MALA IN SE: Jurnal Hukum Pidana, Kriminologi dan Viktimologi
Volume 1 Nomor 2 Oktober 2024
E-ISSN 3063-2293
https://jurnal.dokterlaw.com/index.php/malainse

PENEGAKAN HUKUM TERHADAP PELAKU DAN KORBAN TINDAK PIDANA *PHISING* DI INDONESIA (STUDI KASUS PUTUSAN PENGADILAN NEGERI BANJARBARU NOMOR 85/PID.SUS/2022/PN BJB)

Ady Teguh Basthian[1], Niru Anita Sinaga[2]
Faculty Of Law, Dirgantara Marsekal Suryadarma University
Email : adyteguh14@gmail.com[1], nirusinaga@unsurya.ac.id[2]

Cititation: Ady Teguh Basthian., Niru Anita Sinaga. Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana *Phising* Di Indonesia (Studi Kasus Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/Pn Bjb). *MALA IN SE: Jurnal Hukum Pidana, Kriminologi dan Viktimologi* 1.2.2024. 32-47
Submitted:01-08-2024 **Revised:**09-09-2024 **Accepted:**01-10-2024

Abstrak

Kejahatan dunia maya pada saat ini yaitu dengan memperoleh data identitas diri seperti user id dan password dengan menggunakan teknik *Phising.* Terdapat perbedaan pencurian yang dilakukan di dunia maya, di mana umumnya diawali dengan pencurian data. Data yang dicuri ini kemudian digunakan untuk melakukan tindakan yang merugikan korban. Permasalahanya yakni Bagaimana pengaturan tindak pidana *Phising* di Indonesia dan penegakan hukum terhadap pelaku dan korban tindak pidana Phising pada Putusan PN. Banjarbaru No 85/Pid.Sus/2022/PN Bjb ?. Tujuan penelitian ini adalah untuk mengetahui pengaturan tindak pidana *Phising* dan penegakan hukum terhadap pelaku dan korban tindak pidana *Phising* pada Putusan PN.Banjarbaru No 85/Pid.Sus/2022/PN.Bjb. Metode penelitian ini menggunakan normatif yaitu penelitian yang dilakukan dengan cara menganalisa hukum yang tertulis dari bahan pustaka atau data sekunder. Hasil penelitian ini didapatkan kesimpulan bahwa pengaturan tindak pidana *Phising* merujuk Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penegakan hukum yang berkaitan dengan *Cyber Crime* masih cukup ringan dan tidak sebanding dengan kerugian yang dialami korban. Sebagaimana pada Putusan No 85/Pid.Sus/2022/PN Bjb, terdakwa di jatuhi hukuman penjara selama 2 (dua) tahun dan 6 (enam) bulan serta denda sejumlah Rp 500.000.000,00 (lima ratus juta rupiah). Hal tersebut tidak sejalan dengan ketentuan yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Saran penelitian ini diharapkan pemerintah dan masyarakat untuk memahami pentingnya melindungi data pribadi dan menerapkan Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi dengan tepat untuk menjamin hak privasi masyarakat dibentuknya lembaga otoritas khusus dan idependen untuk mengatasi permasalahan data pribadi.
Kata Kunci : Penegakan Hukum, Tindak Pidana, *Phising*

Abstract

Cybercrime nowadays involves obtaining personal identification data such as user IDs and passwords using phishing techniques. There is a distinction between theft in cyberspace, which generally begins with data theft. The stolen data is then used to commit actions that harm the victim. The issue is how phishing crimes are regulated in Indonesia and the legal enforcement against the perpetrators and victims of phishing crimes in the Banjarbaru District Court Decision No. 85/Pid.Sus/2022/PN Bjb. The purpose of this research is to understand the regulation of phishing crimes and the legal enforcement against the perpetrators and victims in the Banjarbaru District Court Decision No. 85/Pid.Sus/2022/PN Bjb. This research uses a normative method, which is conducted by analyzing written laws from literature or secondary data. The results of this study conclude that the regulation of phishing crimes refers to Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions. Law enforcement related to cybercrime is still relatively light and not proportional to the losses experienced by the victims. As in Decision No. 85/Pid.Sus/2022/PN Bjb, the defendant was sentenced to two years and six months in prison and fined Rp 500,000,000.00 (five hundred million rupiah). This is not in line with the provisions set out in Law No. 27 of 2022 on Personal Data Protection. The recommendation of this research is that the government and society should understand the importance of protecting personal data and properly implement Law No. 27 of 2022 on Personal Data Protection to guarantee privacy rights. The establishment of a special and independent authority to address personal data issues is also suggested.
Keyword : Law Enforcement, Crime, Phishing

Volume 1 Nomor 2 Oktober 2024
E-ISSN 3063-2293
https://jurnal.dokterlaw.com/index.php/malainse

A. PENDAHULUAN

Penegakan hukum adalah proses dilakukannya upaya untuk tegaknya atau berfungsinya norma-norma hukum secara nyata sebagai pedoman perilaku dalam lalu lintas atau hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara.[1] Pemaknaan penegakan hukum dalam konteks yang luas berada pada ranah tindakan, perbuatan atau perilaku nyata atau faktual yang bersesuaian dengan kaidah atau norma yang mengikat. Namun demikian, dalam upaya menjaga dan memulihkan ketertiban dalam kehidupan sosial maka pemerintahlah *actor security.*[2]

