PERLINDUNGAN HUKUM BAGI KORBAN TINDAK PIDANA *CYBER CRIME PHISHING*

Oleh

Khanifah Jannatul Diniyah
Fakultas Hukum Universitas Islam Malang
Jl. Mayjen Haryono Nomor 193, Kota Malang
*khanifahjd@gmail.com

ABSTRACT

This research is motivated by the rise of cases of phishing circulating in the community.cases Phishing circulating in the community are very detrimental, both material and moral losses. The legal issue raised in this research is how to regulate cyber crime phishing in Indonesia and a form of legal protection for its victims. This research is a normative juridical law research through a statutory approach, a conceptual approach and a case approach. The collection of legal materials is done through the literature study method. Sources of legal materials consist of primary, secondary and tertiary legal materials. The legal material obtained is then analyzed and processed to be compiled systematically. The results of the study indicate that the regulation of cyber crime phishing is regulated in the Criminal Code and the ITE Law, and legal protection can be obtained from Article 378 of the Criminal Code, Article 28 paragraph (1) and Article 35 of the ITE Law and Article 40 of Law Number 36 of 1999 concerning Telecommunications.

Keywords*: Legal Protection, Crime, Cyber crime, Phishing*

ABSTRAK

Penelitian ini dilatarbelakangi oleh maraknya kasus-kasus *phishing* yang beredar di masyarakat. Kasus-kasus *phishing* yang beredar di masyarakat sangat merugikan, baik itu kerugian secara materil maupun moril. Isu hukum yang diangkat dalam penelitian ini adalah bagaimana bentuk pengaturan tindak pidana *cyber crime phishing* di Indonesia dan bentuk perlindungan hukum bagi korbannya. Penelitian ini merupakan penelitian hukum yuridis normatif melalui pendekatan perundang-undangan, pendekatan konseptual dan pendekatan kasus. Pengumpulan bahan hukum dilakukan melalui metode studi literatur. Sumber bahan hukum terdiri dari bahan hukum primer, sekunder dan tersier. Bahan hukum yang diperoleh kemudian dianalisis dan diolah untuk disusun secara sistematis. Hasil penelitian menunjukkan bahwa pengaturan tindak pidana *cyber crime phishing* diatur dalam KUHP dan UU ITE, serta perlindungan hukum dapat diperoleh dari pasal 378 KUHP, Pasal 28 ayat (1) serta pasal 35 UU ITE dan pasal 40 UU Nomor 36 Tahun 1999 tentang Telekomunikasi.

Kata Kunci: Perlindungan Hukum, Tindak Pidana, *Cyber crime, Phishing*

PENDAHULUAN

Dalam era modern seperti sekarang ini, internet merupakan suatu hal yang tidak dapat dipisahkan dalam kehidupan sehari-hari di masyarakat. Keberadaan internet tentu saja semakin memudahkan kehidupan. Banyak hal yang dapat dilakukan dengan internet. Misalnya sebagai sarana komunikasi, *e-money*, *internet banking*, dan masih banyak lagi. Internet sudah menjadi kebutuhan hidup di hampir sebagian besar masyarakat. Seiring dengan semakin populernya internet, masyarakat penggunanya seakan-akan mendapati suatu dunia baru yang dinamakan *cyber space*. Alam baru yang terbentuk oleh media internet ini pada perkembangannya menciptakan masyarakat baru yang sering disebut sebagai *netizen*.[1]

Disamping banyaknya manfaat serta kemudahan yang didapatkan dari penggunaan internet, tak jarang pula terdapat hal negatif yang ditimbulkan dari penggunaan internet ini sendiri. Untuk melindungi dan menghormati hak-hak masyarakat dibidang kebebasan serta memberikan keadilan yang merata bagi seluruh masyarakat dengan pertimbangan keamanan dan ketertiban umum, kemudian dibentuklah Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik agar terwujud keadilan, ketertiban umum, dan kepastian hukum.

