ISSN : 2301-7295
e-ISSN : 2657-2494

TINJAUAN ASAS LEGALITAS MENGENAI RUMUSAN PENGATURAN TINDAK PIDANA *PHISING* DALAM HUKUM PIDANA INDONESIA

Roro Indah Pramodhawardani, Mahfudz Fahrazi
Magister Hukum, Universitas Islam Kadiri
Email: roroindahp@gmail.com

ABSTRAK

Lahirnya UU Nomor 19 Tahun 2016 tentang Perubahan atas jo. UU Nomor 11 Tahun 2008 tentang ITE dikarenakan KUHPidana yang jangkauannya tidak mampu menghalau tindak pidana yang terus bermunculan, Namun meskipun sudah terdapat pembaharuan pengaturannya kasus tindak pidana ini masih menunjukkan angka tertinggi diantara kasus *cybercrime* yang lainnya. Rumusan masalahnya ialah Bagaimana karakteristik dari tindak pidana *phising* dan bagaimana rumusan pengaturan terkait *phising* di dalam Hukum Pidana Indonesia menurut tinjauan asas legalitas. Jenis penelitian yuridis normatif dengan teknik analisa deskriptif kualitatif dan melalui pendekatan peraturan perundang-undangan dan pendekatan konseptual. Berdasarkan hasil penelitian data, menyatakan bahwa Indonesia telah menempati urutan teratas selaku negara yang menjadi *hosting* situs *phising* domain.id. Hal tersebut disebabkan karena substansi hukum yang lemah dalam mengatur kejahatan itu.
Kata Kunci: Substansi Hukum, Phising, Internet

ABSTRACT

The existence The enactment of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) was due to the limited scope of the Criminal Code (KUHP) in deterring continuously emerging criminal acts. However, despite the regulatory updates, cases of this criminal activity still show the highest figures among other cybercrime cases. The problem formulation is how to characterize phishing crimes and how to formulate regulations related to phishing in Indonesian Criminal Law according to the principle of legality. This is a normative juridical research with qualitative descriptive analysis technique and through the approach of legislation and conceptual approach. Based on the research data, it is stated that Indonesia has ranked at the top as a country hosting phishing sites with the domain .id. This is due to the weak legal substance in regulating such crimes.
Keywords: Legal Substance, Phising, Internet

A. PENDAHULUAN

Dewasa ini terdapat tindak kejahatan yang sangat marak terjadi di Indonesia yang disebut dengan *phising*. *Phising* dalam artian singkatnya merupakan tindakan kejahatan dengan menggunakan teknik perekayasaan sosial dalam melancarkan aksinya. Kegiatan dibidang siber ini dilaksanakan oleh pihak tertentu yang ingin mengekploitasi kelemahan sistem serta kesadaran penyandangnya terhadap kegiatan virtual. Pelaku dalam kejahatan ini memiliki upaya untuk menipu korban yang sasaran utamanya meraup informasi atau data pribadi dari korban, yang bentuknya seperti *username*(id), *password* dan rincian kartu kredit Keberadaan UU Nomor 19 Tahun 2016 tentang Perubahan atas jo. UU Nomor 11 Tahun 2008 tentang ITE dikarenakan KUHPidana yang jangkauannya tidak mampu menghalau

Menurut Yudho Giri Sucahyo, Ketua PANDI (Pengelolaan Nama Domains Internet di Indonesia) menjelaskan bahwa tercatat jumlah *phising* kurun waktu 5 tahun terkahir telah mencapai angka 34.622, dimana serangan *phising* unik pada kuartal 3 tahun 2022 adalah 7.988. Sasaran penyerangan *phising* pada kuartal 3 2022 adalah lembaga pemerintahan. Selain, itu tercatat domain unik yang dipergunakan untuk meluncurkan *phising* yakni 181 kasus.[1] Selanjutnya, dalam catatan IDADX (*Indonesia Anti Phising Data Exchange*) menyatakan pada tahun 2022 kuartal 4 jumlah *phising* kurun waktu 5 tahun yakni 42.442, sedangkan tahun 2022 sendiri dalam kuartal 4 terdapat 6.206 laporan, laporan per-bulan

[1] Praditya Fauzi Rahman, "*Ada 34.622 Kasus Phising di Indonesia Selama 5 Tahun Terakhir*" https://www.detik.com/jatim/berita/d-6483650/ada-34622-kasus-phising-di-indonesia-selama-5-tahun-terakhir. Akses 30 September 2023.

ISSN : 2301-7295
e-ISSN : 2657-2494

kuartal 4 2022 yakni Oktober 2.318, November 2.779, Desember 1.009. Sasaran utama pada tahun 2022 kuartal 4 ini ialah Lembaga keuangan 54%, posisi kedua e-commerce 31% yang mengalami adanya perubahan posisi pada sebelumnya. Sehingga, dalam tahun 2022 kuartal 3 mengalami peningkatan disbanding dengan kuartal 2 yakni 9.428 laporan.[2] Tahun 2023, tercatat 26.675 kasus *phising* pada kuartal pertama tahun 2023 telah tercatat pada IDADX. Sedangkan sebagaimana telah disebutkan diatas bahwa pada kuartal 4 tahun 2022 terdapat 6.206 dimana jumlah kenaikannya sebanyak 20.569.[3]

IDADX menyatakan terdapat sepuluh nama brand atau organisasi yang menjadi serangat dari target *phising* pada kuartal 4 tahun 2022 yakni Morrisons; First National Bank of South Africa; Microsoft; Bank BRI; Facebook; Malicious Domain; BNP Paribas; British Telecom; Santander; Wells Fargo. Selain itu IDAX menyatakan bahwa Indonesia telah menempati urutan teratas selaku negara yang menjadi *hosting* situs *phising* domain.id selama kuartal 4 tahun 2022, silanjutkan pada posisi kedua yakni USA.[4] Berdasarkan data diatas menunjukkan bahwa tingginya kasus *phising* di Indonesia melewati tahun-ketahun hingga lima tahun terakhir meskipun sudah terdapat Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menanggulanginya.