Kejahatan *phishing* di Indonesia telah membuat transaksi elektronik menjadi rentan, terutama karena pengguna internet berasal dari berbagai kalangan dengan pemahaman yang berbeda tentang ancaman dunia maya. *Phishing,* sebagai bagian dari kejahatan siber, melibatkan tipu muslihat yang sulit dikenali oleh pengguna.[3]

Cyber Crime diatur dalam Undang-Undang Nomor 19 Tahun 2016 yang mengubah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, untuk membuktikan tindak phishing, undang-undang ini tidak cukup, karena bersifat administratif.

Jaminan perlindungan terhadap tindak pidana phishing diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 2 undang-undang ini menyatakan bahwa perlindungan berlaku bagi semua orang, badan publik, dan organisasi internasional yang melakukan tindakan hukum di wilayah Indonesia atau di luar negeri yang berdampak hukum di Indonesia, termasuk bagi warga negara Indonesia di luar negeri. Namun, undang-undang ini tidak berlaku untuk pemrosesan data pribadi dalam konteks pribadi atau rumah tangga.[4]

Phishing, sebagai bagian dari kejahatan siber *(cyber crime),* merupakan ancaman serius di seluruh dunia karena ruang dan waktu kejadian sering kali berbeda. Ini membuat korban dan penegak hukum memerlukan kemampuan khusus untuk menanganinya. Kewaspadaan dan ketelitian dalam menggunakan media elektronik adalah kunci untuk menghindari *phishing*.[5]

---

[1] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan* (Jakarta: Kencana Prenada Media Group, 2007), 21.
[2] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum* (Jakarta: Rajawali Pers, 2008), 21.
[3] Maskun, *Kejahatan Siber Cybercrime: Suatu Pengantar* (Jakarta: Kencana, 2013), 29.
[4] Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Pasal 2. LN Tahun 2022 No. 196, TLN No. 6820
[5] Dikdik M. dan Elisatris Gultom, *Cyber Law: Aspek Hukum dan Teknologi Informasi* (Bandung: Refika Aditama, 2009), 2.

Saat menjatuhkan sanksi pidana, perlu mempertimbangkan aspek kemanusiaan, menjunjung harkat martabat, bersifat edukatif untuk menyadarkan pelaku, dan memberikan rasa keadilan bagi pelaku, korban, serta masyarakat.[6]

Perkembangan teknologi, terutama internet, membawa dampak negatif seperti penyalahgunaan data. Phishing adalah salah satu bentuk kejahatan yang menargetkan informasi pribadi seperti user ID dan password melalui teknik manipulatif.[7]

Dengan kemajuan teknologi informasi, modus operandi kejahatan juga semakin canggih.[8] Dalam jaringan komputer seperti internet, kriminalitas menjadi lebih kompleks karena tidak terbatas oleh teritorial dan tidak memerlukan interaksi langsung antara pelaku dan korban. Kejahatan siber *(cyber crime)* adalah fenomena global yang berdampak pada semua negara yang menggunakan internet. Salah satu bentuk kejahatan siber yang harus diwaspadai adalah *phishing,* yang berkembang pesat seiring dengan meningkatnya penggunaan internet.

Dengan segala kemudahan yang diberikan di dunia maya maka semakin besar pula kemudahan untuk melakukan *cyber crime.* Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan baru dibidang itu juga muncul. Saat ini berbagai macam bentuk *cyber crime* berkembang di masyarakat, salah satu kejahatan *cyber crime* yang berkembang pada saat ini yaitu tindak pidana *phising (password harvesting fishing).*[9]

Contoh kasus phishing dapat dilihat dalam Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb, di mana Terdakwa Riswanda Noor Saputra diduga terlibat dalam pembuatan dan distribusi perangkat lunak yang digunakan untuk memfasilitasi phishing. Kasus ini dilaporkan oleh INTERPOL dan Kedutaan Besar Amerika Serikat setelah website "16 Shop" diidentifikasi sebagai kit phishing yang menargetkan pengguna akun Apple, Amazon, PayPal, dan American Express. Terdakwa diduga terkait dengan kit tersebut melalui data akun dan penggunaan bahasa Indonesia pada perangkat.

Jaksa menuntut terdakwa berdasarkan Pasal 51 dan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, serta Pasal 3 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Jaksa menuntut terdakwa dengan hukuman berupa pidana penjara selama 1 (satu) tahun dan dan pidana denda sebesar Rp. 200.000.000,00 (dua ratus juta ribu rupiah) dengan ketentuan

[6] Hanafi Amrani, *Politik Pembaharuan Hukum Pidana* (Yogyakarta: UII Press, 2019), 128–129.
[7] Kristian dan Yopi Gunawan, *Penyadapan Dalam Hukum Positif di Indonesia* (Bandung: Nuansa Aulia, 2013), 1.
[8] Maskun, *Op. Cit.*, 44.
[9] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime)* (Bandung: Refika Aditama, 2005), 3.

