi masyarakat. Teknologi memberikan dampak yang berbeda – beda sebab kehidupan masyarakat sangat bergantung kepada teknologi dalam meningkatkan kesejahteraan, dan kemajuan bagi masyarakat tetapi penyalahgunaan teknologi banyak terjadi yang memberikan dampak negatif dalam suatu penggunaan teknologi sehingga munculnya kejahatan.

Kejahatan yang menggunakan teknologi biasa disebut dengan *cybercrime* dengan menggunakan media internet dan perangkat elektrtonik lainnya. Internet sebagai dampak dari kemajuan teknologi membuka peluang bagi para pelaku kejahatan yang beraksi dalam dunia maya yang melakukan kejahatan dengan tersembunyi, terorganisasi, dan lebih rapi serta menembus ruang waktu dengan jangkauan yang sangat luas. Teknologi sebagai dampak dari bentuk globalisasi menyebabkan kejahatan siber bisa dilakukan dimana pun oleh para pelaku kejahatan yang berada di dalam maupun diluar wilayah yuridiksi negara korban.

*Cybercrime* dalam bentuk *phising* adalah suatu kejahatan kejahatan siber yang membuat pemalsuan data di suatu *website* palsu yang tampilannya mirip dengan *website* aslinya, tetapi mempunyai tujuan yang sama untuk mendapatkan informasi mengenai indentitas orang lain yang akan digunakan dengan illegal tanpa sepengetahuan pemilik asli tersebut.[3] Pasal 35 Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang memuat unsur pemalsuan data suatu *website* yang seolah-olah membuat *website* terlihat seperti asli tetapi telah diubah *hacker*/peretas yang tidak terdapat tujuan dan maksud hanya digunakan untuk meretas data.

Seperti dalam kasus yang terjadi pada Kredivo yang penyebabnya adalah *phising*. Beberapa pengguna Kredivo menjadi korban tindak pidana siber *phising*. Pengguna kredivo masuk kedalam perangkat *hacker* setelah dihubungi oleh oknum yang mengiming-imingkan promo,

[1] Alcianno G. Gani. (2018). "*Pengenalan Teknologi Internet serta dampaknya*". Jurnal Universitas Suryadarma. hlm 72

[2] Ketaren, Abdurrahman Harit'S. "*Analisis Yuridis Tindak Pidana Cybercrime dalam Perbuatan Pidana Pencemaran Nama Baik Ditinjau dari Undang-Undang No. 8 Tahun 2011 Tentang Informasi Transaksi dan Elektronik dan Hukum Pidana*." (2018).

[3] Mia Haryati Wibowo,Nur Fatimah, "*Ancaman phising terhadap pengguna sosial media dalam dunia Cyber Crime*", Jurnal of Education and Information Communication Technology, Volume 1, Nomor 1, 2017, hlm. 1.

bonus hingga hadiah. Yang dimana korban malah mendapatkan biaya tagihan yang membesar dari pembelian barang melalui Bukalapak(*e-commerce*). Pakar IT dan *Internet Security* sekaligus pengajar di ITB, menjelaskan bahwa fakta pelaku mengetahui data pribadi korban melalui panggilan telepon. Pelaku memastikan nama dan nomor telepon korban sesuai untuk melakukan *hack* serta memberikan *web phising*.[4] Kebocoran data bisa terjadi Ketika dalam keadaan *offline* maupun *online* yang contohnya secara *offline* korban tidak sengaja mengisi data diri di layanan Lembaga keuangannya di selembar kertas pada saat mendaftar yang kemudian hilang yang dimanfaatkan pelaku untuk mengambil data diri korban dan secara *online* korban mengunjungi halaman situs *phising* untuk mengisi data diri.

Dalam kasus ini dapat dilihat *hacker* menggunakan modus melakukan *phising* dengan cara:

1. *Phising* melalui telepon
   Pelaku menggunakan telepom yang mengatas namakan pihak bersangkutan. Menanyakan maupun meminta hal yang bersifat pribadi baik *user id* maupun *password* yang digunakan korban serta kode OTP yang digunakan pelaku dalam mengakses *handphone* yang digunakan korban
2. *Web Forgery*
   Situs web yang dibuat oleh pelaku yang digunakan untuk menipu korban dengan tampilan yang sangat mirip dengan *website* aslinya. Digunakan pelaku untuk mengetahui *user id* maupun *password* korban yang biasanya korban diharuskan mengisi data diri di *website* palsu tersebut. Data yang telah dimasukkan korban lah yang akan dimanfaatkan pelaku untuk disalah gunakan.[5]

Berdasarkan pada uraian tersebut, maka pembahasan yang akan dipaparkan di artikel ini adalah bagaimanakah pengaturan hukum bagi pelaku phising bersumber pada Undang-Undang ITE.