Sebelum lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah mengalami perbuahan sebanyak dua kali (yang selanjutnya akan disebut dengan UU ITE), penegak hukum menggunakan instumen hukum KUHPidana dengan pasal penipuan. Pastinya para penegak hukum harus mengeluarkan tenaga ekstra dalam melakukan penafsiran pasal demi pasal tersebut agar bisa dipergunakan untuk mejerat tindak pidana *phising* ini. Pada dasarnya *phising* ini akarnya adalah tindak pidana penipuan, namun apabila ditelaah lebih jauh dari pengertiannya, maka jelas *phising* memiliki perbedaan dengan tindak pidana penipuan biasa yang terdapat dalam Pasal 378 KUHPidana.

Cybercrime yang berupa *phising* ini di Indonesia dimungkinkan untuk dikenakan Pasal 35 Juncto Pasal 51 ayat (1) UU ITE. Namun, pasal *aquo* masih belum menjelaskan secara tegas dan jelas mengenai konsep *phising* sendiri, oleh karena itu masih belum dapat ditarik suatu kesimpulan bahwa apakah tindak pidana *phising* ini bisa dikategorikan sebagai tindak pidana di dalam UU ITE dikarenakan uraian kejahatan *phising* ini bisa terjadi apabila sang pelaku memiliki kesengajaan dalam tujuannya agar dapat memancing korban dalam membeberkan informasi pribadinya ke pelu sehingga pelaku bisa dengan mudah mengambil alih akses akun dari korban. Sedangkan, pasal *aquo*, menyatakan bahwa tujuan dari *phising* ini merupakan tindak pidana dimana pelaku membuat situs palsu yang seolah-olah mirip dengan aslinya (otentik). Selanjutnya, *phising* ini juga dapat dikenakan pasal 28 Juncto Pasal 45A ayat (1) UU ITE dikarenakan *phising* juga merupakan suatu kebohongan yang dilakukan oleh pelaku untuk menyesatkan korbannya, dimana sang korban yang dibohongi inipun akan berimbas memberikan informasi kepada sang pelaku. Namun pasal *aquo* pun belum memiliki kejelasan dalam unsur pasalnya mengenai pembuatan situs palsu yang digunakan untuk melancarkan aksi pelaku. Hal ini menimbulkan kekaburan hukum terkait aturan manakah tindak pidana *phising* seharusnya dapat dijerat.

Dalam rumusannya, Satjipto Rahardjo menyatakan bahwa penegakan hukum ialah proses untuk mewujudkan harapan hukum menjadi kenyataan.[5] Yang dimaksud dengan harapan hukum merupakan suatu hasil pemikiran dari pembentuk undang-undang yang dileburkan dalam betuk peraturan hukum.[6] Sehingga, dengan terbentuknya suatu aturan harapannya dapat

[2] Sari, U. I. P. *Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia.* Jurnal Studia Legalia, 2(01), 58-77 (2021). Hlm 3.

[3] Nada Naurah, "*Serangan Phising di Indonesia Terus Meningkat, Ini Datanya".* https://goodstats.id/article/serangan-phishing-di-indonesia-terus-meningkat-ini-statistiknya-U8VdY Akses 30 September 2023.

[4] *Ibid.* Hlm 4.

[5] Satjipto Rahardjo. *Masalah Penegakan Hukum*. (Bandung: Sinar Baru, 1983) Hlm. 24

[6] Rahman. 2020. "*Penegakan Hukum Di Indonesia."* Jurnal Al Himayah Vol 4.1.142-159 (2020) Hlm. 6.

ISSN : 2301-7295
e-ISSN : 2657-2494

efektif dalam menekan angka suatu kejahatan. Namun, tingginya kasus phising yang ada di Indonesia yang mengalami kenaikan signifikan setiap tahunnya menandakan kurang efektifnya penegakan hukum yang ada di suatu negara.

Menurut Soerjono Soekanto 5 (lima) faktor yang dapat mempengaruhi suatu penegakan hukum, ialah: [7]

1. Faktor substansi hukumnya, yakni berkaitan dengan aturan hukum;
2. Faktor penegak hukumnya, yakni peran aparat dalam menegakkan hukum yang ada;
3. Faktor sarana dan fasilitas yang mendukung suatu proses penegakan hukum;
4. Faktor masyarakatnya, yakni pengetahuan masyarakat terhadap norma hukum yang berlaku serta dimana hukum itu diberlakukan;
5. Faktor budaya hukumnya, yakni hubungannya dengan pengaruh perilaku yang ada di masyarkat sebelum dan setelah mengetahui adanya norma hukum yang berlaku.

Selanjutnya, Lawrence M. Friedman menyatakan bahwa substansi hukum, struktur hukum serta budaya hukum ialah suatu satu kesatuan yang ada di sistem hukum dan memiliki pengaruh didalam penegakan hukumnya.[8] Kedua teori tersebut memiliki kesamaan yakni substansi hukum merupakan salah satu faktor yang dapat memberikan pengaruh pada penegakan hukum. Substansi hukum dapat dikatakan baik apabila berdasarkan landasan yuridis, sosiologis dan filosofis.[9] Berkatian dengan itu, maka rekonstruksi sangat diperlukan pada kebijakan tindak pidana *phising*. Dalam suatu kebijakan, rekonstruksi adalah bentuk ketegasan terhadap penanganan suatu tindak pidana, sehingga tidak jadi kekeliruan yang bisa merugikan masyarakat.[10] Jangan sampai hadirnya perundang-undang terpana oleh adanya perkembangan teknologi berdampak pada munculnya *overlegislate regulation* yang mana sejatinya akan membawa dampak tidak baik.[11]

Rumusan Masalah

Bagaimana karakteristik dari tindak pidana *phising*?

