



Kajian Yuridis Modus Kejahatan Phishing Melalui *Whatsapp*

A Legal Analysis of Phishing Crimes Committed via WhatsApp

Desy Wulandari^{1*}, Ismiyanto², Hafid Zakariya³

¹²³ Program Pascasarjana, Magister Hukum, Universitas Islam Batik Surakarta

*Email Correspondence: desywulandari897@gmail.com

Abstract

Crime in the current era of technological advancement and globalization has emerged with a variety of modes. Supported by the rapid development of digitalization, by relying on the internet network all communication and transaction processes both between people and each other and between companies and each other can be done quickly and easily. But behind this sophistication, there are bad people who try to find loopholes to commit crimes using the internet network or what is known as cybercrime. One of the cyber crimes that threaten the security of personal data is phishing, the crime is an attempt to obtain a person's personal information data by deceiving where the perpetrator acts disguised as someone or a trusted party by asking the victim to fill in confidential personal information or the perpetrator simply sends a link to the victim so that the victim is encouraged to click on the link so that the perpetrator succeeds in gaining access to launch the action. Phishing crimes are rampant via whatsapp, considering that Indonesia is the country with the largest number of whatsapp users in the world quoted from the opinion of Whatsapp Asia Pacific Policy Director, Clair Deevy. The purpose of this study is to explain the juridical study of the mode of phishing crime via whatsapp. The research method used is normative juridical with an emphasis on the statutory approach in examining a legal problem that is rampant.

Keywords: *cybercrime; personal data; phishing; technology*

Abstrak

Kejahatan di era kemajuan teknologi dan globalisasi saat ini banyak sekali muncul dengan beragam modus. Didukung dengan perkembangan digitalisasi yang semakin pesat, dengan mengandalkan jaringan internet semua proses komunikasi dan transaksi baik antara orang satu dengan yang lain maupun antara perusahaan satu dengan yang lain dapat dilakukan secara cepat dan mudah. Namun dibalik kecanggihan tersebut, ada oknum nakal yang berusaha mencari celah untuk melakukan tindak kejahatan menggunakan jaringan internet atau yang dikenal dengan *cybercrime*. Salah satu kejahatan *cyber* yang mengancam keamanan data pribadi adalah *phishing*, aksi kejahatan tersebut merupakan upaya untuk memperoleh data informasi pribadi seseorang dengan cara mengelabui dimana pelaku bertindak menyamar sebagai seseorang atau pihak yang terpercaya dengan meminta korban untuk mengisi informasi pribadi yang bersifat rahasia atau pelaku cukup mengirimkan link kepada korban sehingga korban terdorong untuk mengklik link tersebut sehingga pelaku berhasil mendapatkan akses guna melancarkan aksinya. Kejahatan *phishing* marak terjadi melalui whatsapp, mengingat Indonesia merupakan negara dengan jumlah pengguna whatsapp terbesar di dunia dikutip dari pendapat Direktur Kebijakan Whatsapp Asia Pasific, Clair Deevy. Tujuan penelitian ini adalah menjelaskan tentang kajian yuridis modus kejahatan *phishing* melalui whatsapp. Metode penelitian yang digunakan adalah yuridis normatif dengan penekanan pada pendekatan peraturan perundang-undangan dalam mengkaji suatu permasalahan hukum yang sedang marak terjadi.

Kata kunci : *cybercrime; data pribadi; phishing; teknologi.*

PENDAHULUAN

Perubahan di bidang digitalisasi komunikasi membawa dampak yang besar di seluruh aspek kehidupan masyarakat baik dampak baik positif maupun negatif. Dampak positif yang dirasakan adalah mampu meningkatkan efektifitas dan efisiensi komunikasi, meningkatkan produktivitas kerja karena dapat terselesaikan tanpa memerlukan waktu yang banyak, membangun hubungan