## II. METODE PENELITIAN

Metode pendekatan yang digunakan dalam penelitian ini adalah metode pendekatan yuridis normatif, spefikasi penelitian yang digunakan yaitu deskriptif. Penarikan kesimpulan dari hasil penelitian ini dilakukan dengan metode analisis normatif kualitatif. Normatif yaitu menggunakan sumber data sekunder saja yaitu peraturan perundang-undangan, teori-teori hukum dan pendapat-pendapat para sarjana terutama. Kualitatif karena merupakan proses analisis data tanpa menggunakan rumus dan angka-angka yang berasal dari informasi-informasi hasil kepustakaan yaitu data yang diambil dari instansi-instansi terkait maupun hasil pengamatan dalam penelitian yang dilakukan dengan masalah yang dibahas tersebut.[6]

## III. HASIL PENELITIAN

Dalam kasus *phising* yang terjadi pada kredivo sangat berdampak bagi banyak pihak baik korban maupun perusahaan kredivo. Dalam pengaturan hukum bagi pelaku *phising* yang diatur dalam Pasal 378 KUHP mengenai penipuan yang terbagi menjadi beberapa unsur, yakni:[7]

a) Barang siapa: pelaku yang melakukan penipuan

[4] Aziz Rahardyan (2021). "*Kredivo Lapor Kasus Cybercrime ke Polisi, Tagihan Pengguna Bengkak Gara-gara Promo Fiktif*". (*Online*) https://finansial.bisnis.com/read/20211224/563/1481571/kasus-phising-kredivo-pengamat-pelaku-manfaatkan-kebocoran-data

[5] Erizka Permatasari (2021)." *Jerat Hukum Pelaku Phishing dan Modusnya*". (Online) https://www.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-iphishing-i-dan-modusnya

[6] Holyness N. Singadimedja, "*Analisis Yuridis terhadap Politik Hukum Kewenangan Pengawas Ketenagakerjaan: Desentralisasi atau Resentralisasi Berdasarkan UU Nomor23 Tahun 2014 tentang Pemerintahan Daerah"*, Jurnal Ilmiah Hukum, Volume 2, Nomor 2, September, 2017, hlm. 5.

[7] Kitab Undang-Undang Hukum Pidana

b) Dengan maksud untuk membuat untung dirinya maupun orang lain: maksud yang menjadi kesengajaan melakukan
c) Secara melawan hukum: pelaku tidak memiliki hak dalam mengambil dan menikmati keuntungan dari korban penipuan
d) Menggunakan nama palsu atau kedudukan palsu, dengan berbagai tipu muslihat serta rangkaian kebohongan: nama palsu yang merupakan kenalan baik korban sedangkan kedudukan palsu seperti penipuan dengan mengatasnamankan pihak dari perusahaan yang menawarkan bonus, promo maupun hadiah.
e) Menggerakan orang lain: pelaku mengarahkan korban untuk melakukan sesuatu yang diinginkan pelaku seperti menyerahkan sesuatu.
f) Penyerahan suatu barang atau untuk memberi hutang atau penghapusan piutang: pelaku memperoleh objek dari penipuan yang dapat digunakan membuat utang maupun menghapus piutang.

Didalam Undang-Undang No.19 Tahun 2016 mengenai perubahan atas Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Perbuatan *phising* dilakukan diatur dalam pada Pasal 35 jo Pasal 51 ayat(1), yang dijelaskan sebagai berikut:[8]

- Pasal 35 bahwa "Setiap orang yang melakukan secara sengaja dan tanpa hak atau perbuatan secara melawan hukum, memanipulasi, menciptakan, perubahan, menghilangkan, pengrusakan suatu informasi elektronik ataupun dokumen elektronik dengan tujuan supaya dianggap seolah-oleh merupakan data otentik".
- Pasal 51 bahwa "Setiap orang yang memenuhi pasal 35 maka dipidana dengan pidana penjara paling lama 12(dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00(dua belas miliar rupiah).