Bagaimana rumusan pengaturan terkait *phising* di dalam Hukum Pidana Indonesia menurut tinjauan asas legalitas?

B. METODE PENELITIAN

Jenis Penelitian

Penelitian ini adalah jenis penelitian yuridis normatif yakni dengan mengkaji adanya produk-produk hukum yang berupa peraturan perundang-undangan ataupun melakukan penelaahan system kaidah, dengan sistematik hukum yang sedemikian rupa sehingga hukum yang dijadikan sebagai suatu ilmu kaidah bisa dipahami dengan jelas.[12]

Pendekatan Penelitian

Hukum ialah kaidah dengan sifat memaksa dan ketidak ada individu yang melakukan pelanggaran kaidah tersebut maka akan terancam dengan sanksi yang bentuknya nyata.[13] Unruk memperoleh suatu kebenaran yang ilmiah sesuai dengn harapan, oleh karena itu dalam penelitian ini menggunakan beberapa pendekatan, seperti pendekatan konseptual (*conseptual approach*) serta pendekatan undang-undang (*statute approach*).

C. PEMBAHASAN

Karakteristik Tindak Pidana *Phising*

Phising ini dikenal pula sebagai *Carding* atau *Brand Spoorfing* suatu layanan untuk menipu korbannya dengan menyediakan sebuah keamanan dan keabsahan dari transfer suatu data yang dilakukan oleh orang tersebut. Felten et al Spoofing mendefinisikan *phising* sebagai teknik untuk mendapatkan akses

[7] Soerjono Soekanto. *Faktor-faktor yang Mempengaruhi Penegakan Hukum*. (Cetakan VI. Jakarta. Rajawali, 2002) Hlm.5.

[8] Saifullah. *Refleksi Sosiologi Hukum*. Bandung. Refika Aditama dalam Mahanani, A. E. E. 2019. *Rekonstruksi budaya hukum berdimensi Pancasila dalam upaya penegakan hukum di Indonesia*. Jurnal Yustika. Media Hukum dan Keadilan, Vol 22(01). (2007) Hlm 2.

[9] Saifullah. (2007). *Ibid*. Hlm 5.

[10] Nur Baiti Aprilianti. *TINDAK PIDANA PENCEMARAN NAMA BAIK DI MEDIA SOSIAL (Studi Komparatif antara Hukum Islam dan Hukum Pidana)*. Skripsi. Institute Agama Islam Negeri Purwokerto (IAIN) (2019). Hlm. 9.

[11] Barda Nawawi. *Bunga Rampai Hukum Pidana*. (Bandung: PT. Citra Aditya Bakti, 2000) Hlm. 40.

[12] Soedjono Dirdjosisworo. *Pengantar Imu Hukum*. (Bandung: Mandar Maju, 1994). Hlm 82.

[13] Jhonny Ibrahim. *Teori dan Metodologi Penelitian Hukum Normatif*. (Surabaya: Bayu Media, 2005) Hlm 51.

ISSN : 2301-7295
e-ISSN : 2657-2494

komputer yang dilakukan dengan cara tidak sah dan menimbulkan ancaman.

Berdasarkan pada definisi tersebut maka untuk dapat melangsungkan tindak pidana *phising,* pelaku harus membuat halaman palsu terlebih dahulu untuk mendapat data pribadi korban (secara melawan hukum). Halaman palsu tersebut dapat berupa link, website atau nama domain yang identik dengan yang aslinya yang berisikan username dan password untuk memancing korban agar memasukkan data pribadinya. Perbuatan penguasaan terhadap data identitas milik pribadi seseorang dengan cara melawan hukum disebut dengan *identity theft*.

Identity theft ini terjadi jika seseorang memperoleh atau mendapatkan, memiliki, mengirimkan, bahkan menggunakan informasi milik pribadi orang ataupun badan hukum dengan cara yang illegal yang maksudnya adalah untuk melakukan dan/atau berhubungan dengan adanya kegiatan penipuan, kebohongan dan tindakan kejahatan lainnya.[14] Tindakan ini jarang dilakukan untuk menjadikan informasi data pribadi untuk target tujuan utamanya, namun tindakan ini dilakukan sebagai suatu sarana dalam hal memperlancar kejahatan lain dan biasanya kegiatan ini dilakukan dalam bidang keuangan untuk memperkaya diri pelakunya dengan mengorbankan lembaga pemerintahan, keuangan, bisnis ataupun individu.[15] Atau dengan kata lain tindakan ini merupakan tindakan pendahuluan untuk saranan melakukan suatu tindak pidana.

Tindak pidana *phising* ini, terdapat 3 tahap besar:

Tahapan pertama, sebelum dapat melaksanakan tindak pidana *phising*, pelaku harus membuat halaman palsu terlebih dahulu untuk mendapat data pribadi korban (secara melawan hukum). Halaman palsu tersebut dapat berupa link, website atau nama domain yang identik dengan yang aslinya. Pelaku harus mendapatkan informasi elektronik milik orang lain terlebih dahulu, seperti pada informasi banking yakin username, password, nama ibu, nomor identitas pribadi dan lain sebagainya. Teknik *phising* yang dilakukan ini disebut sebagai *identity theft*.

Tahapan kedua, menggunakan data informasi pribadi dari akun korban untuk melakukan transaksi tanpa seizin dari pemegang akun sah.