sosio-ekonomi serta membantu di berbagai bidang. Hampir seluruh masyarakat melakukan aktivitas sehari-hari menggunakan teknologi berbasis online untuk membuat setiap informasi dapat diakses dengan cepat. Selain dampak positif, kemajuan teknologi juga memberikan dampak negatif yaitu maraknya kejahatan *cyber* (*cyber crime*) seperti maraknya penyebaran dan penyalahgunaan data pribadi untuk melancarkan aksi kejahatan sehingga menyebabkan kerugian bagi korbannya. Eratnya hubungan antara masyarakat dengan fasilitas jaringan internet sehingga demi melancarkan akses, pengguna internet diminta untuk memasukkan data pribadi sebagai bentuk keamanan. Data pribadi merupakan data privasi seseorang yang harus dijaga kerahasiaannya. Memasuki revolusi industri 4.0 mengakibatkan pesatnya perkembangan teknologi yang mengubah gaya hidup masyarakat menjadi sangat ketergantungan dengan kecanggihan teknologi dalam menjalankan aktivitas kehidupan sehari-hari.

Seiring kemajuan teknologi dan globalisasi seperti saat ini menyebabkan munculnya banyak sekali kejahatan dengan berbagai modus. Didukung dengan perkembangan digitalisasi yang semakin pesat, dengan mengandalkan jaringan internet semua proses komunikasi dan transaksi baik antara orang satu dengan yang lain maupun antara perusahaan satu dengan yang lain dapat dilakukan secara cepat dan mudah. Namun dibalik kecanggihan tersebut, ada oknum nakal yang berusaha mencari celah untuk melakukan tindak kejahatan menggunakan jaringan internet atau yang dikenal dengan *cybercrime*. Kejahatan menggunakan jaringan internet ini merupakan kejahatan *cyber* yang incarannya data-data pribadi yang digunakan untuk memudahkan aksi pencurian, penyebaran data bahkan merusak sistem keamanan. Salah satu kejahatan *cyber* yang mengancam keamanan data pribadi adalah *phishing*, aksi kejahatan tersebut merupakan upaya untuk memperoleh data informasi pribadi seseorang dengan cara mengelabui atau menipu dimana pelaku bertindak menyamar sebagai seseorang atau pihak yang terpercaya dengan meminta korban untuk mengisi informasi pribadi yang bersifat rahasia atau pelaku cukup mengirimkan link kepada korban sehingga korban terdorong untuk mengklik link tersebut sehingga pelaku berhasil mendapatkan akses guna melancarkan aksinya. Kejahatan *phishing* sering dilakukan melalui whatsapp, mengingat Indonesia merupakan negara dengan jumlah pengguna whatsapp terbesar di dunia dikutip dari pendapat Direktur Kebijakan Whatsapp Asia Pasific, Clair Deevy (Kementerian Komunikasi dan Informatika). Maraknya penggunaan sosial media di dunia, membuat para *hacker* beraksi memunculkan ide-ide baru untuk merusak kegiatan di internet dengan mengincar data-data pribadi untuk memperoleh keuntungan.

Perkembangan kejahatan *cyber* yang semakin beragam, maka hukum menjawab kebutuhan masyarakat (teori hukum responsif) dengan menghadirkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Instrumen hukum tersebut hadir digunakan sebagai doktrin hukum yang bertujuan untuk memberikan solusi penyelesaian permasalahan hukum.

Penelitian ini dibuat dengan tujuan untuk menjelaskan tentang kajian yuridis modus kejahatan *phishing* melalui whatsapp. Selain itu, penelitian ini bertujuan untuk mengubah pemikiran orang-orang agar lebih peduli dan tidak acuh terhadap ancaman kejahatan *phishing* yang mengintai setiap waktu sehingga dapat dilakukan upaya preventif karena di penelitian ini dibahas juga mengenai ciri-ciri berbagai modus kejahatan *phishing* melalui whatsapp dengan harapan mampu menekan jumlah angka korban yang terjebak *phishing*.

Berdasarkan latar belakang masalah tersebut, maka peneliti mengangkat rumusan masalah yang akan dibahas yaitu bagaimana kajian yuridis modus kejahatan *phishing* melalui whatsapp? Rumusan masalah tersebut muncul sebagai bentuk dukungan dilakukannya tindak represif oleh penegak hukum terhadap maraknya kasus kejahatan *phishing*.

METODE

Penelitian hukum ini menggunakan jenis penelitian yuridis normatif atau *legal research* yaitu penelitian hukum berdasarkan peraturan perundang-undangan yang berlaku atau dapat juga disebut sebagai penelitian hukum doktrinal. Penelitian secara normatif adalah penelitian hukum kepustakaan yang dapat dilakukan dengan cara meneliti bahan pustaka yang merupakan data sekunder. Penelitian hukum yuridis normatif merupakan penelitian tentang norma-norma dari hukum positif dengan tujuan praktis yaitu sinkronisasi norma hukum dengan permasalahan hukum yang terjadi (Asmak UI. Hosnah, et. al. 2021).

Alasan peneliti menggunakan metode penelitian hukum yuridis normatif karena sifat masalah yang dianalisis dalam penelitian ini yaitu kajian yuridis modus kejahatan *phishing* melalui whatsapp, dimana peneliti mengkaji menggunakan peraturan perundang-undangan yang berlaku terhadap modus kejahatan *phishing* melalui whatsapp sehingga ditemukan penyelesaian permasalahan hukum dengan berpedoman pada hukum positif. Kajian yuridis yang dilakukan dengan cara mengidentifikasi ciri-ciri dari setiap modus kejahatan *phishing* melalui whatsapp sehingga pembaca dapat memahami ciri-ciri sekaligus kajian dari sudut pandang hukum.

Analisis penelitian yang digunakan adalah analisis kualitatif yaitu peneliti mendeskripsikan gambaran temuan kasus dengan kata-kata dengan mengutamakan kualitas dari data yang diperoleh. Analisis data dilakukan dengan cara mengkaji atau menelaah terhadap hasil pengolahan data yang dibantu dengan teori-teori sebelumnya (Mukti Fadjar dan Yulianto Achmad, 2010). Metode kualitatif digunakan dalam penelitian ini karena peneliti menginterpretasikan atau melakukan penafsiran terhadap bahan-bahan hukum terhadap permasalahan hukum yang diteliti.

Jenis data penelitian yang digunakan adalah data sekunder yaitu penelaahan kepustakaan atau penelaahan terhadap berbagai literatur (bahan kepustakaan) (Sugiyono, 2018). Sumber data penelitian ini adalah Undang-Undang berkaitan dengan Informasi dan Transaksi Elektronik dan Perlindungan Data Pribadi, buku, jurnal, artikel yang berkaitan pencurian data pribadi. Bahan hukum yang digunakan adalah bahan hukum primer yang bersumber dari peraturan perundang-undangan tentang informasi dan transaksi elektronik serta perlindungan data pribadi. Bahan hukum primer antara lain Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Bahan hukum sekunder yaitu buku-buku literatur yang berisi mengenai prinsip-prinsip dasar ilmu hukum dan pandangan-pandangan para ahli hukum, jurnal, hasil penelitian, artikel dan lainnya yang berhubungan dengan penelitian ini (Peter Mahmud Marzuki. 2016).

HASIL DAN PEMBAHASAN

Mengenal Modus Kejahatan *Phishing* melalui Whatsapp

Pesatnya kemajuan ilmu teknologi informasi dan komunikasi memberikan banyak manfaat bagi kehidupan manusia dalam menjalankan aktivitas sehari-hari, namun di balik perkembangan yang pesat tersebut juga diiringi dengan banyaknya penyalahgunaan teknologi informasi dan komunikasi yang menimbulkan permasalahan di lingkungan dunia maya sehingga meresahkan masyarakat. Kejahatan mayantara dilakukan oleh oknum-oknum nakal atau biasa dikenal dengan *hacker* yang aksinya menggunakan berbagai modus. Penjahat dunia maya melakukan aksinya dengan cara meretas, menipu, mencuri bahkan merusak. Jumlah kasus kejahatan mayantara yang terjadi di Indonesia selama periode tahun 2021 mencapai 612 kasus kemudian mengalami peningkatan berkali-kali lipat pada periode tahun 2022 mencapai 8.831 kasus, dikutip dari Pusat Informasi Kriminal Polri (Kepolisian Republik Indonesia).