UU ITE bermaksud untuk melindungi hak dan kewajiban bagi para pengguna internet. Karena kejahatan tidak hanya ada pada dunia nyata tetapi juga di dunia maya. Kejahatan yang dilakukan dengan media internet ini dikenal pula dengan istilah *cyber crime*. *Cyber crime* sendiri adalah suatu bentuk kejahatan yang dilakukan menggunakan jaringan komputer sebagai unsur utamanya. Hingga hari ini kasus kejahatan di dunia maya (*cyber crime*) semakin bertambah, modusnya pun makin beragam, serta makin bervariasi karateristik pelaku

[1] Ki Jagad Tomara (2013), Skripsi Fakultas Hukum Universitas Brawijaya, Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs *Phishing*, hlm 3

kejahatannya, dan makin serius akibatnya.[2] Bentuk kejahatan di dunia maya atau *cyber crime* bermacam-macam, berikut uraiannya:

1. Pertama: mengandung kekerasan (*cyber crime with violence*), diantaranya adalah:
   a. *Cyber terrorism*, *Assault by Threat* (serangan terorisme dunia maya),
   b. *Cyber stalking* (penguntitan dunia maya),
   c. *Child Pornography* (pornografi pada anak).
2. Kedua: tanpa kekerasan (*cyber without violence*), diantaranya adalah:
   a. *Cyber trespass* (memasuki jaringansecara ilegal),
   b. *Cyber thief* (pencurian dunia maya),
   c. *Cyber fraud* (penipuan dunia maya),
   d. *Destructive Cyber crimes* (perusakan jaringan),
   e. *Cyber Prostitute Ads* (iklan prostitusi online),
   f. *Cyber gambling* (perjudian online),
   g. *Cyber Drugs Sales* (penjualan obat & narkotika di internet),
   h. *Cyber Laundering* (pencucian uang),
   i. *Cyber Phishing* (pencurian data pribadi antara lain berawal dari penipuan berupa link/situs web site).[3]

Phishing merupakan salah satu kejahatan maya paling populer. Melansir artikel bebas *Phishing*.org dalam salah satu esainya yang berjudul What is *Phishing*?, *Phishing* didefinisikan sebagai kejahatan dunia maya di mana seseorang yang menyamar sebagai institusi resmi pemerintah mendekati korban/target melalui email, telepon, atau pesan teks, meminta data sensitif seperti informasi identitas pribadi, informasi perbankan dan kartu kredit, serta kata sandi. Informasi tersebut kemudian digunakan untuk mendapatkan akses ke akun sensitif

[2] Widodo (2013), Memerangi Cybercrime Karateristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi, Asswaja Pressindo, Yogyakarta, hlm, 1.

[3] Hilman Mursidi (2019), Skripsi Fakultas Hukum Universitas Sriwijaya, Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Cyber crime Phishing* (Studi Kasus Putusan Pengadilan Negeri Medan Nomor : 3006/Pid.Sus/2017/PN.Mdn), hlm 5

seperti bank, data pribadi, yang berpotensi mengakibatkan pencurian identitas dan kerugian finansial.[4]

Pengaruh kemajuan dari penjelasan diatas, Teknologi Internet mampu mengubah berbagai pola-pola yang sudah mapan dalam suatu tindak pidana dengan kata lain modus operandi yang umumnya dilakukan dalam kejahatan konvesional melalui teknologi internet telah diubah menjadi modus operandi yang sifatnya baru, sehingga hal ini mengakibatkan perlunya ditemukan upaya-upaya penanganan yang baru pula.[5]

Perkembangan teknologi serta perkembangan masyarakat telah membawa perubahan pada pola hidup masyarakat, sehingga hukum perlu untuk mengikutinya. Oleh karena itu diatur pula mengenai hukum pidana khususnya mengenai tindak pidana yang kemudian disertai dengan ancaman sanksi pidananya. Pemberian sanksi dilakukan sesuai dengan ketentuan pidana yang berlaku menurut undang-undang yang bersangkutan.

Pidana selain dimaksudkan untuk memberikan penderitaan kepada pelaku tindak pidana serta memberikan efek jera kepada pelakunya, juga dapat digunakan sebagai peringatan kepada masyarakat agar tidak melakukan kejahatan yang serupa serta senantiasa waspada dan berhati-hati dalam bertingkah laku.

Di Indonesia sendiri kejahatan di dunia maya sudah diatur dalam suatu undang-undang khusus, yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektornik. Didalam undang-undang ini telah diatur berbagai hal yang berkaitan dengan suatu informasi elektronik berserta kriteria-kriterianya.

Berdasarkan latar belakang tersebut, penulis merasa perlu untuk mengkaji dan menganalisis permasalah sebagai berikut: 1. Bagaimana pengaturan tindak pidana *Cyber crime Phishing* di Indonesia? 2. Bagaimana perlindungan hukum bagi korban tindak pidana *Cyber crime Phishing*?

Adapun tujuan dari penulisan penelitian ini adalah: 1. Untuk mengetahui bagaimana bentuk pengaturan tindak pidana *cyber crime phishing* di Indonesia. 2.