Berdasarkan dari penjelasan diatas, maka dapat ditarik benang bahwa karakter dari tindak pidana phising ini selalu terdiri dari, minimal dua tindak pidana, yakni pertama membuat halaman palsu, kedua *identity theft,* ketiga menggunkan data informasi pribadi dari akun korban untuk melakukan transaksi tanpa seizin dari pemegang akun sah. Karakter yang dimiliki oleh tindak pidana phising ini dikualifikasikan sebagai *concursus* dalam hukum pidana.

Bersesuaian dengan penjelasan diatas, terdapat skema dari tindak pidana *phising* terdapat sebagai berikut:[16]

1. *Link Manipulations*, yakni membuat sebuah link atau web yang memiliki kemiripan dengan akun aslinya namun dengan ejaan yang sedikit berbeda sehingga terlihat seperti asli;
2. *Filter Evasion*, kegiatan mengecoh korban *Phising* dengan menngunakan email yang didalamnya terdapat tautan atau link yang dihubungkan dengan alamat web yang asli sehingga korban memberikan informasi pribadinya kedalam link tersebut.
3. *Website Phising/Forgery*, kegiatan memanfaatkan celah keamanan pada suatu website dan digunakan untuk memasang link di file multimedia. Kegiatan ini marak dilakukan dengan cara xss (*cross site scripting*) dimana pelaku menanamkan link palsu ke web yang aslinya.

Modus yang dilakukan oleh pelaku *phising* adalah melakukan jebakan terhadap korban agar tidak menyadari bahwa korban telah memberikan informasi pribadi miliknya kepada pelaku, pelaku phising menggunakan kalimat dengan rangkaian kebohongan serta

[14] OECD, Scoping Paper on Online Identity Theft, Ministerial Backgroud Report: DSTI/CP (2007)/FINAL, hlm 12, 2008, diunduh dari [10/12/2023]

[15] Depository Institutions of Financial Crimes Enforcement Network, Identity Theft: Trends, Patterns, and typologies Reported in suspicious Activity Reports, 2010, hlm 1, diunduh dari < http://www.fincen.gov/news_room/rp/reports/pdf/ID%20Theft.pdf>02 Desember 2023.

[16] Dian Rachmawati, 'Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber' (2014) 13 Jurnal SAINTIKOM.Hal.216.

ISSN : 2301-7295
e-ISSN : 2657-2494

tipuan muslihat, ciri umum yang dilakukan pelaku yakni terjadi di email, dimana pelaku mempermainkan kalimat dalam subjeknya dan isi dari email tersebut agar terlihat asli dan meyakinkan dengan permintaan untuk memberikan data agar bisa memverifikasi akunnya, disertai ancaman lain seperti akan adanya penutupan akun dalam jangka waktu tertentu, selanjutnya pelaku akan menggunakan kalimat yang halus, sopan dan professional seperti "*Dear Valued Customer*" karena mereka akan menjaring sebanyak-banyaknya target menggunakan link untuk menjaring korban.[17]

Selanjutnya, *Website Forgery* ditujukan hanya untuk menipu pengunjung web tersebut. Cara kerjanya yakni pelaku membuat website atau domain internet dimana dia menjadi host dari website tersebut dan pelaku akan membuat design semirip dan sedetail mungkin seperti website asli, baik dari pewarnaan, logo, objek, dan seterusnya, hal inilah yang mebuat target akan mengira bahwa yang mereka kunjungi adalah website yang sah, sehingga mereka akan mempercayakan data pribadinya baik seperti username dan password yang selanjutnya data tersebut akan disimpan dalam *database* pelaku.

Rumusan Pengaturan Terkait *Phising* dalam Hukum Pidana Indonesia menurut Tinjauan Asas Legalitas

Substansi hukum pidana mempunyai pernanan besar terhadap adanya penegakan hukum pidana di negara Indonesia. Peraturan dalam hukum pidana bisa dikatakan sebuah aturan yang baik jika penyusunan aturan itu menggunakan bahasa lugas dan jelas.[18] Hal ini menunjukan bahwa sejatinya peraturan di hukum pidana harus mempunyai unsur yang spesifik dan bahasa yang digunakan tidak menimbulkan maksud lain supaya tiada multitafsir dalam proses penerapan penegakan hukumnya. Unsur spesifik yang terdapat dalam hukum pidana bisa mencegah analogi dalam menafsirkannya. Olehnya, hukum pidana harus mempunyai kejelasan untuk mengatur apapun jenis dan unsur tindak pidana yang dimaksud.

Pada bab 2 sebelumnya penjabaran lebih lengkap mengenai asas legalitas telah diberikan, bahwa asas tersebut mengandung 3 makna. Kesatu, bahwa suatu peraturan/undang-undang harus tertulis (*lex certa*); Kedua, bahwa suatu peraturan/undang-undang harus memiliki kejelasan dan ketegasan dalam bahasanya agar tidak menimbulkan multitafsir (*lex certa*), Ketiga, bahwa suatu peraturan/undang-undang harus diterapkan secara ketat tanpa ada analogi (*lex stricta*). Ketiga makna tersebut harus dipenuhi dalam rangka penegakan hukum pidana di negara Indonesia. Seiring dengan hal itu, terlihat bahwa asas legalitas ini tidak hanya sebatas ada pada dimensional penegakan hukum namun juga pada pembentukan hukumnya. Hal ini terlihat pada syarat kedua yakni *lex certa* bahwa suatu aturan pidana harusalah jelas dan tidak multitafsir, proses pembentukan hukumnya haruslah disusun dengan bahasa-bahasa yang jelas dan tegas.

Kualitas peraturan hukum pidana pada dasarnya bisa diukur menggunakan syarat asas legalitas. Bahwa aturan hukum pidana bisa dikatakan aturan yang baik jika peraturan itu disusun menggunkan bahasa-bahasa yang jelas dan tegas, dalam arti rumusan unsur tindak pidana yang dimuat dalam aturan tersebut haruslah spesifik dan tidak mempergunakan bahsa yang ambigu. Merumuskan unsur tindak pidana yang lebih spesifik dilakukan agar menghalangi kemungkinan dipakainya penafsiran analogi Dimana hal itu dilarang dalam hukum pidana. Maka, dalam penyusunannya aturan hukum pidana ini membutuhkan aturan yang lengkap dalam hal mengatur setiap jenisnya tindak pidana diiringi dengan sanksi pidana.

Begitu pula dalam penyusunan aturan hukum pidana mengenai *phising*, sebaiknya dalam perumusannya menggunakan bahasa yang sifatnya umum. Hal itu pasti akan lebih memperingan kinerja hakim dalam hal penafsirannya sehingga suatu kepastian hukum akan bisa tercapai. Penggunaan bahasa yang sifatnya spesifik akan memberikan dampak penyempitan ruang lingkup larangan perbuatan. Maka dari itu diperlukan

[17] Nur Khalimatus Sa'diyah, 'Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik', (2012), 17 Perspektif. Hal.84.

[18] Said Noor Prasetyo. 2016. *Rumusan Pengaturan Credit Card Fraud dalam Hukum Pidana Indonesia Ditinjau dari Asas Legalitas*. Legality. Vol. 24, No. 1. Hal. 111.

ISSN : 2301-7295
e-ISSN : 2657-2494

perumusan tindak pidana yang jauh lebih lengkap terhadap setiap jenis tindak pidana *phising*.

Pada poin sebelumnya penulis telah menjabarkan bahwa tindak pidana *phising* ini karakteristiknya berbeda dengan tindak pidana pada umumnya. Agar bisa menyelesaikan tindak pidana phising ini butuh beberapa tahap. Tahapan pertama, sebelum dapat melaksanakan tindak pidana *phising*, pelaku harus membuat halaman palsu terlebih dahulu untuk mendapat data pribadi korban (secara melawan hukum). Halaman palsu bisa dibuat sendiri oleh pelaku ataupun membelinya kepada domain *owner* yang lain. Halaman tersebut dapat berupa link, website atau nama domain yang identik dengan yang aslinya. Selanjutnya, pelaku harus mendapatkan informasi elektronik milik orang lain terlebih dahulu, seperti pada informasi banking yakin username, password, nama ibu, nomor identitas pribadi dan lain sebagainya. Teknik *phising* yang dilakukan ini disebut sebagai *identity theft*.

Tahapan kedua, menggunakan data informasi pribadi dari akun korban untuk melakukan transaksi tanpa seizin dari pemegang akun sah. Pada dasarnya kedua tahapan tersebut memiliki kesamaan yakni menggunakan link atau web atau nama domain untuk mengambil identitas targetnya dan digunakan untuk bertransaksi, namun ketiga tahapan tersebut mempunyai perbedaan unsur perbuatan yang berbeda satu dengan lainnya.

Pada penentuan kualifikasi tindak pidana yang sekaligus hukum pidana yang mengaturnya maka perlu melihat berdasarkan bentuk-bentuk perbuatan yang digunaan oleh pelaku. Sebagaimana bab sebelumnya penjabaran mengenai tahapan yang dilakukan oleh pelaku tindak pidana *phising* dalam mengambil suatu keuntungan milik orang lain telah dijelaskan. Beberapa bentuk tahapannya adalah sebagai berikut:

Membuat halaman palsu berupa link, website atau nama domain yang memiliki kemiripan dengan aslinya, menyebarkan kepada orang lain dan mengambil identitas milik orang lain.

Pada bentuk pertama ini pelaku akan menciptakan, memanipulasi, melakukan perubahan link, website atau nama domain yang meyakinkan dan menaruh detail kecil semirip mungkin dengan situs legalnya sehingga akan membuat targetnya meyakini bahwa hal tersebut adalah hal yang asli atau otentik dan tanpa sadar memasukkan informasi data penting pribadinya.

Apabila dipahami, terhadap rumusan pada perbuatan tahap pertama diatas sejatinya bisa dijatuhkan pidana Pasal 378 KUHPidana, Pasal 263 KUHPidana dan Pasal 362 KUHPidana. Pasal 378 sejatinya mengatur mengenai penipuan yakni berbunyi bahwa barangsiapa secara melawan hukum menggunakan nama atau martabat palsu untuk menguntungkan diri sendiri atau orang lain dengan tipu muslihat atau rangkaian kebohongan yang bertujuan menggerakan orang tersebut untuk menyerahkan sesuatu atau memberi sesuatu diancam karena penipuan dengan pidana penjara paling lama empat tahun.

Jika berbicara tentang *phising,* unsur menguntungkan diri sendiri pada Pasal 378 KUHPidana dapat ditarik kesimpulan pelaku *phising* menggunakan kemampuan yang mereka miliki untuk menjaring keuntungan dari orang lain meskipun tidak selalu dalam bentuk uang/barang.

Penjelasan unsurnya adalah sebagai berikut:

Unsur memakai nama palsu atau martabat palsu dengan tipu muslihat atau rangkaian kebohongan, sering digunakan oleh pelaku untuk mengecoh targetnya, *phising* ini digunakan untuk memancing targetnya dengan cara memakai nama atau martabat dari suatu organisasi atau instansi tertentu, selanjutnya isi dari emailnya pun harus identik dengan aslinya agar melancarkan aksi pelaku.

Unsur menggerakkan orang lain untuk menyerahkan suatu barang, dalam hal ini sasaran utama tindak pidana phising bukanlah sebuah barang, namun data informasi pribadi targetnya dimana hal ini bisa saja dianggap memenuhi unsur pasal 378 KUHPidana karena sejatinya data informasi pribadi seseorang merupakan benda yang tak berwujud tapi bisa dibuktikan keberadaannya.

Selanjutnya mengenai Pasal 263 KUHPidnana yang berkaitan dengan pemalsuan surat. Bahwa pada pejelasan sebelumnya tindak pidana *phising* ini sejatinya merupakan tindak pidana penipuan yang dilakukan oleh pelaku dengan cara membuat email palsu atau situs palsu yang identik dengan aslinya. Perjelasan lebih lanjut

mengenai makna phising dalam Hukum Pidana Indonesia masih belum diatur lebih lanjut, maka Pasal 263 KUHPidana mengalami perluasan maknanya, yakni email dalam hal ini dianggap sebagai sebuah surat dalam bentuk elektronik.

Penjelasan lebih lanjut mengenai unsur pasalnya, ialah:

Unsur membuat surat palsu atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan atau pembebasan hutang, atau yang diperuntukan sebagai buktu daripada suatu hal, bahwa *phising* ialah tindak pidana yang dasarnya penipuan, oleh karenanya pelaku tindak pidana ini membuat email (surat elektronik) dengan mengatasnamakan suatu instasi, organisasi atau perusahaan tertentu supaya email itu dianggap otentik, dimana isi dari email (surat elektronik) tersebut berupa link untuk menjaring informasi milik korbannya.

Unsur dengan maksud untuk memakai atau menyuruh orang lain memakai surat tersebut seolah-olah isinya benar dan tidak palsu. Unsur ini menunjukkan bahwa tujuan dari pelaku tindak pidana *phising* ini adalah untuk menuntun pelaku dengan memanfaatkan email palsu dengan tujuan untuk mendapatkan informasi data pribadi korban yang akan digunakan oleh pelaku tindak pidana ini dengan sewenang-wenang seperti berbelanja menggunakan kartu kreditnya atau uang rekening dari korban,[19] hal-hal tersebut diatas telah memenuhi unsur dari pasal 263 KUHPidana terkait ancaman pemidanaan jika pemakaian tersebut menyebabkan kerugian pada korban akibat pemalsuan surat.

Unsur Pasal 362 KUHPidana terkait pencurian pula menjadi salah satu dari acuan oleh penuntut umum dalam mendakwakan tuntutan pada pelaku phising karena tujuan pelaku *phising* ini sendiri adalah unruk mengambil sesuatu ataupun seluruh milik korban yang menjadi targetnya dengan maksudnya untuk memiliki secara melawan hukum, dalam hal ini pelaku tindak pidana *phising* secara umum mempunyai tujuan untuk mencuri data informasi pribadi milik korbannya dengan tujuan menggunakan data informasi pribadi tersebut demi keuntungan pribadi pelaku.

KUHPidana sendiri dalam mengatur mengenai hukum pidana dalam dunia maya pembahasannya masih dilakukan secara umum, di Indonesia dikenal asas "*Lex Specialis derogate legi Generalis"* maknanya bahwa suatu aturan hukum khusus akan mengesampingkan aturan hukum yang lebih umum. Bahwa Indonesia telah memiliki aturan khusus dalam hal mengatur terkait tindak pidana yang dilakukan di dunia maya yakni Undang-Undang Informasi dan Transaksi Elektronik atau lebih dikenal dengan UU ITE.

Apabila dipahami, maka rumusan perbuatan dalam *phising* tahap satu ini dalam UU ITE adalah dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, menciptakan halaman palsu dengan tujuan untuk mendapatkan data informasi pribadi milik orang lain. Berdasarkan rumusan perbuatan diatas dapat dipahami bahwa perbuatan itu terkualifikasi dalam Pasal 35 UU ITE dan Pasal 28 UU ITE.

Memperhatikan pasal tersebut dapat diketahui bahwa perbuatan pada tahap kesatu ini memenuhi rumusan terkait terciptanya halaman palsu yang tujuannya agar dianggap sebagai halaman yang otentik/asli. Namun, tindak pidana phising bukan semata hanya memanipulasi atau membuat sebuat situs/halaman palsu dan menggunakan email sebagai mediannya untuk mengecoh para targetnya tetapi pelaku tindak pidana phising juga melakukan suatu kebohongan, dengan kata lain untuk menyesatkan korbannya sehingga mengalami kerugian. Pada pasal *aquo* belum memenuhi rumusan mengenai suatu kebohongan untuk menyesatkan tujuan lain agar data informasi pribadi orang dapat diambil oleh pelaku. Terhadap perbuatan ini pada dasarnya dapat dikualifikasikan sebagai suatu kebohongan yang terdapat pada Pasal 28 ayat (1) UU ITE.

Untuk bisa atau tidaknya Pasal 28 ayat (1) UU ITE menjerat perbuatan diatas maka hal yang perlu diperhatikan ialah melihat kecocokan unsur pasal dan unsur perbuatannya. Demi melancarkan aksinya pelaku pasti memiliki unsur kesengajaan untuk mendistribusikanan/atau mentransmisikan

[19] Pengadilan Negeri Cirebon, "Putusan No : 155/Pid.Sus/2018/PN.Cbn".Hal. 29.

ISSN : 2301-7295
e-ISSN : 2657-2494

informasi pemberitahuan bohong atau informasi yang sesat sehingga membuat targetnya terpancing untuk mengaksesnya dan targetnya tentu akan mendapatkan kerugian dalam hal ini.

Berdasarkan penjelasan dua pasal diatas terhadap tahap pertama tindak pidana *phising* ini dapat terlihat perbedaan pengaturan dalam rumusan pasalnya. Bahwa pada Pasal 35 UU ITE hanya mengatur mengenai pembuatan situs atau halaman palsu yang dibuat oleh pelaku yang identik dengan situs asli. Oleh karena itu, dalam satu tahap perbuatan terdapat beberapa unsur yang berbeda, dalam hal ini perbuatan *phising* itu tidak hanya pelaku membuat suatu halaman palsu yang mirip dengan halaman aslinya saja tetapi juga terdapat unsur kebohongan yang dilakukan oleh pelaku untuk menyesatkan atau menipu targetnya hingga mengalami kerugian dikarenakan data informasi pribadi miliknya diketahui oleh pelaku.