Perbuatan pelaku juga bukan hanya membuat situs palsu yang seolah-olah menyerupai *website* asli namun juga berbohong untuk menipu korban sehingga banyak korban yang mengalami kerugian dikarenakan informasi pribadi diketahui oleh pelaku *phising* sehingga dapat dikenakan pasal 28 ayat(1) jo Pasal 45A ayat(1) Undang-Undang No.19 Tahun 2016 mengenai perubahan atas Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik atas tindakan kebohongan.

a. Pasal 28 ayat(1) bahwa"Setiap orang yang melakukan secara sengaja, dan tanpa kewenangan menyebarkan kabar hoaks dan sesat yang menyebabkan kerugian bagi pengguna dalam transaksi elektronik".
b. Pasal 45A ayat(1) bahwa"Setiap orang yang memenuhi pasal 28 ayat(1) maka dipidana dengan pidana penjara paling lama 6(enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00(satu miliar rupiah)

Pelaku juga melakukan penerobosan data untuk menggunakan indentitas juga *password* korban tanpa sepengetahuan korban, sehingga dapat dijerat Pasal 30 ayat(3) jo.Pasal 46 ayat(3) Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik [9] yang disimpulkan sebagai berikut:

Setiap orang yang melakukan secara sengaja, dan tanpa kewenangan maupun melawan hukum dalam mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos,atau menjebol sistem keamanan maka dipidana dengan penjara paling lama 8(delapan) tahun dan/atau

[8] Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

[9] Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik

denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Dapat dilihat bahwa pelaku *phising* melakukan penipuan dengan mengiming-imingkan promo, bonus hingga hadiah, manipulasi dengan mengirimkan email yang seolah-olah berasal dari perusahaan kredivo, menyebarkan berita palsu dengan membuat suatu perubahan dokumen elektronik biar seolah-olah berasal dari perusahaan kredivo, dan penerobosan dengan menggunakan data kredivo korban untuk melakukan dari pembelian barang melalui Bukalapak(*e-commerce*).

## IV. KESIMPULAN

Pengaturan hukum pada tindak pidana cybercrime *phising* dengan bersumber kepada Undang-Undang No.19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik adalah dapat dikenakan sanksi pidana kepada pelaku *phising* dikarenakan di dalam Pasal 35jo. Pasal 51 ayat (1) yang mempunyai unsur kebohongan yang membuat kerugian bagi korban dan Pasal 28 ayat (1)jo.

Pasal 45A ayat (1) yang mempunyai unsur manipulasi, penciptaan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap menyerupai data yang asli dan mirip situs asli resminya serta Pasal 30 ayat(3) jo.Pasal 46 ayat(3) Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik penerobosan dengan menerobos sistem keamanan korban. Dalam kasus ini pelaku *phising* telah memenuhi dinyatakan bersalah dan memenuhi unsur "barang siapa", "dengan maksud untuk membuat untung dirinya maupun orang lain","secara melawan hukum", "menggerakan orang lain", dan "penyerahan suatu barang atau untuk memberi hutang atau penghapusan piutang" atas tindakan pidana *cybercrime*.

## REFERENSI

Gani, Alcianno G. (2018). "Pengenalan Teknologi Internet serta dampaknya". Jurnal Universitas Suryadarma. hlm 72

Ketaren, Abdurrahman Harit'S. "Analisis Yuridis Tindak Pidana Cybercrime dalam Perbuatan Pidana Pencemaran Nama Baik Ditinjau dari Undang-Undang No. 8 Tahun 2011 Tentang Informasi Transaksi dan Elektronik dan Hukum Pidana." (2018).

Wibowo Mia Haryati, Fatimah Nur. "Ancaman phising terhadap pengguna sosial media dalam dunia Cyber Crime", Jurnal of Education and Information Communication Technology, Volume 1, Nomor 1, 2017, hlm. 1.

Rahardyan, Aziz (2021). "Kredivo Lapor Kasus Cybercrime ke Polisi, Tagihan Pengguna Bengkak Gara-gara Promo Fiktif". (Online) https://finansial.bisnis.com/read/20211224/563/1481571/kasus-phising-kredivo-pengamat-pelaku-manfaatkan-kebocoran-data

Permatasari Erizka (2021)." Jerat Hukum Pelaku Phishing dan Modusnya". (Online) https://www.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-iphishing-i-dan-modusnya

Singadimedja Holyness N, "Analisis Yuridis terhadap Politik Hukum Kewenangan Pengawas Ketenagakerjaan: Desentralisasi atau Resentralisasi Berdasarkan UU Nomor23 Tahun 2014 tentang Pemerintahan Daerah", Jurnal Ilmiah Hukum, Volume 2, Nomor 2, September, 2017, hlm. 5.

Kitab Undang-Undang Hukum Pidana

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

Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik