Penegakan Hukum Kejahatan Siber Berbasis *Phising* dalam Bentuk *Application Package Kit* (APK) Berdasarkan Undang-Undang Informasi dan Elektronik

Naufal Mahira Dewantoro*, Dian Alan Setiawan

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia.
*naufalmahird@gmail.com, dianalan.setia@yahoo.com

Abstract. *The rapid development of information and communication technology is related to the needs for everyday human life. With these developments, information technology itself has changed the behavior of global society and has made the world borderless and caused significant social changes to occur quickly. Phishing is a form of cybercrime that involves defrauding individuals into providing personal information, such as login credentials or credit card numbers, under the guise of a trustworthy entity. This study aims to determine law enforcement against cybercrime crimes using the phishing method in relation to the Electronic Information and Transaction Law. This study uses law enforcement theory which explains that law enforcement is an activity of harmonizing value relationships in the rules to create peace, if phishing cases can be enforced properly then security will be created in society. The method used in this study is an analytical descriptive method, namely by finding facts from news articles and determining the research object to obtain data on cybercrime crime problems using the phishing method and then connecting them with Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions and compiled and analyzed using law enforcement theory which produces an overview of this research. The results of the research include the factors that cause phishing-based cybercriminals to commit their crimes due to financial motivation, the desire to gain profits, the vulnerability of technological systems, and weaknesses in security infrastructure.*

Keywords: *Law Enforcement, Cybercrime, Phising*

Abstrak. Pesatnya perkembangan teknologi informasi dan komunikasi berkaitan dengan kebutuhan untuk kehidupan manusia sehari-hari. Dengan perkembangan tersebut, teknologi informasi itu sendiri telah mengubah perilaku masyarakat global dan telah membuat dunia menjadi tanpa batas dan menyebabkan perubahan sosial. *Phishing* yang merupakan salah satu bentuk kejahatan siber yang melibatkan penipuan terhadap individu untuk memberikan informasi pribadi, seperti kredensial login atau nomor kartu kredit, dengan menyamar sebagai entitas yang dapat dipercaya. Penelitian ini bertujuan untuk mengetahui penegakan hukum terhadap tindak pidana *cybercrime* dengan metode *phising* dihubungkan dengan Undang-Undang .Informasi dan Transaksi Elektronik. Penelitian ini menggunakan teori penegakan hukum yang menjelaskan bahwa penegakan hukum merupakan suatu kegiatan menyerasikan antara hubungan nilai dalam kaidah untuk menciptakan kedamaian, apabila kasus *phising* dapat ditegakkan dengan baik maka akan terciptanya keamanan di masyarakat. Metode yang digunakan dalam penelitian ini adalah metode deskriptif analitis yaitu dengan mencari fakta-fakta dari artikel berita dan menentukan objek penelitian untuk mendapatkan data permasalahan tindak pidana *cybercrime* dengan metode *phising* kemudian dihubungkan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta disusun dan dianalisis dengan teori penegakan hukum yang menghasilkan menghasilkan gambaran penelitian ini. Hasil penelitian diantaranya faktor penyebab pelaku kejahatan siber berbasis phising melakukan kejahatannya adalah karena faktor motivasi finansial, keinginan untuk mendapatkan keuntungan, kerentanan sistem teknologi, dan kelemahan dalam infrastruktur keamanan. Upaya penegakan hukum kejahatan siber berbasis phising perlu di maksimalkan lagi dalam mencegah kejahatan siber berbasis *phising*.

Kata Kunci: *Penegakan Hukum, Kejahatan Siber, Phising.*

Corresponding Author
Email: dianalan.setia@yahoo.com

A. Pendahuluan

Perkembangan Zaman saat ini sangat pesat, Indonesia sebagai Negara berkembang turut terkena dampak dari perubahan zaman ini. Teknologi salah satunya sebagai bentuk perkembangan zaman yang saat ini telah menjadi bagian dari semua makhluk hidup di muka bumi. Maka seiring berjalannya waktu peraturan pun ikut berubah karena teknologi juga yang semakin modern memungkinkan seseorang untuk menyalahgunakan sistem dari teknologi itu sendiri.

Pesatnya perkembangan teknologi informasi dan komunikasi berkaitan juga dengan kebutuhan untuk kehidupan manusia sehari-hari. Internet merupakan salah satu teknologi yang lahir dari perkembangan teknologi. Kehidupan manusia pula tidak pernah luput dari internet. Secara keseluruhan Internet adalah jaringan besar yang saling berhubungan dari jaringan-jaringan komputer yang menghubungkan orang-orang dan komputer-komputer diseluruh dunia, melalui telepon, satelit dan sistem-sistem komunikasi yang lain.