apabila denda tidak dibayar maka diganti dengan pidana penjara selama 3 (tiga) bulan penjara.[10]

Kasus di atas relevan karena memberikan gambaran konkret tentang penegakan hukum terhadap tindak pidana *phishing* di Pengadilan Indonesia. Analisis terhadap putusan ini dapat memberi wawasan mengenai tantangan dan potensi dalam menangani kejahatan phishing, terutama dalam konteks *cyber crime.*

Cyber crime di dunia maya kini hampir menyerupai kejahatan konvensional, seperti pencurian. Namun, perbedaannya terletak pada metode pencurian di dunia maya, yang biasanya diawali dengan pencurian data. Data ini kemudian digunakan untuk tindakan yang merugikan korban, seperti pembobolan dana di bank. Sayangnya, masih banyak masyarakat Indonesia yang belum cukup waspada terhadap ancaman *cyber crime,* khususnya *phishing,* yang merupakan upaya penipuan dengan menyamar sebagai email atau situs palsu untuk mencuri informasi pribadi.

Korban *phishing* sangat dirugikan, terutama secara materiil, dan mereka berhak mendapatkan perlindungan serta pengembalian hak-hak yang hilang. Negara perlu bertindak untuk mengembalikan kesejahteraan korban.

Penegakan hukum terhadap pelaku phishing menjadi sangat penting karena dampaknya yang merugikan, baik secara finansial maupun psikologis. Meski kasus *phishing* terus meningkat, penegakan hukum dan keadilan bagi korban masih belum optimal. Hal ini menimbulkan pertanyaan tentang kesiapan sistem hukum Indonesia dalam menghadapi tantangan era digital. Selain itu, kurangnya pemahaman masyarakat tentang bahaya phishing juga menjadi faktor penting yang harus diperhatikan.

Berdasarkan uraian latar belakang diatas, maka peneliti tertarik untuk melakukan penelitian dengan mengangkat judul "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana *Phising* di Indonesia (Studi Kasus Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN. Bjb)".

B. METODE PENELITIAN

Jenis penelitian yang dipergunakan dalam penelitian ini adalah jenis penelitian hukum yuridis normatif. Pendekatan penelitian hukum *(approach)* yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan *(statute approach),* pendekatan konseptual

[10] Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb

Volume 1 Nomor 2 Oktober 2024
E-ISSN 3063-2293
https://jurnal.dokterlaw.com/index.php/malainse

(conceptual approach), dan pendekatan kasus *(case approach).* Jenis Data yang dipergunakan dalam penelitian ini adalah data sekunder dimana data sekunder adalah sekumpulan informasi yang telah ada sebelumnya dan digunakan sebagai pelengkap kebutuhan data penelitian. Untuk memperoleh informasi atau data yang diperlukan guna menjawab rumusan masalah penelitian, Peneliti menggunakan metode atau teknik pengumpulan data dengan Penelitian Kepustakaan *(Library Research).* Metode analisis data yang dipergunakan adalah analisis data kualitatif, yaitu proses penyusunan, mengkatagorikan data kualitatif, mencari pola atau tema dengan maksud memahami maknanya.[11]

C. HASIL PENELITIAN DAN PEMBAHASAN

1. Pengaturan Tindak Pidana *Phising* Di Indonesia

Kejahatan *cracking* atau *cracker,* salah satunya adalah *phishing,* bertujuan untuk mendapatkan keuntungan pribadi dengan merugikan pihak lain. Dalam konteks keamanan komputer, *phishing* adalah penipuan elektronik yang bertujuan mencuri informasi sensitif seperti username, password, dan detail kartu kredit. Teknik ini dilakukan dengan menyamar sebagai entitas yang tampak sah, biasanya melalui media elektronik seperti email atau situs palsu yang meniru organisasi tepercaya.

Phishing umumnya menargetkan pengguna layanan perbankan online, di mana pengguna tanpa sadar memasukkan informasi pribadi mereka ke dalam form login palsu yang dibuat oleh pelaku. Tindakan ini semakin marak, dengan data dari Anti-Phishing Working Group (APWG) menunjukkan bahwa 42% penipuan global dilakukan dengan modus *phishing. Phishing* juga menyebar melalui media sosial yang terhubung ke internet.[12]

Di Indonesia, *phishing* dapat dikenakan 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, karena kejahatan ini melibatkan pembuatan situs palsu yang menyerupai situs asli. Selain itu, Pasal 28 ayat (1) jo Pasal 45A ayat (1) juga bisa diterapkan karena *phishing* menipu dan menyesatkan korban untuk mengakses situs palsu dan memasukkan data pribadi, yang kemudian digunakan oleh pelaku untuk keuntungan pribadi dan menyebabkan kerugian bagi korban.

[11] Soerjono Soekanto, *Pengantar Penelitian Hukum* (Jakarta: UI Press, 2018).
[12] Al Wisnubroto, *Konsep Hukum Pidana Telematika* (Yogyakarta: Universitas Atmajaya, 2011), 12.