Kejahatan mayantara atau kejahatan *cyber* diartikan menjadi dua macam yaitu kejahatan *cyber* dalam arti sempit dan arti luas. Kejahatan *cyber* dalam arti sempit didefinisikan sebagai kejahatan yang dilakukan terhadap sistem computer, sedangkan kejahatan *cyber* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer (Mohd. Yusuf DM, dkk. 2022). Berdasarkan pengertian tersebut, maka dapat disimpulkan bahwa kejahatan *cyber* (*cybercrime*) adalah tindakan melawan hukum terhadap jaringan atau sistem komputer yang dilakukan menggunakan sarana komputer dan jaringan komputer atau internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi untuk memperoleh keuntungan dengan merugikan orang lain.

Phishing ditemukan pertama kali pada tahun 1996. Cara pertama yang dilakukan oleh phisher adalah menggunakan teknik algoritma yang membuat nomor kartu kredit secara acak. Jumlah kredit acak kartu yang digunakan untuk membuat rekening AOL. Program khusus yang digunakan untuk menyederhanakan proses guna melancarkan aksi kejahatan ini yaitu AOHell. Namun pada tahun 1995 praktek ini diakhiri oleh AOL sebagai langkah membuat keamanan dengan tujuan untuk mencegah keberhasilan penggunaan angka kredit secara acak kartu (Erwin Ginting, dkk. 2023). *Phishing* termasuk dalam salah satu kejahatan *cyber* karena memanfaatkan sarana komputer dan kecanggihan jaringan atau sistem komputer untuk mengelabui korbannya. *Phishing* sebenarnya hampir sama dengan *spoofing* karena prinsipnya menipu atau mengelabui korban untuk melakukan aksi pencurian data informasi pribadi, dimana *spoofing* cara kerjanya langsung melakukan perubahan identitas atau penyamaran untuk mengecoh korban dalam sistem keamanan sedangkan *phishing* cara kerjanya yaitu melakukan pengiriman pesan atau *website* palsu untuk memancing korban agar memberikan data informasi pribadi yang bersifat rahasia. Mengingat data informasi pribadi bersifat rahasia dan sensitif bahkan *European Union Data Protection Directive* melarang untuk melakukan pengolahan data tersebut kecuali jika mendapatkan persetujuan mutlak (tanpa dipengaruhi oleh siapapun) dari si pemilik data (Ananthia Ayu D, dkk. 2019).

Penyebab semakin banyak munculnya ancaman serangan *phishing* yaitu mudahnya ditemukan celah dari kecanggihan teknologi komputer dan telekomunikasi ditambah juga minimnya pengetahuan pengguna terhadap sistem komputer, psikologi dan *privasi social networking services* pengguna. Selain itu, banyak pengguna jaringan komputer yang tidak memahami perbedaan pesan asli dan palsu sehingga mudah terkecoh dan jatuh dalam jebakan si pelaku *phishing*. Platform whatsapp adalah media empuk yang dijadikan perantara untuk

melakukan aksi kejahatan *phishing* mengingat prosesnya mudah dan whatsapp ini merupakan media sosial dengan jumlah pengguna terbesar ketiga di dunia yaitu 112 juta pengguna berdasarkan hasil pengolahan data yang dikelola oleh *Bussiness of Apps* (Erlina F. 2023). Jumlah yang banyak tersebut membuat peluang untuk mendapatkan target korban kejahatan *phishing* semakin besar.

Phishing melalui whatsapp saat ini semakin beragam modusnya, dalam penelitian ini jenis modus kejahatan *phishing* dibagi menjadi 3 (tiga) macam yaitu antara lain :

a. *Phishing* PDF

Kejahatan *phishing* PDF merupakan modus penipuan yang dilakukan dengan cara mengirimkan file PDF. Aksi kejahatan ini berupaya memanfaatkan ketidakwaspadaan dan kurangnya pengetahuan masyarakat terhadap jenis file .apk maupun .pdf. yang membuat korban menjadi ragu sehingga calon korban mudah terpancing untuk membuka file PDF yang sudah dimanipulasi dan sudah ada persetujuan permintaan akses dari file tersebut apabila file di klik sehingga pelaku dapat mengakses seluruh informasi yang tersimpan dalam *smartphone* dan melakukan aksi pencurian data-data informasi pribadi korban. Ciri-ciri modus kejahatan *phishing* PDF ini yaitu :