Menggunakan data informasi pribadi dari akun milik orang lain untuk melakukan transaksi elektronik tanpa seizin dari pemegang akun sah.

Pada perbuatan di tahap kedua ini, pelaku mengelabuhi korban dengan cara berpura-pura sebagai suatu pihak yang sah dengan menyebutkan ataupun memberikan informasi palsu kepada korban agar korban bersedia memberikan data informasi pribadinya kepada pelaku.

Rumusan perbuatan *phising* dalam tahap ini ialah pelaku dengan sengaja dan tanpa hak menggunakan informasi identitas pribadi korban yang telah didapatkannya akibat dari rancangan halaman palsu yang telah diciptakan pelaku dan menyebarkan halaman palsu tersebut dengan menggunakan identitas yang palsu pula untuk mengambil keuntungan dengan melakukan transaksi elektronik tanpa sepengetahuan oleh pemilik akun yang sah. Merujuk pada rumusan perbuatan diatas pada dasarnya hal ini bisa dikualifikasikan atas tindak pidana penipuan yang diatur dalam Pasal 378 KUHPidana.

Kecocokan Pasal 378 dengan perbuatan tersebut dapat dilakukan dengan memperhatikan setiap unsur pasal serta unsur perbuatannya. Untuk melancarkan aksinya pelaku pasti memakai nama palsu dan keadaan palsu. Dalam transaksi elektronik ini, sang pelaku mengaku dirinya sebagai pihak yang sah dengan memakai nama suatu pihak atau institusi. Tentunya hal ini dapat dilakukan dengan sangat mudah karena transaksi elektronik kini dilakukan tanpa tatap muka dan melalui jarak jauh.

Pada saat proses pemindahan data informasi pribadi dari pemilik akun asli kepada pelaku, hanya perlu memberikan data informasi pribadi kedalam *database* halaman palsu yang telah dibuat oleh pelaku. Pada saat itulah pelaku akan melakukan transaksi elektronik yang menyebabkan kerugian terhadap korbannya yakni dengan memindahkan sejumlah nominal yang telah diincarnya kedalam kantong milik pribadi sang pelaku.

Berdasarkan penjelasan diatas, dapat diambil pemahaman bahwa ada sedikit perbedaan dalam hal bentuk perbuatan ditahap ketiga ini dengan rumusan yang terdapat di Pasal 378 KUHPidana. Perbedaan itu terletak pada tujuan dari pelakunya, dimana tujuan dari pelaku dalam tindak pidana penipuan adalah agar korban memberikan barangnya; membuat hutang; ataupun menghapuskan piutang. Sedangkan barang yang dimaksud dari pelaku *phising* tahap ketiga ini adalah suatu data informasi elektronik dimana hal tersebut tidak disebutkan dalam pasal *aquo* meskipun sejatinya data informasi tersebut dianggap sebagai barang yang dapat dibuktikan keberadaannya.

Tidak lepas dari pada itu, tidak berarti bahwa suatu perbuatan dapat dilepas begitu saja karena selalu terdapat konsekuensi disetiap tindak pidana yang dilakukan. Perbuatan tersebut telah dkategorikan sebagai tindak pidana mengingat semakin tingginya angka kejadian dan besar kerugian yang telah ditimbulkan. Banyak pasal yang digunakan oleh penegak hukum untuk memberantas tindak pidan aini, salah satunya adalah Pasal 28 ayat (1) UU ITE yang dilihat dari rumusannya memiliki keterkaitan dengan tahap kedua diatas, yakni pasal yang mengatur mengenai kebohongan yang dilakukan oleh seseorang dalam transaksi elektornik, yakni Pasal 28 ayat (1) UU ITE.

Untuk bisa atau tidaknya Pasal 28 ayat (1) UU ITE menjerat perbuatan diatas maka hal yang perlu diperhatikan ialah melihat kecocokan unsur pasal dan unsur perbuatannya. Unsur dengan sengaja artinya terdapat kesalahan yang berupa kesengajaan

ISSN : 2301-7295
e-ISSN : 2657-2494

dalam perbuatan "mendistribusikanan/atau mentransmisikan Informasi Elektronik dan/ atau Dokumen Elektronik" tetapi dalam UU ITE ini masih belum didapati mengenai penjelasan lebih lanjut terhadap ketiga perbuatan tersebut baik dari sisi Informasi dan Teknologi maupun sisi yuridisnya. Selanjutnya, berkaitan dengan kecocokan rumusan perbuatan pada tindak pidana dan pasal ini yakni demi melancarkan aksinya pelaku pasti memiliki unsur kesengajaan untuk mendistribusikanan/atau mentransmisikan informasi pemberitahuan bohong atau informasi yang sesat sehingga membuat targetnya terpancing untuk mengaksesnya dan targetnya tentu akan mendapatkan kerugian dalam hal ini adalah dalam transaksi elektronik dan barang elektronik.

Berdasarkan pada penjabaran diatas, dapat dipahami bahwa dalam hal melakukan tindak pidana *phising* tidak hanya membuat atau memanipulasi situs/halaman palsu saja tertapi juga terdapat rumusan perbuatan lain yakni disebarkan melalui media tertentu seperti email (surat elektronik) dengan detail kalimat yang meyakinkan agar dapat menipu targetnya, sehingga dalam hal ini terdapat rumusan perbuatan kebohongan yang tujuannya menipu dan menyesatkan targetnya. Hal tersebut menyebabkan tindak pidana *phising* ini tidak dapat disamakan dengan tindak pidana konvensional biasanya oleh karena itu tidak dapat disamakan dengan perbuatan yang diatur dalam KUHPidana karena perbuatannya berkaitan dengan dunia maya dan data informasi yang sifatnya elektronik.