Berdasarkan tujuan pembentukan Undang-Undang ITE, fokus utamanya adalah upaya preventif yang terkait dengan prinsip itikad baik dalam Pasal 3, untuk mencegah tindak pidana dalam transaksi elektronik. *Phising* adalah tindakan untuk mendapatkan informasi pribadi melalui situs palsu yang menyerupai aslinya, biasanya dengan menggunakan email atau SMS. Pertanyaannya adalah apakah pelaku *phising* hanya dikenakan Pasal 35, Pasal 51 ayat (1), Pasal 28 ayat (1), dan Pasal 45A ayat (1) UU ITE, atau juga terkait dengan pasal lain termasuk KUHP.

Phising dalam *digital trading* terjadi dengan mengirim email palsu yang tampak resmi atau melalui SMS yang meminta informasi pribadi. Hukum yang mengatur *phising* diatur dalam beberapa pasal UU ITE, termasuk Pasal 28, Pasal 45, Pasal 35, dan Pasal 51 yang mengatur penyebaran berita bohong, manipulasi informasi elektronik, dan ancaman pidana hingga 12 tahun penjara atau denda hingga Rp12 miliar. Penyedia jasa internet tidak akan dipidana kecuali terbukti ikut serta dalam kejahatan.[13]

Ketentuan Peraturan Perundang-undangan untuk menjerat pelaku tindak pidana *phising* menurut Undang-Undang Informasi dan Transaksi Elektronik:

1) Pasal 28 ayat (1) menyebutkan bahwa: "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."
2) Pasal 45 ayat (2) menyebutkan bahwa: "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".

Penyedia jasa internet tidak dapat disalahkan jika pengguna jasanya melakukan tindak pidana, kecuali jika terbukti berpartisipasi dalam kejahatan tersebut. Dalam kasus ini, penyedia jasa internet dapat dikenakan tanggung jawab pidana berdasarkan sistem pertanggungjawaban korporasi.

Salah satu contoh umum adalah kejahatan *cyber phising,* yang sering kali tidak disadari oleh masyarakat dan dapat sangat merugikan korban. *Phising (Password Harvesting Fishing)*

[13] Dian Ekawati Ismail, "Cyber Crime di Indonesia," *Delicti: Jurnal Hukum Pidana* 6, no. 3 (April 2021): 19–32.

adalah penipuan yang memanfaatkan email atau situs web palsu untuk mengelabui pengguna dan mengumpulkan data pribadi mereka. Data ini sering digunakan untuk mengirim email yang terlihat berasal dari perusahaan resmi, seperti bank, dengan tujuan memperoleh informasi pribadi.[14]

Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menegaskan bahwa setiap orang yang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan informasi elektronik dengan tujuan membuatnya terlihat otentik dapat dikenakan sanksi. Menurut Pasal 48 ayat (2), pelanggar dapat dijatuhi hukuman penjara maksimal 9 tahun atau denda hingga Rp3.000.000.000,00. Pasal 51 ayat (1) menambahkan bahwa pelanggar Pasal 35 dapat dijatuhi hukuman penjara hingga 12 tahun dan/atau denda maksimal Rp12.000.000.000,00.

Dalam kasus *cyber crime phising*, terdapat pencurian *UserID* dengan penipuan melalui tautan yang digunakan untuk menyebarkan ujaran kebencian dan berita palsu. Pelaku memanfaatkan *UserID* orang lain untuk menipu publik, sehingga publik mengira tindakan tersebut berasal dari korban, padahal pelaku yang sebenarnya mengontrol *UserID* tersebut.

Kebijakan perundang-undangan sangat penting bagi penegak hukum dan pemerintah untuk menangani kejahatan siber. Jenis hukum yang diterapkan harus sesuai dengan jenis kejahatan dan metode pengungkapan kasus. Pemerintah Republik Indonesia telah berkomitmen untuk memerangi kejahatan dunia maya.

Dengan semakin pesatnya penggunaan teknologi, risiko kejahatan seperti penipuan, pencurian, dan pencemaran nama baik melalui internet juga meningkat. Pada bab ini, akan dibahas upaya yang dilakukan pemerintah Indonesia untuk menangani kejahatan berbasis teknologi informasi, baik yang terjadi di dalam negeri maupun yang dilakukan oleh sindikat internasional di wilayah Indonesia.

Kebijakan memerangi *cyber crime* adalah rangkaian konsep dan asas yang menjadi dasar pelaksanaan tugas pemerintah dan organisasi lainnya. Kebijakan publik bisa bersifat nasional, regional, atau lokal, seperti undang-undang, peraturan pemerintah, dan keputusan daerah. Menurut Easton, kebijakan publik adalah pengalokasian nilai-nilai secara paksa kepada seluruh anggota masyarakat, sedangkan Laswell dan Kaplan mendefinisikannya sebagai program pencapaian tujuan dan nilai dalam praktik.[15]

---

[14] Sofwan Jannah dan M. Naufal, *Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif* (Bandung: Remaja Rosdakarya, 2012), 23.
[15] Kusrini, *Sistem Pakar dan Teori Aplikasi Trading* (Yogyakarta: Andi, 2012), 24.