[4] Jerat Hukum Pelaku *Phishing* dan Modusnya, diakses pada Rabu 26 Mei 2021 dari: https://www.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-i*phishing*-i-dan-modusnya/

[5] Hilman Mursidi, *op cit*

Untuk mengetahui bagaimana bentuk perlindungan hukum bagi korban tindak pidana *cyber crime phishing*. Manfaat diberikan dari penelitian ini yaitu penulis berharap agar penelitian ini dapat bermanfaat untuk menambah serta memperluas wawasan di bidang hukum pidana mengenai perlindungan hukum bagi korban tindak pidana *Cyber crime Phishing*. Manfaat selanjutnya yaitu penulis berharap agar penelitian ini dapat bermanfaat untuk menambah serta memperluas wawasan di bidang hukum pidana mengenai perlindungan hukum bagi korban tindak pidana *Cyber crime Phishing*.

II. METODE PENELITIAN

Pengertian sederhana dari metode penelitian adalah tata cara bagaimana melakukan penelitian. Metode penelitian membicarakan mengenai tata cara pelaksanaan penelitian.[6] Penulis dalam menyelesaikan penelitian ini menggunakan jenis penelitian yuridis normatif. Penelitian hukum normatif diartikan sebagai penelitian atas aturan-aturan perundangan, baik ditinjau dari sudut hierarki perundang-undangan (vertikal) maupun hubungan harmoni perundang-undangan (horizontal).[7] Penelitian ini menggunakan 2 macam pendekatan, yakni pendekatan perundang-undangan *(statute approach*) dan pendekatan konseptual (*conseptual approach*). Penelitian hukum normatif disebut juga penelitian kepustakaan atau studi dokumen, karena penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan tertulis atau bahan-bahan hukum yang lain.[8] Bahan hukum yang digunakan dalam penelitian ini adalah bahan hukum primer, sekunder dan tersier.

Bahan hukum primer merupakan bahan hukum yang bersifat autoratif, artinya, mempunyai otoritas. Bahan hukum terdiri dari perundang-undangan, catatan-catatan resmi.[9] Bahan hukum sekunder adalah dokumen atau bahan hukum yang memberikan penjelasan terhadap bahan hukum primer seperti buku-

[6] Jonaedi Efendi, Johnny Ibrahim, 2018, Metode Penelitian Hukum Normatif dan Empiris, Prenada Media, Jakarta, hlm 2

[7] Elisabeth Nurhaini Butarbutar, 2018, Metode Penelitian Hukum, Refika Aditama, Bandung, hlm 83

[8] *Ibid,* hlm 84

[9] Suratman dan Phillips Dilla, 2015, Metode Penelitian Hukum, Alfabeta Bandung, Bandung hlm 65

buku, artikel, jurnal, hasil penelitian, makalah dan lain sebagainya yang relevan dengan permasalahan yang akan dibahas.[10] Sedangkan Bahan hukum tersier sebagai bahan hukum yang memberikan petunjuk dan penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus, maupun ensiklopedi.[11]

Bahan hukum dikumpulkan melalui prosedur inventarisasi dan identifikasi peraturan perundang-undangan, serta klasifikasi dan sistematisasi bahan hukum sesuai permasalahan penelitian. Oleh karena itu, teknik pengumpulan bahan hukum yang digunakan dalam penelitian ini adalah dengan studi kepustakaan.[12] Studi kepustakaan merupakan suatu metode penelitian yang menggunakan dokumen sebagai sumber datanya. Adapun sumber informasinya dapat berupa jurnal hukum, hasil dari penelitian hukum, laporan, dan berbagai literatur yang relevansi dari beberapa buku yang berkaitan dengan rumusan masalah penelitian ini. Bahan hukum yang diperoleh kemudian dikumpulkan dengan menggunakan studi dokumentasi.

Data yang diperoleh dalam penelitian ini dianalisis secara deskriptif kualitatif. Deskriptif maksudnya pengambilan data yang diperoleh dari hasil penelitian bahan hukum diolah dan disusun secara sistematis dan diuraikan, sehingga diperoleh gambaran yang jelas dan lengkap tentang obyek penelitian. Sedangkan kualitatif maksudnya data yang diperoleh dipisah-pisahkan, diambil yang memiliki relevansi dengan permasalahan untuk kemudian dikaji lebih lanjut dan disusun secara sistematis sehingga diperoleh kesimpulan.[13]

PEMBAHASAN

Pengaturan Tindak Pidana *Cyber crime Phishing* di Indonesia

Kitab Undang-Undang Hukum Pidana Indonesia telah memberikan pengaturan yang jelas mengenai batas-batas berlakunya aturan perundang-