Phising merupakan satu kesatuan dala hal membuat situs/halaman palsu yang identik dengan situs/halaman sahnya dengan perbuatan bohong yang dilakukan oleh pelaku mengirimkan sebuah teks yang isinya informasi palsu untuk mendapatkan data informasi rahasia sesorang baik melalui email atau media lain sehingga informasi tersebut diketahui oleh pelaku dan mengambil keuntungan dari hal trsebut. Merujuk pada hal tersebut, rumusan perbuatan yang dimuat dalam UU ITE dalam hal mengatur tindak pidana *phising* tidak semuanya dapat dijangkau oleh UU ITE. Masih terdapat beberapa rumusan perbuatan yang tidak diatur atau dikriminalisasikan hukum pidana Indonesia. Selain itu, masih terdapat beberapa aturan yang membutuhkan penafsiran analogi agar dapat menjangkau perbuatan yang terdapat dalam tindak pidana *phising*, padahal dalam asas legalitas melarang adanya penggunaan penafsiran analogi dalam aturan hukum pidana.

D. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan tersebut diatas, maka dapat diambil kesimpulan sebagai berikut:

Bahwa tindak pidana *phising* mempunyai karakteristik perbedaan dengan tindak pidana lainnya. Terdapat dua tahapan untuk melancarkan tindak pidana ini. Pertama, sebelum dapat melaksanakan tindak pidana *phising*, pelaku harus membuat halaman palsu terlebih dahulu untuk mendapat data pribadi korban (secara melawan hukum) dan menyebarkan kepada orang lain dan mengambil identitas milik orang lain. Halaman palsu tersebut dapat berupa link, website atau nama domain yang identik dengan yang aslinya. Pelaku harus mendapatkan informasi elektronik milik orang lain terlebih dahulu, seperti pada informasi banking yakin username, password, nama ibu, nomor identitas pribadi dan lain sebagainya. Teknik *phising* yang dilakukan ini disebut sebagai *identity theft*. Kedua, menggunakan data informasi pribadi dari akun korban untuk melakukan transaksi tanpa seizin dari pemegang akun sah.

Bahwa rumusan pengaturan terkait *phising* di dalam Hukum Pidana Indonesia menurut asas legalitas apabila mengacu pada kedua tahapan pada tindak pidana *phising* ini, rumusan perbuatan yang dimuat dalam UU ITE dalam hal mengatur tindak pidana *phising* tidak semuanya dapat dijangkau oleh UU ITE. Masih terdapat beberapa rumusan perbuatan yang tidak diatur atau dikriminalisasikan hukum pidana Indonesia. Selain itu, masih terdapat beberapa aturan yang membutuhkan penafsiran analogi agar dapat menjangkau perbuatan yang terdapat dalam tindak pidana *phising*, padahal dalam asas legalitas melarang adanya penggunaan penafsiran analogi dalam aturan hukum pidana.

E. DAFTAR PUSTAKA

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana.

Undang-Undang No. 19 Tahun 2016 juncto Undang-Undang No. 11 Tahun 2008

tentang Informasi dan Transaksi Elektronik.

Buku Dan Jurnal

Dirdjosisworo, S. (1994). *Pengantar Imu Hukum*. Bandung: Mandar Maju.

Ibrahim, J. (2005). Teori dan Metodologi Penelitian Hukum Normatif, Surabaya. *Bayumedia Johny Ibrahim, Teori dan Metodelogi Penelitian Hukum Normatif (Surabaya, Bayumedia)*.

Ibrahim, F. M. A., & Arifin, M. A. (2025). The Quran And Positive Law: A Philosophical Review In A Normative Legal Perspective. *Klausula (Jurnal Hukum Tata Negara, Hukum Adminitrasi, Pidana Dan Perdata)*, *4*(1), 32-38.

Prasetyo, S. N. (2016). Rumusan Pengaturan Credit Card Fraud Dalam Hukum Pidana Indonesia Ditinjau Dari Asas Legalitas. *Legality*, *24*(1), 101-119.

Pengadilan Negeri Cirebon, "Putusan No : 155/Pid.Sus/2018/PN.Cbn".Hal. 29.

Rachmawati, D. (2014). Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber'.13 Jurnal SAINTIKOM. Hlm 216. Rahardjo, S. (1980). *Masalah penegakan hukum: Suatu tinjauan sosiologis*. Sinar Baru.

Rahman. (2020). *Penegakan Hukum Di Indonesia.* Jurnal Al Himayah: Vol 4.1.142-159.

U. I. P. Sari, (2021). *Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia*. Jurnal Studia Legalia, 2(01), 58-77.

Sa'diyah, N.K. (2012). Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik 17 Perspektif. Hlm. 84 Soerjono, S., & Mamudji, S. (1995). Penelitian Hukum Normatif suatu tinjauan singkat.

Nawawi, B. (2000). *Bunga Rampai Hukum Pidana*. Bandung: PT. Citra Aditya Bakti.

Nur Baiti, A. (2019). *TINDAK PIDANA PENCEMARAN NAMA BAIK DI MEDIA SOSIAL (Studi Komparatif antara Hukum Islam dan Hukum Pidana)* (Doctoral dissertation, IAIN Purwokerto).

Ibrahim, F. M. A., & Arifin, M. A. (2025). The Quran And Positive Law: A Philosophical Review In A Normative Legal Perspective. *Klausula (Jurnal Hukum Tata Negara, Hukum Adminitrasi, Pidana Dan Perdata)*, *4*(1), 32-38.