Sebagai hasil dari perkembangan tersebut, teknologi informasi itu sendiri juga telah mengubah perilaku masyarakat global dan peradaban manusia. Selain itu, perkembangan teknologi informasi telah membuat dunia menjadi tanpa batas dan menyebabkan perubahan sosial yang signifikan yang terjadi dengan cepat. Penggunaan media internet pada zaman ini juga cukup menjadi sebuah sarana yang memudahkan manusia dalam mendapatkan informasi maupun hal lainnya. Semua hal menjadi lebih praktis dalam dunia internet, akan tetapi diiringi dengan kepraktisan yang dibawanya, internet juga membawa dampak negatif berupa keamanan yang belum bisa terjamin. Keamanan dalam dunia siber masih sangat rentan dikarenakan adanya unsur mudahnya dalam mengakses teknologi itu sendiri yang menyebabkan banyak peretas yang dapat dengan mudah menjangkau sebuah system keamanan yang dibuat sedimikian rupa, dalam dunia internet akan selalu ada celah apabila berbicara mengenai system keamanan, maka dari itu lahirlah *cybercrime.*

Di Indonesia, kejahatan siber diatur dalam Undang-Undang Nomor 19 Tahun 2016 yang merupakan revisi dari Undang-undang no 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Berbagai cara dapat dilakukan untuk pembuktian di pengadilan dan penyidikan oleh pihak kepolisian dalam kejahatan siber, antara lain dengan mengoptimalkan undang-undang tersebut, mengembangkan pengetahuan dan kemampuan penyidik di dunia siber, serta menambah dan meningkatkan fasilitas forensik komputer di Kepolisian Republik Indonesia.

Kejahatan siber merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan komputer. Dapat disimpulkan bahwa kejahatan siber adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran kejahatan. Kejahatan tersebut adalah bentuk-bentuk kejahatan yang bertentangan dengan peraturan perundang-undangan.Indonesia sebagai negara hukum, selalu mengutamakan semua kegiatan kenegaraan dan kemasyarakatan didasarkan pada ketentuan hukum.

Phishing yang merupakan salah satu bentuk kejahatan siber yang melibatkan penipuan terhadap individu untuk memberikan informasi pribadi, seperti kredensial login atau nomor kartu kredit, dengan menyamar sebagai entitas yang dapat dipercaya. Meningkatnya teknologi digital telah membuat serangan phishing menjadi lebih canggih dan lebih sulit dideteksi, yang mengarah pada meningkatnya kebutuhan akan strategi penegakan hukum yang efektif untuk memerangi jenis kejahatan siber ini. Untuk menegakkan hukum secara efektif terhadap phishing, lembaga penegak hukum perlu memiliki unit kejahatan siber khusus yang dilengkapi dengan teknologi terbaru dan terlatih dalam teknik terbaru. Hal ini termasuk kemampuan untuk melakukan investigasi forensik digital, melacak jejak digital, dan bekerja sama dengan penyedia layanan internet untuk menemukan dan menangkap penjahat.

Salah satu tantangan dalam menegakkan hukum terhadap phishing adalah sering kali sulit untuk mengidentifikasi pelaku. Serangan phishing bisa berasal dari mana saja di seluruh dunia, sehingga menyulitkan lembaga penegak hukum untuk melacak pelakunya. Selain itu, serangan phishing dapat dilakukan secara anonim, yang semakin memperumit upaya untuk mengidentifikasi dan menuntut para pelaku.

Tantangan lain dalam menegakkan hukum terhadap phishing adalah bahwa hukuman untuk jenis kejahatan siber ini bisa sangat bervariasi tergantung pada yurisdiksinya. Di beberapa negara, phishing diklasifikasikan sebagai pelanggaran ringan dan hanya dikenai denda kecil atau hukuman penjara singkat. Di negara lain, phishing diklasifikasikan sebagai kejahatan serius dan membawa hukuman yang jauh lebih berat, seperti hukuman penjara yang panjang dan denda yang besar.

Selain upaya penegakan hukum, ada juga kebutuhan untuk meningkatkan kesadaran masyarakat terhadap serangan phishing. Banyak orang yang menjadi korban serangan phishing karena mereka tidak menyadari taktik yang digunakan oleh penjahat siber. Dengan mengedukasi masyarakat tentang risiko phishing dan bagaimana mengidentifikasi serta menghindari serangan ini, kita dapat mengurangi jumlah korban dan pada akhirnya mempersulit penjahat siber untuk berhasil.

Salah satu dampak dari produk kejahatan siber berbasing phising yang sedang ramai saat ini yaitu APK. *Application Package Kit* atau yang disingkat APK adalah format berkas yang digunakan untuk mendistribusikan dan memasang *software* dan *middleware* ke ponsel dengan sistem operasi Android. Tercatat hingga 19 Januari 2023, 483 warga Indonesia yang terkena penipuan modus phising berbentuk APK ini. Polisi mengatakan bahwa total kerugian yang dicapai hingga 12 Milliar rupiah. Maka darinya berikut cara kerja kejahatan siber berbasing phising APK:

1. Pelaku akan mengirim pesan berupa APK kepada calon korban dengan modus bahwa mereka merupakan kurir dari perusahaan ekspedisi.
2. Lalu kemudian pelaku meminta korban untuk membuka pesan tersebut yang berupa APK.
3. Sesudah korban membuka APK yang telah dikirim pelaku, maka akan ter *install* sebuah aplikasi asing yang tidak akan terdeteksi oleh korban.
4. Setelah aplikasi asing tersebut ter *install*, disinilah korban memulai kejahatannya tersebut. Pelaku dapat mengais informasi data pribadi korban, hingga apabila korban mempunyai aplikasi *m-banking* atau "dompet digital", maka pelaku dapat mengakses aplikasi tersebut secara illegal hingga memindahkan uang korban ke pelaku.

Kehadiran Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam pemanfaatan Teknologi Informasi, media, dan teknologi komunikasi telah mengubah perilaku masyarakat dan peradaban manusia, khususnya di Indonesia. Perkembangan teknologi informasi dan komunikasi juga menyebabkan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya yang signifikan berlangsung begitu cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peningkatan kesejahteraan, juga menjadi sarana yang efektif untuk melakukan perbuatan melawan hukum. Saat ini telah muncul rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika.

Secara detail isi pasal tersebut yang menerangkan tentang perbuatan yang dianggap melawan hukum menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik berupa penipuan situs. Undang-Undang ini dapat dipandang sebagai langkah awal pemerintah dalam menangani *cybercrime*. Kejahatan phising tidak bisa disamakan dengan penipuan biasa, karena aksi phising memanfaatkan kemajuan sistem teknologi.

Kebutuhan akan perlindungan hukum bagi pengguna internet dalam era digital semakin meningkat, namun masih terdapat kelemahan dalam sistem hukum yang ada saat ini. Undang-Undang Informasi dan Transaksi Elektronik (*Electronic Information and Transactions Law*) belum mampu menjangkau seluruh aspek kejahatan siber dan belum memberikan perlindungan yang memadai bagi korban.

Penanggulangan tindak pidana kejahatan siber berbasis phishing sangatlah penting dilakukan agar masyarakat dapat terlindungi dari dampak negatif dari tindak pidana tersebut. Pemerintah dan pihak yang berwenang harus berusaha mengambil tindakan yang efektif untuk mengatasi masalah ini dan memberikan perlindungan bagi masyarakat. Oleh karena itu, penting untuk melakukan studi dan analisis tentang penanggulangan tindak pidana kejahatan siber

berbasis phishing, agar dapat ditemukan solusi dan upaya yang efektif untuk mengatasi masalah ini.

Menurut Pasal 9 ayat (3) PSE pemerintah diharuskan untuk memastikan, sistem elektroniknya tidak memuat dan tidak memfasilitasi penyebaran informasi atau dokumen elektronik yang dilarang. Walaupun pemerintah terutama Kominfo sudah meregulasi platform-platform yang tidak mematuhi aturan Penyelenggara Sistem Elektronik (PSE), namun pada fakta dilapangan masih banyak terjadi pelanggaran *cybercrime.* Penggunaan teknologi yang semakin canggih membuat pelaku kejahatan siber semakin mudah untuk melakukan kegiatan phising. Maka dari itu pemerintah perlu meregulasi ulang peraturan perundang-undangan agar masyarakat dapat terhindar dari kejahatan siber berbasis phising tersebut. Dengan Identifikasi Masalah:

1. Apa faktor terjadinya tindak pidana kejahatan siber berbasis *phising*?
2. Bagaimana Penegakan Hukum terkait kejahatan siber berbasis *phising* berdasarkan Undang-Undang Informasi dan Transaksi Elektronik?

B. Metodologi Penelitian

Bahwa Penelitian ini menggunakan metode pendekatan yuridis normatif. Penelitian yuridis normatif adalah pendekatan masalah dengan melakukan tinjauan terhadap peraturan perundang-undangannya. Metode yuridis normatif merupakan penelitian untuk mengkaji peraturan perundang-undangan untuk memecahkan masalah. Metode hukum normatif adalah kajian hukum yang dilakukan melalui kajian data atau bahan pustaka, yaitu data sekunder berupa undang-undang, teori, berbagai literatur, internet, konsep, dan ulama yang menjelaskan tentang tindak pidana perjudian.

Spesifikasi yang digunakan adalah deskriptif-analitis. Artinya, memberikan penjelasan yang sistematis dan logis dalam menganalisisnya. Hal ini dilakukan dalam rangka mengkaji bahan dan literatur yang berlaku, peraturan perundang-undangan di Indonesia dalam kaitannya dengan teori-teori hukum yang terkait dengan masalah yang secara sistematis ditangani masalah tersebut. dijelaskan dan dianalisis. Faktual, logis, dan beralasan.

C. Hasil Penelitian dan Pembahasan.

Pada hakekatnya, perkembangan teknologi sangat besar pengaruhnya terhadap sikap masyarakat. Kemajuan teknologi dan industri merupakan hasil dari kebudayaan manusia dan selain berdampak positif, yang dimaksudkan untuk dimanfaatkan bagi kemaslahatan umat manusia, juga berdampak negatif terhadap perkembangan peradaban manusia itu sendiri.

Kejahatan dunia maya atau lebih dikenal dengan kejahatan siber (*cyber crime)* berasal dari kehidupan mereka yang mengeksploitasinya dan cenderung meningkatkan konsentrasinya di dunia maya dari waktu ke waktu. Perkembangan tersebut berdampak pada kehidupan sosial masyarakatnya dan di sisi lain juga berdampak pada munculnya berbagai bentuk kejahatan pada tingkat kemajuan yang dialami.

Salah satu kejahatan siber yang marak hari ini terjadi adalah kejahatan siber berbasis *phishing*. Kejahatan Siber berbasis phishing telah menjadi ancaman yang semakin nyata dan meresahkan dalam dunia digital saat ini. *Phishing* adalah metode yang digunakan oleh penjahat untuk memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi dengan menyamar sebagai entitas tepercaya. Dalam upaya ini, penipu menggunakan pesan elektronik, pesan instan, atau situs web palsu yang tampak asli untuk menipu korban yang tidak curiga. Dalam beberapa detik, korban bisa terjebak dan memberikan data pribadi mereka kepada penjahat tanpa mereka sadari. Ada beberapa faktor yang dapat menyebabkan timbulnya kejahatan siber. Berikut ini adalah beberapa faktor utama:

1. Kemajuan Teknologi: Kemajuan teknologi dan konektivitas internet memberikan pelaku kejahatan ciber lebih banyak kesempatan untuk melakukan serangan. Keberadaan perangkat yang terhubung ke internet dan penggunaan teknologi informasi yang luas memberikan ruang gerak bagi para penyerang untuk mencuri data, merusak sistem, atau menyebabkan gangguan lainnya.
2. Keuntungan Finansial: Kejahatan siber dapat menghasilkan keuntungan finansial yang besar bagi para pelaku. Serangan siber seperti pencurian identitas, pencurian data kartu

kredit, atau ransomware dapat memberikan imbalan finansial yang signifikan bagi para penyerang. Dorongan finansial ini menjadi motivasi kuat bagi mereka untuk terlibat dalam kejahatan siber.

3. Anonimitas: Salah satu faktor menarik dari kejahatan siber adalah kemampuan untuk melakukan serangan secara anonim. Pelaku kejahatan ciber dapat menyembunyikan identitas mereka dengan menggunakan alat-alat seperti jaringan privat virtual (VPN) atau teknik lainnya untuk menyembunyikan jejak digital mereka. Hal ini membuat sulit bagi pihak yang ditargetkan atau lembaga penegak hukum untuk mengidentifikasi dan menangkap pelaku.
4. Kurangnya Keamanan Sistem: Banyak organisasi atau individu yang tidak memiliki langkah-langkah keamanan yang memadai untuk melindungi sistem mereka dari serangan kejahatan siber. Kelemahan dalam sistem keamanan, kerentanan perangkat lunak, atau kurangnya pembaruan terhadap perangkat lunak yang rentan dapat memberikan peluang bagi penyerang untuk masuk dan merusak sistem.
5. Faktor Manusia: Seringkali, kejahatan siber melibatkan faktor manusia. Pelaku dapat memanfaatkan ketidaktahuan atau kelalaian pengguna untuk mendapatkan akses ke informasi sensitif. Serangan phishing, misalnya, melibatkan pengiriman email palsu yang mengelabui pengguna agar mengungkapkan informasi pribadi atau login ke situs palsu.
6. Konflik Politik dan Perang Dunia Maya: Dalam beberapa kasus, negara-negara atau kelompok-kelompok dengan kepentingan politik atau militer tertentu dapat melakukan serangan siber sebagai bentuk perang dunia maya. Serangan semacam itu dapat melibatkan spionase, sabotase, atau usaha untuk mencuri informasi rahasia dari negara atau organisasi lain.

Teori kriminologi mencoba memahami beberapa variabel yang juga dapat mempengaruhi hukum, keputusan eksekutif, dan penegakan hukum dalam sistem peradilan pidana. Efektivitas strategi pencegahan kejahatan memerlukan pertimbangan faktor-faktor yang menyebabkan kejahatan. teori kontrol sosial yang dapat memberikan pemahaman tentang faktor-faktor yang mempengaruhi terjadinya perilaku kriminal dalam dunia maya. Beberapa elemen dalam teori kontrol sosial dapat dihubungkan dengan faktor-faktor yang relevan dengan kejahatan siber, seperti berikut:

1. Ikatan; Ikatan sosial yang kuat dengan orang-orang di sekitar individu dapat memiliki dampak pada perilaku kejahatan siber. Jika individu memiliki ikatan yang kuat dengan keluarga, teman, atau anggota komunitasnya, mereka mungkin cenderung untuk mematuhi nilai-nilai dan norma-norma yang melarang kejahatan siber. Dalam hal ini, dukungan sosial dan pengarahan positif dari lingkungan dapat meminimalkan kemungkinan individu terlibat dalam kegiatan kriminal online.
2. Keterlibatan; Keterlibatan individu dalam kegiatan positif dalam dunia nyata dan dunia maya juga dapat mempengaruhi terjadinya kejahatan siber. Jika individu terlibat dalam aktivitas yang membangun keterampilan dan pengetahuan yang positif, seperti pendidikan, pekerjaan, atau hobi yang konstruktif, maka kemungkinan mereka terlibat dalam kejahatan siber dapat berkurang.
3. Keyakinan; Keyakinan individu terhadap nilai-nilai dan norma-norma yang berlaku juga berperan penting dalam kejahatan siber. Jika individu memiliki keyakinan yang kuat terhadap pentingnya menghormati privasi orang lain, menghindari peretasan, pencurian identitas, atau penyebaran informasi palsu, maka mereka cenderung untuk menghindari perilaku kriminal dalam dunia maya.
4. Keterampilan; Komitmen individu terhadap tujuan jangka panjang dan investasi yang mereka miliki dalam mencapai tujuan tersebut dapat berpengaruh terhadap perilaku kejahatan siber. Jika individu memiliki keterampilan dan komitmen terhadap pengembangan teknologi yang positif, seperti keamanan siber, etika *hacking* atau meretas, lalu penelitian keamanan informasi, mereka (pelaku) mungkin lebih condong untuk menggunakan keterampilan mereka dengan cara yang legal dan etis.

Phishing sendiri dapat diartikan sebagai suatu tindakan kejahatan menggunakan teknik rekayasa sosial dalam menjalankan aksinya. Pelaku kejahatan ini memiliki sebutan tersendiri yaitu *phisher*, yang dalam kejahatan phishing pelaku berupaya untuk menipu korban dengan sasaran utama mendapatkan informasi pribadi atau data pribadi dari korban tersebut seperti username, password dan rincian kartu kredit. Hal tesebut dapat menjadi salah satu tolak ukur dalam penegakan hukum siber di Indonesia. Pada saat ini Indonesia dalam menangani hukum siber mengacu pada ketentuan Undang-undang no 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) mengatur beberapa ketentuan yang berkaitan dengan kegiatan phishing atau penipuan online, Pasal 26 UU ITE yang menyebutkan bahwasannya;

"Melarang setiap orang untuk mengakses sistem elektronik milik orang lain tanpa hak atau melawan hukum. Dalam konteks kejahatan phishing, pelaku yang melakukan akses tanpa izin atau dengan cara memalsukan identitas untuk memperoleh data pribadi korban, telah melakukan pelanggaran terhadap ketentuan ini.". Kemudian dalam pasal 30 UU ITE yang berbunyi;

"Melarang setiap orang untuk membuat atau menyebarkan informasi palsu dan menyesatkan yang dapat menimbulkan kerugian atau kehilangan bagi orang lain. Dalam konteks kejahatan phishing, pelaku yang membuat atau menyebarkan informasi palsu dan menyesatkan dengan tujuan untuk memperoleh data pribadi korban, telah melanggar ketentuan ini.".

Selanjutnya mengenai larangan dalam melakukan pencurian identitas terdapat dalam Pasal 31 UU ITE termaktub bahwasannya *"Melarang setiap orang untuk melakukan tindakan pencurian identitas atau merusak identitas orang lain dengan cara menggunakan identitas palsu atau memalsukan identitas orang lain. Dalam konteks kejahatan phishing, pelaku yang menggunakan identitas palsu atau memalsukan identitas orang lain untuk memperoleh data pribadi korban, telah melanggar ketentuan ini".* Dan dilanjutkan dengan Pasal 45A UU ITE yang menegaskan bahwa: *"Setiap orang yang dengan sengaja dan tanpa hak memasukkan, mengirimkan, mengeluarkan, menyiarkan, atau membuat tersedia Informasi atau Dokumen Elektronik yang memiliki muatan penghinaan dan atau pencemaran nama baik akan dipidana dengan sanksi pidana. Dalam konteks kejahatan phishing, pelaku yang membuat situs web palsu atau pesan palsu yang menipu korban dengan iming-iming hadiah atau promosi palsu, dapat dipandang sebagai tindakan yang merusak reputasi seseorang."*

Konteks phising dalam UU ITE masuk kedalam 3 kategori utama, yaitu manipulasi, penerobosan, dan memindahkan atau mentransfer data seseorang. Pada kategori manipulasi, pelaku yang mengirimkan surat elekronik (e-mail) yang seolah-olah asli dapat dijerat Pasal 35 jo. Pasal 51 UU ITE, sebagai berikut: *"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 dipidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12 miliar."*

Selanjutnya kegiatan *phising* dapat dikategorikan sebagai suatu usaha penerobosan atau penjebolan suatu sistem Jika pelaku menerobos atau menjebol suatu sistem elektronik tertentu, menggunakan identitas dan password korban dengan tanpa hak, ia dapat dijerat Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE, sebagai berikut: *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800 juta."* Pada upaya *phising* selanjutnya adalah memindahkan atau mentransfer Atas perbuatan memindahkan atau mentransfer informasi dan/atau dokumen elektronik milik korban, misalnya isi rekening, pelaku phishing dapat dijerat dengan Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE yang berbunyi: *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak dipidana penjara paling lama 9 tahun dan/atau denda paling banyak Rp3 miliar."*

Pada kasus yang penulis bahas mengenai kejahatan siber berbasis *phising* dalam bentuk *Application Package Kit* (APK), bahwasannya apa yang dikerjakan oleh pelaku *phising* termasuk kedalam 3 kategori utama dalam UU ITE. Dimana proses daripada kejahatan siber berbasis *phising* dalam bentuk *Application Package Kit* (APK) pelaku membagikan aplikasi berupa file resi yang sudah masuk kedalam penipuan, dan ketika aplikasi itu sudah dipasangkan kepada *handphone* korban aplikasi tersebut yang nantinya akan membobol dan mentransfer data-data dari korban. Sehingga dalam hal terjadinya *phising* diperlukannya suatu pembuktian dalam menentukan suatu tindak pidana pelaku.

Dalam menentukan pelaku itu bersalah atau tidak, diperlukannya suatu alat bukti dalam proses peradilan pidana . Dalam ilmu hukum pidana dikenal asas *In criminalibus, probationes bedent esse luce clariores*, artinya dalam perkara pidana, bukti harus lebih terang dari cahaya/seterang cahaya. Penjelasan bukti yang diberikan atau diperlihatkan di pengadilan harus jelas. Semakin penting, prinsip ini menekankan bahwa bukti harus lebih dari sekedar tidak langsung. Asas ini menunjukkan bahwa pembuktian merupakan hal utama yang harus ada, karena tanpa adanya pembuktian, suatu kejahatan tidak dapat diselesaikan. Untuk pembuktiannya sendiri, setidaknya harus ada dua alat bukti. Jika hanya ada satu, tindakan orang tersebut tidak dapat diadili. Alat bukti menjadi suatu tolak ukur dalam penentuan proses peradilan pidana. Ekstensifikasi alat bukti konvensional sebagaimana yang terdapat dalam Pasal 184 ayat (1) KUHAP mengenalkan alat bukti baru yang terus menerus dan berubah-ubah dari waktu ke waktu, namun dalam pencantumannya sebagai alat bukti, Data Elektronik atau alat bukti elektronik menimbulkan beberapa masalah yaitu :

1. Permasalahan mengenai *locus delicti* (tempat kejadian tindak pidana), dalam tindak pidana siber penyidik menemukan suatu kesulitan untuk menentukan lokasi atau tempat yang akurat dalam terjadinya tindak pidana. Karena seringkali pelaku dapat merubah atau menghapus "jejak digital" perangkat yang dipergunakannya untuk melakukan tidak pidana siber maupun mensetting lokasi yang berbeda dengan lokasi yang sebenarnya.
2. Permasalahan mengenai tempus delicti (waktu kejadian tindak pidana), penyidik tidak dapat menentukan dengan pasti kapan suatu kejahatan terjadi, karena pelaku kejahatan siber seringkali dapat mengulang waktu dan tanggal perbuatannya.
3. Persoalan pembuktian menjadi persoalan tersendiri bagi aparat penegak hukum. Bukti-bukti yang dicari terkait dengan segala sesuatu yang digunakan untuk mendukung, melakukan dan hasil kejahatan dunia maya sangat sulit untuk diketahui karena dibalik kecanggihan sistem jaringan internet juga terdapat celah bagi orang-orang yang memiliki keahlian untuk menghapus atau menghancurkannya. identitas dan. langit. Di sisi lain, teknologi informasi adalah teknologi dengan sistem terbuka yang tidak mungkin didorong atau ditutup secara ilegal, di mana siapa pun yang memiliki keterampilan di bidang ini dapat mengontrol data, mengubah data, ada untuk mengubah data palsu menjadi data palsu asli.

Dalam hal ini, hukum berfungsi sebagai *rechtzeken heid* atau pemberi kepastian hukum, di mana apabila terjadi persoalan dan permasalahan ada kepastian hukum untuk dijadikan pedoman oleh seluruh masyarakat, menjadikan faktor hukum dalam pelaksanaan transaksi elektronik khususnya dalam sektor perbankan dapat menjadi pegangan oleh pihak terkait baik penegak hukum seperti pegawai bank itu sendiri maupun masyarakat. Sebagaimana arti dari kepastian hukum itu sendiri yaitu suatu interpretasi dari hukum tertulis yang dapat dijadikan pedoman kepada masyarakat, sebagai upaya penanggulangan terhadap suatu perbuatan yang dianggap melawan hukum. Berdasarkan urarian diatas, hal-hal yang dapat penulis analisis dalam penegakan hukum terkait kejahatan siber berbasis phising berdasarkan undang-undang hukum informasi dan transaksi elektronik adalah sebagai berikut:

1. Aparat Penegak
   Dalam hal penegakan hukum, turut andil daripada para aparat penegak hukum sangat diperlukan. Hal-hal yang memang menjadi prasyarat dalam menentukan tindak pidana dalam kejahatan siber untuk menentukan suatu proses pidana, Dalam kehidupan bermasyarakat banyak disertai dengan adanya kejahatan, sehingga pemidanaan dituntut

untuk memperhatikan upaya mempertahankan dan melestarikan tujuan hidup masyarakat. Menghukum pelaku kejahatan tentu saja merupakan hal yang harus dilakukan, selain untuk membuat jera pelaku kejahatan, juga merupakan bagian dari upaya negara untuk menjaga keadilan dalam negeri. Maka dari itu dalam proses penegakan hukum, kualitas dan kapabilitas daripada setiap aparat penegak hukum sangat diperlukan. Memperkuat fungsi aparat penegak hukum yang mumpuni baik secara individu maupun secara organisasi dan terstruktur untuk menyatukan komunitas-komunitas spesialisasi dalam penanganan segala jenis *cyber crime* dapat memberikan rasa kepercayaan dimasyarakat tentunya dalam proses penegakan hukum di Indonesia

2. Peningkatan Sarana Dan Prasarana
   Setiap aparat penegak hukum, dalam upaya menegakan siber berbasis *phising* dalam bentuk *Application Package Kit* (APK) turut andil dalam menegakan hukum di Indonesia. Aparat penegak hukum tidak dapat melakukan tugasnya dengan baik jika tidak dilengkapi dengan sarana dan prasarana yang sepadan, yang dalam hal ini merupakan seperangkat norma dan asas hukum yang baik. Karenanya penentuan sarana dan prasarana dalam menunjang tindakan preventif dalam hukum siber di Indonesia sangat diperlukan. Penegakan hukum kemungkinan besar tidak dapat menjalankan fungsi yang dimaksudkan tanpa sarana atau fasilitas tertentu untuk membantu aparat penegak hukum. Maka dari itu sudah sepatutnya dalam proses pennegakan hukum diperlukan suatu alat-alat yang sepadan dalam mendeteksi daripada phising dalam bentuk *Application Package Kit* (APK) sehingga penegakan daripada hukum siber di Indonesia dapat dijalankan secara maksimal.
3. Undang-Undang Khusus Mengenai Hukum Siber Di Indonesia
   Pada awalnya, Undang-undang no 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) sebagai penunjang daripada kejahatan siber. *Framing* yang terjadi di masyarakat hari ini bahwa UU ITE hanya sebagai alat pembungkaman berkegiatan di sosial media. Karena apabila kita kaitkan pada kejahatan siber berbentuk *phising* dalam bentuk *Application Package Kit* (APK), mengenai penyelesaian perkara bagi pelaku *phising* dengan pemberian pidana berupa pidana penjara dan/atau pidana denda. Para korban phising yang pada dasarnya memiliki kebutuhan dalam pemenuhan kerugian material yang dialaminya, terdapat didalam UU Perlindungan Saksi dan Korban atau disebut dengan UUPSK menyebutkan terdapat adanya perlindungan korban dan/atau saksi tindak pidana yaitu dalam bentuk kompensasi, restitusi dan bantuan. Maka dari itu efektifitas daripada UU ITE hingga hari ini masih dipertanyakan untuk penegakan hukum korban *phising* karena belum diatur secara eksplisit mengenai hak-hak korban.