[10] Pengenalan Bahan Hukum, diakses pada Kamis 27 Mei 2021 dari https://simdos.unud.ac.id/uploads/file_penelitian_1_dir/7847bff4505f0416fe0c446c60f7e8ac.pdf

[11] *Ibid*

[12] Metode Penulisan, diakses pada Kamis 27 Mei 2021 dari: http://repository.umy.ac.id/bitstream/handle/123456789/23062/BAB%20III.pdf?sequence=4&isAllowed=y

[13] Metode Analisis Bahan Hukum, diakses dari http://repository.ub.ac.id pada Minggu, 26 September 2021

undangan hukum pidana. Hal ini diatur dalam Bab I Buku Kesatu Kitab Undang-Undang Hukum Pidana yang terdiri dari sembilan pasal mulai dari pasal 1 sampai dengan pasal 9. Dalam Pasal 1 Kitab Undang-undang Hukum Pidana diatur mengenai batas-batas berlakunya hukum pidana menurut waktu atau saat terjadinya perbuatan. Sedangkan dalam Pasal 2 sampai dengan Pasal 9 Kitab Undang-Undang Hukum Pidana diatur mengenai batas-batas berlakunya perundang-undangan hukum pidana menurut tempat terjadinya perbuatan.

Berkenaan dengan pengaturan diatas, Moeljatno menjelaskan bahwa dari sudut negara terdapat dua kemungkinan pendirian, yaitu: "Pertama, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang terjadi didalam wilayah negara, baik dilakukan oleh warga negaranya sendiri maupun warga negara asing (asas teritorial). Kedua, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang dilakukan oleh warga negara, dimana saja, juga diluar wilayah negara (asas personal). Juga dinamakan prinsip nasional yang aktif."[14]

Perkembangan teknologi informasi yang semakin pesat telah membuka aliran arus informasi tanpa mengenal batas-batas negara. Perubahan ini tentu saja membawa dampak baik bagi kehidupan masyarakat. Akses informasi dan perkembangan dunia terbaru dapat diakses dengan sangat mudah. Jarak ribuan kilometer sudah tidak menjadi penghalang untuk tetap terhubung dan saling bertukar informasi. Fenomena ruang siber ini menggambarkan sebuah realitas bahwa aktivitas masyarakat modern saat ini sudah saling terkoneksi melalui ruang siber dan internet.

Indonesia sendiri sudah tidak asing lagi dengan keberadaan internet. Kementerian Komunikasi dan Informatika (Kemenkominfo) mengungkapkan pengguna internet di Indonesia saat ini mencapai 63 juta orang. Tahun 2021 pengguna internet di Indonesia meningkat 11 persen dari tahun sebelumnya, yaitu dari 175,4 juta menjadi 202,6 juta pengguna. Dari angka tersebut, 95 persennya

[14] Moeljatno, 1985, Azas-Azas Hukum Pidana, Bina Aksara, Jakarta hlm 38

menggunakan internet untuk mengakses jejaring sosial.[15] Dunia maya sekarag ini solah tak ada bedanya dengan dunia nyata.

Dalam masyarakat modern yang meng-global seperti sekarang ini kejahatan dapat terjadi kapan saja dan dimana saja. Baik itu berupa kejahatan didunia nyata maupun didunia maya (*cyberspace*). Bentuk kejahatannya pun beragam, makin canggih modusnya, makin beragam karakteristik pelakunya serta makin bahaya akibat yang dapat ditimbulkannya. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan caria paling mudah untuk melancarkan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang *hacker*.

Kejahatan dunia maya makin marak seiring penggunaan internet yang makin bertambah banyak. Jenisnya pun beragam. 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.[16]

Serangan siber di Indonesia memang cukup luar biasa. Sebagai contoh, Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Jenis serangan yang paling banyak adalah trojan activitysebanyak 56% dan kemudian disusul dengan aktifitas *information gathering* (pengumpulan informasi) sebanyak 43% dari total keseluruhan

[15] Data Pengguna Internet Indonesia, diakses pada Kamis, 25 November 2021 dari https://kominfo.go.id/index.php/content/detail/3415/Kominfo+%3A+Pengguna+Internet+di+Indonesia+63+Juta+Orang/0/berita_satker

[16] Siswanto Sunarso, 2009, Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari, Rineka Cipta, Jakarta, hlm. 39

serangan, sedangkan1% sisanya merupakan web application attack.[17] Jumlah ini mungkin saja terus bertambah apabila tidak dubarengi dengan sikap waspada dari masyarakat pengguna itu sendiri. Namun peranan pemerintah juga sangat penting, terutama soal edukasi kepada masyarakat akan pentingnya memiliki budaya keamanan siber. Karena budaya ini masih cukup rendah. Contohnya masih lemahnya masyarakat memproteksi akun-akun atau data-data pribadinya. Seperti jarang atau bahkan tidak pernah mengganti nomor PIN atau password pribadi pada email, ATM dan lain-lain.