Volume 1 Nomor 2 Oktober 2024
E-ISSN 3063-2293
https://jurnal.dokterlaw.com/index.php/malainse

Dalam menghadapi kejahatan *cyber crime,* pendekatan yang dilakukan pemerintah Indonesia mencakup strategi pencegahan dan penindakan. Usaha pertama adalah pencegahan dengan sistem peradilan pidana, sedangkan usaha kedua melibatkan penegakan hukum yang didukung oleh masyarakat. Penanganan kejahatan *phising* memerlukan peran aktif masyarakat untuk melaporkan tindakan kejahatan. Korban *phising* sebaiknya melapor kepada polisi *cyber* untuk memproses hukum kasus tersebut dan mengenali ciri-ciri kejahatan *phising* agar tidak menjadi korban.

Ciri umum penipuan *phising* adalah iming-iming hadiah yang meminta data pribadi. Oleh karena itu, pesan yang tidak masuk akal sebaiknya tidak direspon, dan berhati-hatilah terhadap tautan mencurigakan. Selain *phising,* terdapat kejahatan lain seperti skimming, yang bertujuan untuk mencuri data penting dan mendapatkan keuntungan dari data tersebut. Untuk menghindari kejahatan ini, penting untuk tidak memberikan password atau username kepada pihak lain dan melaporkan tindakan mencurigakan kepada pihak berwajib.

Undang-Undang Informasi dan Transaksi Elektronik telah mengatur tentang kejahatan *phising.* Upaya menghindari kejahatan siber dimulai dari diri sendiri dengan menjaga keamanan data pribadi dan akun. Risiko *phising* dapat mengakibatkan kerugian besar, termasuk pencurian data pribadi yang bisa disalahgunakan atau dijual. Dalam konteks digital trading, anggota sering diminta mengisi form data pribadi yang sebenarnya bertujuan untuk mencuri informasi. Korban *phising* juga dapat mengalami kerugian finansial.[16]

Kasus *phising* yang terjadi pada Kredivo mengakibatkan beberapa pengguna menjadi korban tindak pidana siber. Mereka dihubungi oleh oknum yang menawarkan promo dan hadiah, tetapi akhirnya menghadapi tagihan yang membengkak akibat pembelian barang di Bukalapak.

Seorang pakar IT dan *Internet Security* dari ITB menjelaskan bahwa pelaku memperoleh data pribadi korban melalui telepon, memastikan nama dan nomor telepon korban untuk melakukan hack dan memberikan tautan situs *phising.* Kebocoran data dapat terjadi baik secara offline misalnya, korban secara tidak sengaja mengisi data diri pada selembar kertas yang hilang maupun online saat korban mengunjungi situs *phising* untuk mengisi data pribadi.[17]

[16] Aziz Rahardyan, "Kredivo Lapor Kasus Cybercrime ke Polisi, Tagihan Pengguna Bengkak Gara-gara Promo Fiktif," *Jurnal Hukum Pidana & Kriminologi* 2, no. 3 (Desember 2021): 81–98.
[17] Andrew Christian Banjarnahor, "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phishing Kredivo," *Hermeneutika* 6, no. 1 (Februari 2022): 33–36.

Hukum terkait tindak pidana *cybercrime phising* diatur dalam Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pelaku *phising* dapat dikenakan sanksi pidana berdasarkan Pasal 35 jo. Pasal 51 ayat (1), yang mengandung unsur kebohongan yang merugikan korban, serta Pasal 28 ayat (1) jo. Pasal 45A ayat (1), yang berkaitan dengan manipulasi informasi elektronik. Selain itu, Pasal 30 ayat (3) jo. Pasal 46 ayat (3) juga menjelaskan penerobosan sistem keamanan korban.

Dalam kasus ini, pelaku *phising* memenuhi unsur pidana seperti "barang siapa," "dengan maksud untuk membuat untung," dan "secara melawan hukum." Penulis berpendapat bahwa *phising* adalah tindak kejahatan siber di mana pelaku memperoleh informasi sensitif, seperti kata sandi dan nomor kartu kredit, dengan menyamar sebagai entitas tepercaya. *Phising* sering dilakukan melalui email, situs web palsu, pesan teks, atau media sosial.

Pengaturan hukum untuk *phising* terdapat pada Pasal 50 Undang-Undang No. 19 Tahun 2016, sedangkan perlindungan hukum bagi korban diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Tantangan dalam penanggulangan *phising* mencakup penegakan hukum yang efektif, kerjasama internasional, dan edukasi publik. Diperlukan upaya berkelanjutan untuk memperbarui regulasi dan strategi guna menghadapi teknik *phising* yang semakin canggih

2. Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana *Phising* Pada Putusan PN. Banjarbaru No 85/Pid.Sus/2022/PN Bjb

a. Kasus Posisi:

Pada bab ini, penulis menjelaskan kasus tindak pidana *phising* yang diambil dari Putusan PN Banjarbaru No. 85/Pid.Sus/2022/PN Bjb dengan terdakwa Riswanda Noor Saputra, mahasiswa berusia 22 tahun. Ia ditangkap pada 19 November 2021 dan ditahan sejak 20 November 2021. Penahanannya diperpanjang beberapa kali oleh penuntut umum, Ketua Pengadilan Negeri, dan Ketua Pengadilan Tinggi. Riswanda dinyatakan bersalah atas tindak pidana manipulasi elektronik dan pencucian uang sesuai Pasal 51 UU ITE No. 19 Tahun 2016 serta Pasal 3 UU Pencucian Uang No. 8 Tahun 2010.