- 1) Nama ekstensi file “.Pdf”, sedangkan ekstensi file asli biasanya huruf kecil semua (.pdf).
- 2) Logo PDF tidak berwarna merah seperti logo PDF pada umumnya.
- 3) Tidak ada peninjauan file PDF.
- 4) File memiliki ukuran yang terbilang besar untuk sebuah file pesanan.

b. *Phishing* Undangan Pernikahan Digital

Kejahatan *phishing* Undangan Pernikahan Digital merupakan modus penipuan melalui undangan pernikahan digital. Pesan yang disebar itu diberi nama Surat Undangan Pernikahan dengan format file APK atau format file untuk aplikasi Android. Pesan yang disebar tidak mencantumkan nama pengirim atau pengirim tidak memperkenalkan dirinya, namun pengirim hanya meminta penerima agar membuka file APK yang dikirimkannya untuk mengetahui informasi yang diberikan. Ciri-ciri modus kejahatan *phishing* Undangan Pernikahan Digital ini yaitu pesan yang dikirimkan berisi tautan yang mengarahkan korban ke sebuah situs web yang berkedok sebagai situs pernikahan. Kemudian korban diminta untuk mengisi informasi pribadi mereka seperti nama, alamat, nomor telepon dan informasi keuangan.

c. *Phishing* Mobile Banking

Kejahatan *phishing* mobile banking merupakan modus penipuan melalui link *phishing* dengan cara mengirimkan pesan percakapan whatsapp. Sasaran kejahatan ini adalah mencuri data pribadi hingga menguras isi saldo rekening korban. Pelaku umumnya mengaku atau menyamar sebagai *customer service* sebuah perusahaan dan memberikan link *phishing* dengan dalih memberikan bantuan. Upaya ini dilakukan untuk mengecoh psikologis korban dengan membuat percaya bahwa yang mengirimkan pesan tersebut adalah pihak resmi dari perusahaan yang *bonafide*. Ciri-ciri modus kejahatan *phishing* Mobile Banking ini yaitu :

- 1) Link *phishing* terlihat mirip dengan yang asli. Data yang menjadi sasaran aksi kejahatan ini adalah data pribadi (nama, usia dan alamat), data akun (*username* dan *password*) serta data finansial (kartu kredit atau rekening bank).
- 2) Website palsu tidak ada logo gembok terkunci, sedangkan kalau website asli terdapat logo gembok terkunci yang berarti *secure* atau aman.
- 3) Link *phishing* menggunakan alphabet yang tidak standar.

Kajian Yuridis Modus Kejahatan *Phishing* melalui Whatsapp

Dalam analisa hukum, modus kejahatan *phishing* ini termasuk dalam tindak pidana pencurian dan penipuan yang dilihat dari sudut pandang KUHP diatur dalam pasal 362 dan pasal 378. Pasal 362 KUHP menerangkan bahwa barangsiapa yang mengambil barang seluruhnya atau sebagian kepunyaan orang lain dengan maksud untuk memiliki barang itu dengan melawan hukum diancam dengan pidana penjara selama maksimal lima tahun. Selain di pasal 362 KUHP, pencurian juga diatur dalam pasal 476 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang menerangkan bahwa setiap orang yang mengambil suatu barang yang sebagian atau seluruhnya milik orang lain dengan maksud untuk dimiliki secara melawan hukum dipidana penjara paling lama lima tahun atau pidana denda paling banyak kategori V (lima ratus juta rupiah). Kemudian pasal 378 KUHP menerangkan bahwa kondisi yang dilakukan oleh siapapun memakan harta orang lain untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu dengan tipu muslihat (jalan batil atau tidak dibenarkan) diancam dengan pidana penjara paling lama empat tahun. Selain di pasal 378 KUHP, penipuan juga diatur dalam pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang menerangkan bahwa setiap orang dengan maksud menguntungkan diri sendiri secara melawan hukum dengan memakai tipu muslihat atau rangkaian kata bohong menggerakkan orang supaya menyerahkan suatu barang dipidana karena penipuan dengan pidana penjara paling lama empat tahun atau pidana denda paling banyak kategori V (lima ratus juta rupiah).