Masyarakat masih banyak yang tidak waspada terhadap kejahatan dunia maya. Masih banyak yang menganggap kejahatan dunia maya sebagai ancaman ringan, sehingga dalam menggunakan internet dan media sosial tidak disertai dengan proteksi diri. Sikap lengah seperti inilah yang memancing para penjahat dunia maya untuk melancarkan aksinya. Apalagi di zaman yang yang modern dan serba digital seperti sekarang ini, dimana kegiatan perekonomian sudah banyak yang beralih ke sistem digital. Misalnya saja jual beli online, internet banking, layanan transportasi dan masih banyak lagi.

Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan. Hingga kini, banyak sekali akun sosial media yang sudah terjebak dalam *phishing*. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh fake link pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan. Dengan hal tersebut penyerang dapat mengambil informasi pengguna dan menggunakannya untuk mencari keuntungan misalnya untuk mengambil uang dari rekening pengguna atau menggunakan rekening untuk pembayaran online.

Phishing sendiri adalah suatu kegiatan yang berupa ancaman atau jebakan dengan konsep memancing orang tersebut. Yaitu dengan cara menipu orang tersebut sehingga secara tidak langsung korban yang terpancing akan memberikan data-data diri, *password*, atau PIN mereka pada pelaku. Informasi sensitif seperti

[17] Rekap Serangan Siber Januari-April 2020, diakses pada Jumat 26 November 2021 dari https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

inilah yang dibutuhkan pelaku untuk meraup keuntungan dari korban yang terjebak dalam *phishing* yang diciptakan oleh pelaku. Setelah memperoleh data-data tersebut, pelaku kemudian menggunakannya untuk kepentingan pribadi yang bersifat merugikan korban seperti melakukan pencurian pada rekening korban.

Untuk megantisipasi serangan *phishing* semacam itu yang paling sederhana yaitu untuk tidak meng-klik jika ada link yang masuk melalui akun sosial media maupun email yang di gunakan untuk akun sosial media. Karena link yang tidak di kenal patut di curigai sebagai serangan *phishing* yang menjebak akun sosial media untuk menyebar luaskan hal-hal yang tidak baik pada pengguna sosial media yang lain. Tentu kita harus mencari Anti-*phishing* untuk mencegahnya. Karena sekali kita terkena serangan, maka ancaman *phishing* juga akan menyerang pengguna yang lain. Dan serangan akan terus menyebar dan menyebar ke seluruh penjuru dunia.

Pengaturan tindak pidana siber di Indonesia dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas.[18]

Dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 19/2016). UU ITE memang tidak memberikan definisi mengenai *cyber crimes*, tetapi membaginya menjadi beberapa pengelompokkan. Pengelompokan yang dimaksud yaitu:[19]

[18] Landasan Hukum Penanganan *Cyber crime* di Indonesia, diakses pada Senin 29 November 2021 dari https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia

[19] *Ibid*

1) Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:

a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari:

- Kesusilaan (Pasal 27 ayat (1) UU ITE);
- Perjudian (Pasal 27 ayat (2) UU ITE);
- Penghinaan dan/atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE);
- Pemerasan dan/atau pengancaman (Pasal 27 ayat (4) UU ITE);
- Berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE);
- menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE);
- mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);

b. Dengan cara apapun melakukan akses illegal (Pasal 30 UU ITE);

c. Intersepsi atau penyadapan illegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU 19/2016);

2) Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:

a. Gangguan terhadap Informasi atau Dokumen Elektronik (data interference - Pasal 32 UU ITE);

b. Gangguan terhadap Sistem Elektronik (*system interference*–Pasal 33 UU ITE);

3) Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);

4) Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);

5) Tindak pidana tambahan (accessoir Pasal 36 UU ITE); dan

6) Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE

A. Perlindungan Hukum Bagi Korban Tindak Pidana *Cyber crime Phishing*

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.[20]