b. Dakwaan dan Tuntutan

Jaksa Penuntut Umum mendakwa Riswanda dengan pelanggaran Pasal 50 dan 51 UU ITE No. 19 Tahun 2016 serta Pasal 3 UU Pencucian Uang No. 8 Tahun 2010. Setelah mendengar keterangan saksi, ahli, dan terdakwa, serta meninjau bukti-bukti, jaksa menuntut

Riswanda dengan hukuman penjara 1 tahun dan denda Rp 200.000.000. Jika denda tidak dibayar, diganti dengan 3 bulan penjara. Selain itu, barang bukti disita dan biaya perkara sebesar Rp 5.000 dibebankan kepada terdakwa.

c. Putusan Majelis Hakim

Berdasarkan alat dan barang bukti yang diajukan, diperoleh fakta-fakta hukum sebagai berikut:

1) Terdakwa dihadirkan ke persidangan terkait penjualan software phishing yang menyerupai situs seperti Apple, Amazon, dan PayPal.
2) Pembuatan software dimulai Desember 2017, berdasarkan permintaan teman di Facebook tanpa mengetahui tujuannya.
3) Terdakwa membuat software sendiri menggunakan laptop dan aplikasi XAMPP dan Sublime Text, dengan menyalin kode dari desain situs-situs terkenal dan memprogramnya menggunakan HTML, PHP, JavaScript, dan CSS.
4) Pada 2018, Terdakwa menyadari bahwa software tersebut digunakan untuk mencuri data identitas, alamat, nomor telepon, dan data kartu kredit.
5) Pada Desember 2019, Terdakwa memperbarui software di rumahnya dan membuat situs 16shop untuk menjual software phishing tersebut demi keuntungan.
6) Software tersebut meniru tampilan situs resmi untuk mencuri data pengguna.
7) Cara kerja software adalah dengan mengirim email palsu kepada korban, mengarahkan mereka untuk mengisi data pribadi dan kartu kredit di situs palsu.
8) Terdakwa menyediakan script di website 16shop, yang memungkinkan pelaku kejahatan untuk mengakses tampilan seperti situs resmi.
9) Website Terdakwa mampu meniru tampilan situs asli PayPal dan Apple, tetapi bukan merupakan website resmi, dan tindakan ini melanggar UU ITE karena menyediakan fasilitas untuk mencuri data.
10) Perbuatan Terdakwa terungkap dari laporan FBI dan NCB Interpol yang menyebutkan bahwa Terdakwa diduga pemilik website 16shop yang menjual tool kit untuk pencurian data identitas secara ilegal.

Berdasarkan Pasal 50 dan Pasal 34 ayat (1) huruf a Undang-Undang Nomor 19 Tahun 2016 serta Undang-Undang lainnya yang terkait, Majelis Hakim memutuskan:

1) Terdakwa, Riswanda Noor Saputra, terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana memproduksi perangkat lunak komputer yang dirancang

Volume 1 Nomor 2 Oktober 2024
E-ISSN 3063-2293
https://jurnal.dokterlaw.com/index.php/malainse

untuk memfasilitasi tindak pidana sebagaimana diatur dalam Pasal 32 ayat (2) dan melakukan perbuatan yang berkaitan dengan pencucian uang.

2) Terdakwa dijatuhi pidana penjara selama 2 tahun 6 bulan dan denda sebesar Rp 500.000.000,00; jika denda tidak dibayar, akan diganti dengan pidana kurungan selama 3 bulan.
3) Masa penangkapan dan penahanan yang telah dijalani Terdakwa akan dikurangkan dari pidana yang dijatuhkan.
4) Terdakwa tetap ditahan.
5) Barang bukti ditetapkan dalam berkas perkara, dan Terdakwa dikenakan biaya perkara sebesar Rp 5.000,00.

d. Analisis Putusan

Dalam analisis putusan, seorang hakim memiliki tanggung jawab untuk menegakkan hukum dan keadilan dengan tidak berpihak. Sebelum memberikan keputusan, hakim harus menelaah kebenaran peristiwa yang dihadapkan kepadanya, mengevaluasi fakta-fakta, dan mengaitkannya dengan hukum yang berlaku. Hal ini didukung oleh Pasal 16 ayat (1) Undang-Undang Nomor 35 Tahun 1999 jo. Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman, yang menyatakan bahwa pengadilan tidak boleh menolak untuk memeriksa dan mengadili suatu perkara, bahkan jika hukum yang relevan dianggap tidak jelas.

Pertimbangan hukum merupakan elemen penting dalam setiap putusan, yang memengaruhi pemahaman pihak-pihak yang terlibat, termasuk dalam proses banding dan kasasi. Telaah terhadap pertimbangan hakim dapat dilakukan dari dua sudut pandang: yuridis dan non-yuridis.[18] Tugas ini sangat penting dalam konteks kekuasaan kehakiman, di mana hakim diharapkan dapat memenuhi rasa keadilan dalam masyarakat. Dalam kasus pidana penipuan, misalnya, pertimbangan hakim harus mencakup keadaan dan kondisi terdakwa, tanpa mengabaikan rasa keadilan yang seharusnya diberikan kepada pelaku tindak pidana phishing.