Kejahatan *phishing* merupakan kejahatan yang dikategorikan sebagai kejahatan informasi dan transaksi elektronik yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu kejahatan *phishing* juga termasuk kejahatan yang mengancam keamanan data pribadi yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Tindak pidana *phishing* merupakan penyalahgunaan telekomunikasi yang melanggar Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Tindak pidana *phishing* dalam aksinya berupaya mengakses data pribadi korban sehingga mengganggu privasi, dimana hak privasi ini termasuk hak asasi manusia yang diatur dalam Pasal 28 G ayat (1) Undang-Undang Dasar Tahun 1945 dan Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Berbagai modus kejahatan *phishing* mulai dari penggunaan perantara PDF, undangan pernikahan digital dan *mobile banking* merupakan tindakan yang sama-sama dilakukan dengan cara menipu korbannya untuk dapat melakukan pencurian data informasi pribadi. Peraturan perundang-undangan yang membahas bidang kejahatan *phishing* memang tidak secara eksplisit menyebutkan ketentuan tindak pidana *phishing*. Namun dalam penelitian ini untuk menganalisis sinkronisasi hukum terhadap isu yang ada maka diuraikan unsur-unsur tindak pidana *phishing* tersebut agar dapat diketahui pengaturan hukumnya. Berikut ini adalah unsur-unsur tindak pidana *phishing* :

- a. Kejahatan yang dilakukan dengan sengaja dan melawan hukum atau tanpa hak menyebarkan berita bohong dan menyesatkan (penipuan) yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
- b. Kejahatan *phishing* dilakukan dengan sengaja dan melawan hukum atau tanpa hak memanipulasi dan menciptakan dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut terlihat seolah-olah data yang otentik atau asli sehingga mampu mengecoh korban untuk memercayainya.

- c. Kejahatan *phishing* mengirimkan pesan palsu untuk mengelabui korbannya agar memberikan akses kepada pelaku sehingga pelaku dapat mengakses sistem elektronik milik orang lain (korban).
- d. Kejahatan *phishing* terdapat unsur penipuan yang dilakukan dengan sengaja membuat data pribadi palsu untuk mengelabui korbannya sehingga mudah percaya bahwa pengirim pesan tersebut seolah-olah dari perusahaan atau pihak yang terpercaya.
- e. Kejahatan *phishing* menargetkan data pribadi korban sehingga berusaha memperoleh data tersebut yang kemudian disalahgunakan untuk melakukan tindakan merugikan korban, seperti menjual data informasi pribadi, mencuri saldo rekening bahkan merusak sistem keamanan korban yang membuat pelaku dapat mengakses sistem elektronik secara bebas.
- f. Kejahatan *phishing* mengganggu perlindungan hak privasi seseorang atas data pribadi sehingga dikatakan sebagai pelanggaran hak asasi manusia.
- g. Kejahatan *phishing* merupakan tindakan memanipulasi akses ke jaringan telekomunikasi atau dapat dikatakan sebagai upaya peretasan akses ke jaringan lain tanpa hak atau melawan hukum.

Setelah mengetahui unsur-unsur tindak pidana *phishing* di atas, maka setiap unsurnya dikaji secara yuridis menggunakan hukum positif sebagai berikut :