Kemudahan serta manfaat yg diberikan dalam pemanfaatan perkembangan teknologi internet dan personal komputer sebagaimana digambarkan di atas, pada lain pihak mengakibatkan berbagai pertentangan hukum. Transaksi online praktis dilakukan karena tidak perlu bertemu secara langsung atau tanpa perlu mengenal terlebih dahulu menyisakan pertanyaan "bagaimana seseorang bisa mempercayai orang lain?" pengiriman atau pertukaran informasi yang dapat dilakukan secara instan (cepat serta murah), menimbulkan keraguan terhadap keamanan informasi yang dipertukarkan: "bagaimana bila informasi tadi diambil orang lain tanpa diketahui para pihak?" semakin berkurangnya saksi yg melihat secara langsung suatu insiden pada internet serta kebebasan anonimitas yang diterapkan dalam komunikasi elektronik pula menimbulkan tantangan bagi aparat penegak hukum untuk mencari dan menemukan pelaku tindak pidana *cyber*.[21]

Saat ini Indonesia telah memiliki *cyber law* untuk mengatur dunia maya berikut sanksi bila terkaji *cyber crime* baik di wilayah Indonesia maupun di luar

[20] Siswanto Sunarso, *loc cit*
[21] Josua Sitompul, 2012, Cyberspace Cybercrimes Cyberlaw: Tinjauan Aspek Hukum Pidana, PT Tatanusa, Jakarta, hlm 61

wilayah hukum Indonesia yang akibatnya dirasakan di Indonesia. *Cyber crime* terus berkembang seiring dengan revolusi teknologi informasi yang membalikkan paradigma lama terhadap kejahatan konvensional ke arah kejahatan virtual dengan memanfaatkan instrumen elektronik tetapi akibatnya dapat dirasakan secara nyata.

Cyber crime banyak jenis dan bentuknya. Salah satu bentuk kejahatan dunia maya (*cyber crime*) adalah penipuan lewat pesan yang berisi link atau *phishing*. Cukup banyak korban yang terkena tindak pidana *phishing* ini, namun kebanyakan menggap kejahatan *phishing* ini sebagai kejahatan ringan. Dalam beberapa kasus bahkan korban *phishing* tidak menyadari bahwa dirinya terkena jebakan *phishing*. Oleh karena itulah perlu adanya perlindungan hukum untuk membantu korban yang terkena *phishing* ini.

Perlindungan hukum bagi korban tindak pidana *Cyber crime Phishing* dapat diperoleh dari pasal 378 KUHP. Tindak pidana *phishing* termasuk dalam kategori penipuan, seperti dijelaskan pada Pasal 378 KUHP yang berbunyi:

"Barangsiapa 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."

Pasal 28 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga dapat digunakan untuk menjerat pelaku tindak pidana *Cyber crime Phishing* ini. Bunyi Pasal 28 Ayat (1) yaitu:

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

Selain pasal 378 KUHP dan Pasal 28 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pelaku tindak pidana *phishing* dapat dijerat Pasal 35 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik 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."

Pelaku tindak pidana *Cyber crime Phishing* memenuhi unsur-unsur sebagaimana yang terdapat dalam Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Selain beberapa pasal yang yang telah dijelaskan diatas, pelaku *phishing* juga dapat dijerat dengan Pasal 40 Undang-Undang No. 36 Tahun 1999 Tentang Telekomunikasi yang berbunyi:

"Bahwa setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun."

Dalam kasus *phishing*, pelaku jelas telah melakukan penyadapan guna memperoleh informasi yang bersifat pribadi dari korban untuk selanjutnya digunakan untuk melakukan kejahatan.

Korban yang dirugikan oleh tindak pidana *phishing* dapat memuntut ganti rugi. Aturan ganti rugi untuk korban tindak pidana dapat dilakukan melalui cara, yaitu:

1) melalui Penggabungan Perkara Ganti Kerugian;
2) melalui Gugatan Perbuatan Melawan Hukum; dan
3) melalui permohonan Restitusi.

Penggabungan perkara Ganti Rugi diatur dalam Pasal 98 ayat (1) KUHAP menjelaskan bahwa, " jika suatu perbuatan yang menjadi dasar dakwaan di dalam suatu pemeriksaan perkara pidana oleh pengadilan negri menimbulkan kerugian bagi orang lain, maka hakim ketua sidang atas permintaan orang itu dapat menetapkan untuk menggabungkan perkara gugatan ganti kerugian kepada perkara pidana itu." Permhonan penggabungan ganti kerugian berdasarkan ketentuan Pasal 98 ayat (2) KUHAP diajukan selambat-lambatnya sebelum penuntut umum mengajukan tuntutan pidana. Pada saat korban tindak pidana meminta penggabungan perkara ganti kerugian maka Pengadilan wajib

menimbang tentang kewenangannya untuk mengadili gugatan tersebut, tentang kebenaran dasar gugatan dan tentang hukuman penggantian biaya yang telah dikeluarkan oleh korban.[22]

Kasus serangan siber belakangan memang meningkat. Apalagi semenjak terjadinya pandemi yang melanda dunia. Pemerintah gencar menggalakkan untuk tetap tinggal dirumah dan mengurangi mobilitas. Termasuk kegiatan belajar mengajar dan bekerja. Sebisa mungkin dilakukan dirumah. Oleh karena itulah penggunaan internet pun ikut meningkat, serangan siber juga ikut meningkat.