D. Kesimpulan

Faktor penyebab pelaku kejahatan siber berbasis phising melakukan kejahatannya adalah karena faktor motivasi finansial, keinginan untuk mendapatkan keuntungan, kerentanan sistem teknologi, dan kelemahan dalam infrastruktur keamanan. Serta kurangnya edukasi masyarakat terhadap teknologi menjadi acuan bagi pelaku untuk melakukan kejahatan siber berasis phising.

Upaya penegakan hukum kejahatan siber berbasis phising perlu di maksimalkan lagi dalam mencegah kejahatan siber berbasis phising. Karena UU ITE dinilai tidak efektif dalam menanggulangi kejahatan siber berbasis phising sehinnga perlunya regulasi ulang. Pentingnya regulasi ulang karena untuk mengatur penyalahgunaan teknologi. Serta harus diadakannya Undang-Undang khusus mengenai kejahatan siber berbasis phising. UU khusus mengenai kejahatan siber berbasis phising akan mempengaruhi kualitas daripada penegakan hukum siber, agar menjadi optimal hingga akhirnya menjadi Undang-Undang yang efektif dalam menanggulangi kejahatan siber berbasis phising.

Pemerintah Indonesia perlu memperhatikan masalah dari kejahatan siber berbasis phising, karena di zaman sekarang isu mengenai hal tersebut masih sering terjadi dan masih banyak pelaku yang berkeliaran di luar sana yang tidak tersentuh oleh aparat penegak hukum. Pemerintah juga hendak memperhatikan dampak dari kejahatan siber berbasis phising tersebut

karena terkadang jumlah kerugian yang didapat diderita oleh korban sangat besar.

Aparat penegakan hukum perlu meningkatkan keamanan siber karena untuk melindungi serangan siber dan kejahatan siber. Serta melakukan sosialisasi untuk mengedukasi masyarakat awam mengenai pentingnya kejahatan siber berbasis phising agar dapat melindungi dirinya dari segala bentuk kejahatan siber berbasis phising.

Pemerintah Indonesia dan Aparat Penegak Hukum perlu melakukan tindakan yang lebih tegas lagi dalam mencegah kejahatan siber berbasis phising. Pemerintah Indonesia perlu meregulasi khusus mengenai peraturan tindak pidana kejahatan siber berbasis phising. Kemudian perlunya patroli khusus dalam dunia maya oleh Aparat Penegak Hukum karena untuk mencegah kejahatan siber berbasis phising.

Daftar Pustaka

[1] Maulana, M. R., & Arif Firmansyah. (2023). Penegakan Hukum Terhadap Pelaku Usaha yang Menambang di Kawasan Hutan Tanpa Izin. *Jurnal Riset Ilmu Hukum*, 11–16. https://doi.org/10.29313/jrih.v3i1.1839

[2] Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*, 81–88. https://doi.org/10.29313/jrih.v2i2.1324

[3] Mansur, Dikdik M. Arief. Cyber Law: Aspek Hukum Teknologi Informasi, Tiga Serangkai, 2005. Hlm 5.

[4] Vikran Fasyadhiyaksa Putra Y, Modus Operandi Tindak Pidana Phishing menurut UU ITE, Vol. 4 No. 6 Jurist-Diction, 2021

[5] Ibrahim Fikma Erdisy, Pengantar Hukum Siber, 2019, Hlm 3.

[6] Ardi Saputra Gulo, Cyber Crime dalam bentuk Phishing Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, Journal of Criminal Law Vol. 1, No. 2, 2020, Hlm 4.

[7] Indarta, Yose, Fadhli Ranuharja, Keamanan Siber: Tantangan di Era Revolusi Industri 4.0. Yayasan Kita Menulis, 2022, Hlm 23.

[8] Ronald E. Rorie, Penegakan Hukum Terhadap Pelaku dan Korban Tindak Pidana Cybercrime Berbentuk Phishing di Indonesia, Vol. 11 No. 3, Lex Crimen, 2022, Hlm 4.

[9] Hafsah, Aplikasi Pencarian Android Package (APK) berbasis Web dan Mobile dengan API, Vol 9, No 1, Program Studi Teknik Informatika UPN "Veteran" Yogyakarta, 2012

[10] Nurfitria, Indah. "Analisis Kriminologis Terhadap Tindak Pidana Korupsi Penyalahgunaan Wewenang Dalam Jabatan Pemerintahan Di Bandar Lampung", Jurnal Poenale,3 (3), 2015 1-12 Hlm 6

[11] Dian Alan Setiawan, "Cyberterrorism And It's Prevention In Indonesia", Jurnal Media Hukum,Vol. 27, No. 2, 2020, Hlm. 268.