Pembuktian dalam persidangan adalah tahap yang krusial, karena hasilnya akan digunakan sebagai dasar pertimbangan dalam menjatuhkan putusan. Pembuktian bertujuan untuk memastikan bahwa suatu fakta benar-benar terjadi, agar hakim dapat mengambil keputusan yang tepat. Seorang hakim tidak dapat menjatuhkan putusan tanpa keyakinan bahwa

[18] Rusli Muhammad, *Potret Lembaga Pengadilan Indonesia* (Yogyakarta: Grafindo Persada, 2006), 142–143.

Volume 1 Nomor 2 Oktober 2024
E-ISSN 3063-2293
https://jurnal.dokterlaw.com/index.php/malainse

fakta yang dihadirkan telah terbukti, sehingga hubungan hukum antara para pihak dapat ditegakkan.

Dalam Putusan Nomor 85/Pid.Sus/2022/PN.Bjb, majelis hakim telah memenuhi unsur-unsur yang diperlukan untuk penegakan hukum. Unsur-unsur tersebut mencakup tindakan mentransfer, mengalihkan, dan menyembunyikan harta kekayaan yang diketahui atau patut diduga merupakan hasil tindak pidana. Penegakan hukum yang dilakukan oleh hakim dianggap sesuai dengan prinsip pemidanaan, dengan menjatuhkan pidana penjara selama 2 tahun 6 bulan dan denda sebesar Rp 500.000.000.

Namun, penting untuk mencermati bahwa penegakan hukum pidana juga berkaitan dengan dua fungsi utama, yaitu untuk menanggulangi kejahatan dan memastikan bahwa pemerintah melaksanakan tugasnya sesuai dengan hukum. Dalam hal ini, pelaksanaan hukum pidana tidak semata-mata bertujuan untuk menghukum, tetapi juga harus mempertimbangkan efektivitasnya dalam mengurangi kejahatan.[19]

Dalam konteks penanganan pelanggaran hukum, termasuk kejahatan terhadap anak, hukuman yang dijatuhkan harus mencerminkan beratnya tindak pidana yang dilakukan. Hal ini menjadi polemik di masyarakat, tetapi penjatuhan hukuman harus didasarkan pada proses hukum yang sah. Majelis hakim harus mempertimbangkan bukti dan keyakinan, serta faktor-faktor yang memberatkan atau meringankan.

Penting untuk menyoroti bahwa Putusan Nomor 85/Pid.Sus/2022/PN.Bjb dalam kasus phishing belum mencerminkan keadilan bagi korban. Dalam hal ini, penuntut seharusnya merujuk pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan Menteri Komunikasi dan Informatika RI Nomor 19 Tahun 2016 yang memberikan panduan perlindungan data. Dalam konteks ini, meskipun Undang-Undang Nomor 19 Tahun 2016 tidak mencakup definisi jelas mengenai "data pribadi", perlindungan data pribadi diatur dalam berbagai ketentuan yang memastikan hak masyarakat.

Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) juga diharapkan dapat bekerja sama dengan lembaga lain, serta mematuhi ketentuan hukum yang berlaku untuk menjalankan tugasnya secara efektif. Sanksi administratif dan pidana harus ditegakkan terhadap pelanggaran perlindungan data pribadi, termasuk phishing.

[19] Tony Yuri Rahmanto, "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik (Legal Enforcement Against Fraudulent Acts in Electronic-Based Transactions)," *Jurnal Penelitian Hukum De Jure* 19, no. 1 (Maret 2019): 37.

Volume 1 Nomor 2 Oktober 2024
E-ISSN 3063-2293
https://jurnal.dokterlaw.com/index.php/malainse

Dalam analisis ini, terlihat bahwa penegakan hukum terhadap pelaku phishing di Indonesia harus lebih komprehensif, dengan melibatkan hukum perlindungan data pribadi dan mengadopsi pendekatan yang bersifat preventif dan represif. Hal ini akan membantu mengurangi jumlah kasus serupa di masa depan dan meningkatkan keamanan siber di Indonesia. Putusan harus mencerminkan keadilan, tidak hanya bagi terdakwa tetapi juga bagi korban, dengan mempertimbangkan ganti rugi yang dapat mengurangi dampak negatif dari tindakan kriminal tersebut.

D. KESIMPULAN

Pengaturan tindak pidana phishing di Indonesia merujuk pada Undang-Undang Nomor 19 Tahun 2016 yang mengubah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam penegakan hukumnya, terkait dengan cybercrime, sanksi yang diterapkan berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang ITE tergolong masih ringan. Padahal, jika melihat pada banyaknya kasus yang terjadi, cybercrime dapat menimbulkan kerugian yang signifikan bagi korban. Oleh karena itu, sanksi yang ada dirasa tidak sebanding dengan dampak yang ditimbulkan oleh para pelaku.