Mengutip CNBC Indonesia Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) mencatat jumlah kasus peretasan di Indonesia selama tahun 2020 cukup besar. Sebab, selama pandemi Covid-19 jumlah pengguna internet pun semakin banyak. Dari laporan Pusopskamsinaskasus peretasan yang cukup banyak dilakukan melalui email *phishing*. Peningkatan email *phishing* ini terbanyak terjadi pada kuartal II tahun lalu yakni bulan Maret-Mei 2020. Jumlah kasus ini terjadi paling banyak pada saat jam kerja.[23]

Adapun email *phishing* merupakah salah satu teknik dari Social Engineering yang banyak digunakan oleh para peretas untuk mengelabui korban. Peretas mengirimkan sebuah email dengan judul yang menarik untuk dibuka oleh korban, biasanya berkaitan dengan finansial ataupun periklanan (hadiah, voucher, diskon, dll). Email biasanya berisi file sisipan (attachment) atau link yang mengarahkan pada diunduhnya program berbahaya. Program ini dapat secara otomatis bekerja di komputer korban dan mencuri kredensial, password, akun, informasi kartu kredit, dan lainnya.

Phishing menjadi pilihan yang populer di kalangan para peretas karena murah, dan kemudahan serta efektifitasnya cukup tinggi. Meskipun banyak organisasi yang telah menerapkan sistem keamanan untuk memblokir serangan

[22] Cara Menuntut ganti Rugi Bagi Korban Tindak Pidana, diakses pada Sabtu, 27 November 2021 dari: https://www.hukumonline.com/klinik/detail/ulasan/cl5928/ganti-rugi-dalam-kasus-pidana

[23] Serangan *Phishing* Indonesia Makin Merajalela, dikutip pada Minggu 28 November 2021 dari https://www.cnbcindonesia.com/tech/20210306162132-37-228322/kasus-*phishing*-email-yang-serang-indonesia-makin-merajalela#

phishing, namun penyerang juga semakin memiliki peralatan *phishing* yang lebih canggih. Selain itu masih banyak masyarakat yang kurang aware mengenai proteksi data internet mereka. Misalnya tidak memberikan *password* atau PIN.

Adanya hukuman atau sanksi bagi pelaku tindan pidana semata-mata untuk melindungi korban yang merasa dirugikan akibat perbuatan pelaku. Selain itu hukuman atau sanksi berfungsi sebagai peringatan terhadap masyarakat agar tidak melakukan hal serupa kedepannya.

KESIMPULAN DAN SARAN

A. Kesimpulan

Dari penjabaran penulis diatas maka dapat ditari kesimpulan yaitu:

1. Pengaturan Tindak Pidana *Cyber crime Phishing* di Indonesia:

- Pengaturan tindak pidana siber di Indonesia dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas.
- Dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Perlindungan Hukum Bagi Korban Tindak Pidana *Cyber crime Phishing*:

- Perlindungan hukum bagi korban tindak pidana *Cyber crime Phishing* dapat diperoleh dari pasal 378 KUHP. Tindak pidana *phishing* termasuk dalam kategori penipuan, seperti dijelaskan pada Pasal 378 KUHP.

- Pasal 28 Ayat (1) serta Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga dapat digunakan untuk menjerat pelaku tindak pidana *Cyber crime Phishing* ini.
- Selain itu pelaku tindang pidana *Cyber crime Phishing* dapat dikenakan Pasal 40 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.

Cyber crime beragam bentuknya, salah satunya adalah berupa *phishing*. *Phishing* secara sederhana dapat diartikan sebagai pencurian data pribadi dengan motif memancing calon korbannya menggunakan link yang berisi gangguan. Setelah itu pelaku dapat mengakses data-data pribadi korban seperti PIN, password bahkan m-banking. Pengaruh kemajuan teknologi tidak hanya merubah kehidupan masyarakat. Namun juga bnetuk-bentuk kejahatan yang ikut berubah dan menjadi lebih canggih.