- a. Kejahatan yang dilakukan dengan sengaja dan melawan hukum atau tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Tindakan tersebut memenuhi unsur penipuan karena terdapat kebohongan (tipu muslihat) yang dilakukan secara sengaja dengan tujuan keuntungan pribadi yang merugikan orang lain, maka hal ini memenuhi unsur tindak pidana penipuan yang diatur pada pasal 378 KUHP dan pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Selain itu, kejahatan *phishing* termasuk kejahatan *cyber* yang diatur dalam pasal 28 ayat (1) *juncto* pasal 45 A ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dijelaskan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum menyebarkan berita bohong dan menyesatkan sehingga mengakibatkan kerugian orang lain dalam transaksi elektronik dan diancam dengan pidana penjara paling lama enam tahun dan/atau denda maksimal satu miliar rupiah. Unsur “berita bohong” sesuai dengan tindakan pelaku kejahatan *phishing* yaitu mengirimkan pesan berupa berita bohong yang tidak sesuai dengan keadaan sebenarnya dan “menyesatkan” selaras dengan tindakan pelaku kejahatan *phishing* yang berusaha menyebabkan seseorang berpandangan keliru karena menganggap pesan yang dikirim pelaku adalah pesan asli sehingga mengakibatkan kerugian seseorang.
- b. Kejahatan *phishing* dilakukan dengan sengaja dan melawan hukum atau tanpa hak memanipulasi dan menciptakan dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut terlihat seolah-olah data yang otentik atau asli sehingga mampu mengecoh korban untuk memercayainya. Tindakan tersebut memenuhi unsur pasal 35 *juncto* pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa 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 terlihat seolah-olah data otentik yang diancam dengan pidana penjara paling lama dua belas tahun dan/atau denda paling banyak dua belas miliar rupiah.

- c. Kejahatan *phishing* mengirimkan pesan palsu untuk mengelabui korbannya agar memberikan akses kepada pelaku sehingga pelaku dapat mengakses sistem elektronik milik orang lain (korban). Jika dianalisis, tindakan tersebut melakukan akses ke sistem elektronik orang lain dengan cara menipu atau mengecoh korban agar memberikan akses kepada pelaku, dimana hal ini memenuhi unsur dalam ketentuan pasal 30 ayat (2) *juncto* pasal 46 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik diancam dengan pidana penjara paling lama tujuh tahun dan/atau denda paling banya tujuh ratus juta rupiah.
- d. Kejahatan *phishing* terdapat unsur penipuan yang dilakukan dengan sengaja membuat data pribadi palsu untuk mengelabui korbannya sehingga mudah percaya bahwa pengirim pesan tersebut seolah-olah dari perusahaan atau pihak yang terpercaya. Tindakan tersebut memenuhi unsur ketentuan hukum pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menjelaskan bahwa setiap orang dengan sengaja membuat “data pribadi palsu” untuk merugikan orang lain dipinana penjara paling lama enam tahun dan/atau denda paling banyak enam miliar rupiah.
- e. Kejahatan *phishing* menargetkan data pribadi korban sehingga berusaha memperoleh data tersebut yang kemudian disalahgunakan dengan maksud menguntungkan diri sendiri yang merugikan korban, seperti menjual data informasi pribadi, mencuri saldo rekening bahkan merusak sistem keamanan korban yang membuat pelaku dapat mengakses sistem elektronik secara bebas. Tindakan tersebut memenuhi unsur ketentuan hukum pasal 67 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menjelaskan bahwa setiap orang dengan sengaja dan melawan hukum memperoleh data pribadi yang bukan miliknya untuk “menguntungkan diri sendiri atau orang lain” yang dapat mengakibatkan “kerugian pemilik data” dipidana dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak lima miliar rupiah. Selain itu, unsur tersebut juga terdapat indikasi pencurian sebagaimana dijelaskan pada pasal 362 KUHP dan pasal 476 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- f. Kejahatan *phishing* mengganggu perlindungan hak privasi seseorang atas data pribadi sehingga dikatakan sebagai pelanggaran hak asasi manusia. Hak privasi merupakan hak asasi manusia yang harus dilindungi kerahasiaan data eksklusifnya yang sesuai dengan amanat dalam ketentuan pasal 28 G Undang-Undang Dasar 1945 yang menerangkan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Jadi pengambilan atau memperoleh data pribadi dengan cara melawan hukum tanpa seijin pemilik data merupakan pelanggaran hak asasi manusia. Ketentuan pasal 28 G Undang-Undang Dasar 1945 tersebut serupa dengan ketentuan pasal 29 ayat (1) Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Kejahatan *phishing* merupakan tindakan memanipulasi akses ke jaringan telekomunikasi atau dapat dikatakan sebagai upaya peretasan akses ke jaringan lain tanpa hak atau melawan hukum, dimana hal ini melanggar ketentuan pasal 22 *juncto* pasal 50 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang menjelaskan bahwa setiap orang dilarang melakukan perbuatan tanpa hak memanipulasi akses ke jaringan telekomunikasi dan/atau akses ke jasa telekomunikasi

dan/atau akses ke jaringan telekomunikasi khusus yang diancam dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak enam ratus juta rupiah.