Dalam kasus penegakan hukum terhadap pelaku dan korban tindak pidana phishing, merujuk pada Putusan PN Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb, hakim menjatuhkan hukuman kepada terdakwa berupa pidana penjara selama dua tahun dan enam bulan, serta denda sebesar Rp 500.000.000,00. Dalam hal denda tidak dibayar, terdakwa harus menjalani pidana kurungan tambahan selama tiga bulan. Namun, penegakan hukum yang diterapkan terhadap korban belum mencerminkan keadilan yang seharusnya. Hal ini seharusnya mengacu pada Pasal 98 ayat (1) Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mengatur hak-hak korban dalam proses hukum. Keterpaduan penegakan hukum terhadap pelaku dan perlindungan yang memadai bagi korban sangat diperlukan untuk mewujudkan keadilan yang seimbang.

E. SARAN

Penting bagi pemerintah dan masyarakat untuk menyadari betapa krusialnya melindungi data pribadi dan menerapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dengan sebaik-baiknya, demi menjamin hak privasi masyarakat.

Kesadaran akan pentingnya perlindungan data pribadi harus ditingkatkan melalui edukasi yang sistematis dari pemerintah kepada masyarakat, agar setiap individu dapat melindungi data pribadi mereka dan juga data orang lain. Selain itu, pemerintah dan lembaga legislatif perlu melakukan evaluasi berkala terhadap peraturan-peraturan yang berkaitan dengan perlindungan data pribadi, serta melakukan perubahan yang diperlukan untuk menghadapi perkembangan teknologi dan ancaman baru.

Dalam hal penanggulangan atau pencegahan penyalahgunaan tindak pidana phishing, Majelis Hakim seharusnya lebih memperhatikan kerugian yang dialami oleh korban. Penjatuhan hukuman terhadap pelaku tidak hanya harus bersifat represif, tetapi juga preventif. Salah satu langkah yang dapat diambil adalah dengan menggabungkan gugatan ganti rugi kepada pelaku tindak pidana phishing, sesuai dengan ketentuan yang diatur dalam Pasal 98 KUHAP. Di samping itu, rujukan hukum dalam kasus ini juga harus mengacu pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang berkaitan erat dengan aspek keamanan siber. Pendekatan yang komprehensif ini diharapkan dapat mencegah tindak pidana phishing dan memberikan perlindungan yang lebih baik bagi masyarakat.

DAFTAR PUSTAKA

Buku :

Al Wisnubroto. Konsep Hukum Pidana Telematika. Yogyakarta: Universitas Atmajaya, 2011.

Barda Nawawi Arief. Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Jakarta: Kencana Prenada Media Group, 2007.

Budi Suhariyanto. Tindak Pidana Teknologi Informasi (Cyber Crime). Bandung: Refika Aditama, 2005.

Dikdik M. Gultom, and Elisatris. Cyber Law: Aspek Hukum dan Teknologi Informasi. Bandung: Refika Aditama, 2009.

Hanafi Amrani. Politik Pembaharuan Hukum Pidana. Yogyakarta: UII Press, 2019.

Kristian, and Yopi Gunawan. Penyadapan Dalam Hukum Positif di Indonesia. Bandung: Nuansa Aulia, 2013.

Kusrini. Sistem Pakar dan Teori Aplikasi Trading. Yogyakarta: Andi, 2012.

Maskun. Kejahatan Siber: Cybercrime: Suatu Pengantar. Jakarta: Kencana, 2013.

Rusli Muhammad. Potret Lembaga Pengadilan Indonesia. Yogyakarta: Grafindo Persada, 2006.

Soerjono Soekanto. Faktor-faktor yang Mempengaruhi Penegakan Hukum. Jakarta: Rajawali Pers, 2008.

Soerjono Soekanto. Pengantar Penelitian Hukum. Jakarta: UI Press, 2018.

Sofwan Jannah, and M. Naufal. Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif. Bandung: Remaja Rosdakarya, 2012.

Jurnal, Skripsi, Tesis Disertasi :

Andrew Christian Banjarnahor. "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus *Phising* Kredivo." Hermeneutika 6, no. 1 (Februari 2022).

Aziz Rahardyan. "Kredivo Lapor Kasus Cybercrime ke Polisi, Tagihan Pengguna Bengkak Garagara Promo Fiktif." Jurnal Hukum Pidana & Kriminologi 2, no. 3 (Desember 2021).

Banjarnahor, Andrew Christian. "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus *Phising* Kredivo." Hermeneutika 6, no. 1 (Februari 2022).

Dian Ekawati Ismail. "Cyber Crime di Indonesia." Delicti: Jurnal Hukum Pidana 6, no. 3 (April 2021).

Tony Yuri Rahmanto. "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik (Legal Enforcement Against Fraudulent Acts in Electronic-Based Transactions)." Jurnal Penelitian Hukum De Jure 19, no. 1 (Maret 2019).

Peraturan Perundang-Undangan :

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-undang Nomor 73 Tahun 1958 tentang Perubahan Atas Undang-undang Nomor 1 Tahun 1946 tentang Kitab Undang-undang Hukum Pidana (KUHP)

Undang-undang Nomor 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana (KUHAP)

Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia

Undang-undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman

Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi Dan Korban

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

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Putusan Pengadilan

Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN. Bjb