Selain kewajiban pemerintah untuk melindungi masyarakat dari dampak negatif penggunaan internet, masyarakat sendiri juga haruslah selalu bersikap waspada dan bijak dalam menggunakan internet dan bersosial media.

B. Saran

Penulis memiliki sesuatu untuk dikatakan:

1. Saat ini kita hidup di zaman modern yang serba praktis dan canggih. Pembaruan teknologi salah satu bentuk kemajuan di zaman modern, internet adalah salah satu wujudnya. Banyak keuntungan yang didapat dari keberadaan internet. Namun selain sisi positif keberadaan internet, tentu saja terdapat hal negatif dari keberadaan internet itu sendiri. Salah satu contohnya adalah kejahatan yang menggunakan internet atau *cyber crime*. Bentuk-bentuk *cyber crime* bermacam-macam, misalnya saja *phishing*. Penulis berharap masyarakat lebih berhati-hati dan bijaksana dalam menggunakan internet. Karena *cyber crime* ini tidak mengincar siapa yang akan dijadikan korbannya. Semua orang yang menggunakan internet berpotensi untuk terkena *cyber crime*.

2. Harapan penulis agar pemerintah membuat satu aturan khusus di dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai tindak pidana *Cyber crime Phishing* ini. Karena selama ini belum ada aturan yang mengatur secara jelas dan spesifik mengenai tindak pidana *Cyber crime Phishing*.

DAFTAR PUSTAKA

Buku

Elisabeth Nurhaini Butarbutar, 2018, Metode Penelitian Hukum, Refika Aditama, Bandung

Jonaedi Efendi, Johnny Ibrahim, 2018, Metode Penelitian Hukum Normatif dan Empiris, Prenada Media, Jakarta

Josua Sitompul, 2012, Cyberspace Cybercrimes Cyberlaw: Tinjauan Aspek Hukum Pidana, PT Tatanusa, Jakarta

Moeljatno, 1985, Azas-Azas Hukum Pidana, Bina Aksara, Jakarta

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

Suratman dan Phillips Dilla, 2015, Metode Penelitian Hukum, Alfabeta Bandung, Bandung

Widodo (2013), Memerangi Cybercrime Karateristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi, Asswaja Pressindo, Yogyakarta

Jurnal, Skripsi, Tesis, Disertasi, Dll

Hilman Mursidi (2019), Skripsi Fakultas Hukum Universitas Sriwijaya, Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Cyber crime Phishing* (Studi Kasus Putusan Pengadilan Negeri Medan Nomor : 3006/Pid.Sus/2017/PN.Mdn)

Ki Jagad Tomara (2013), Skripsi Fakultas Hukum Universitas Brawijaya, Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs *Phishing*

Internet

Cara Menuntut ganti Rugi Bagi Korban Tindak Pidana, diakses pada Sabtu, 27 November 2021 dari: https://www.hukumonline.com/klinik/detail/ulasan/cl5928/ganti-rugi-dalam-kasus-pidana

Data Pengguna Internet Indonesia, diakses pada Kamis, 25 November 2021 dari https://kominfo.go.id/index.php/content/detail/3415/Kominfo+%3A+Pengguna+Internet+di+Indonesia+63+Juta+Orang/0/berita_satker

Jerat Hukum Pelaku *Phishing* dan Modusnya, diakses pada Rabu 26 Mei 2021 dari: https://www.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-i*phishing*-i-dan-modusnya/

Landasan Hukum Penanganan *Cyber crime* di Indonesia, diakses pada Senin 29 November 2021 dari https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia

Metode Analisis Bahan Hukum, diakses dari http://repository.ub.ac.id pada Minggu, 26 September 2021

Metode Penulisan, diakses pada Kamis 27 Mei 2021 dari: http://repository.umy.ac.id/bitstream/handle/123456789/23062/BAB%20III.pdf?sequence=4&isAllowed=y

Pengenalan Bahan Hukum, diakses pada Kamis 27 Mei 2021 dari https://simdos.unud.ac.id/uploads/file_penelitian_1_dir/7847bff4505f0416fe0c446c60f7e8ac.pdf

Rekap Serangan Siber Januari-April 2020, diakses pada Jumat 26 November 2021 dari https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Serangan *Phishing* Indonesia Makin Merajalela, dikutip pada Minggu 28 November 2021 dari https://www.cnbcindonesia.com/tech/20210306162132-37-228322/kasus-*phishing*-email-yang-serang-indonesia-makin-merajalela#