KESIMPULAN

Berdasarkan hasil penelitian dari pengkajian yuridis terhadap isu hukum terkait modus kejahatan *phishing* dapat diambil kesimpulan yaitu :

- a. *Phishing* melalui whatsapp terdapat beragam modus yang meliputi *phishing* PDF, *phishing* undangan pernikahan digital dan *phishing* mobile banking.
- b. Unsur-unsur tindak kejahatan *phishing* dilakukan dengan cara :
 - 1) Mengirimkan berita bohong atau menggunakan tipu muslihat (kebohongan) dan menyesatkan yang menimbulkan kerugian bagi orang lain, dimana hal ini diatur dalam pasal 378 KUHP dan pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, pasal 28 ayat (1) *juncto* pasal 45 A ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
 - 2) Menciptakan dan memanipulasi pesan berupa informasi elektronik dan/atau dokumen elektronik dengan tujuan seolah-olah terlihat seperti aslinya, dimana hal ini diatur dalam pasal 35 *juncto* pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
 - 3) Mengirimkan pesan palsu untuk mengelabui korbannya agar memberikan akses kepada pelaku sehingga pelaku dapat mengakses sistem elektronik milik orang lain (korban), dimana hal ini diatur dalam pasal 30 ayat (2) *juncto* pasal 46 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
 - 4) Dilakukan dengan sengaja membuat data pribadi palsu untuk mengelabui korbannya sehingga mudah percaya bahwa pengirim pesan tersebut seolah-olah dari perusahaan atau pihak yang terpercaya, dimana hal ini diatur dalam pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
 - 5) Menargetkan data pribadi korban sehingga berusaha memperoleh atau mencuri data tersebut yang kemudian disalahgunakan dengan maksud menguntungkan diri sendiri yang merugikan korban, dimana hal ini diatur dalam pasal 67 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pasal 362 KUHP dan pasal 476 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
 - 6) Mengganggu perlindungan hak privasi seseorang atas data pribadi sehingga dikatakan sebagai pelanggaran hak asasi manusia, hal demikian diatur dalam pasal 28 G Undang-Undang Dasar 1945 dan pasal 29 ayat (1) Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
 - 7) Tindakan memanipulasi akses ke jaringan telekomunikasi atau dapat dikatakan sebagai upaya peretasan akses ke jaringan lain tanpa hak atau melawan hukum yang diatur dalam pasal 22 *juncto* pasal 50 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

DAFTAR PUSTAKA

Undang-Undang dan Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

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

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana
Kitab Undang-Undang Hukum Pidana (KUHP)

Buku-Buku

Ayu D, Ananthia, dkk. 2019. *Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital*. Jakarta : Pusat Penelitian dan Pengkajian Perkara dan Pengelolaan Kepustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi

Fadjar, Mukti dan Yulianto Achmad. 2010. *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar

Hosnah, Asmak UI, et. al. 2021. *Karakteristik Ilmu Hukum dan Metode Penelitian Hukum Normatif*. Depok : Rajawali Pers

Marzuki, Peter Mahmud. 2016. *Penelitian Hukum Edisi Revisi*. Jakarta : Prenada Media Group

Sugiyono. 2018. *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung : Alfabeta

Jurnal

DM, Mohd. Yusuf, dkk. 2022. *Kejahatan Phishing dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia*. Jurnal Pendidikan dan Konseling, Volume 4 Nomor 5. Riau : Universitas Pahlawan Tuanku Tambusai

Ginting, Erwin, dkk. 2023. *Analisis Ancaman Phishing Terhadap Layanan Online Perbankan*. *UNES Journal of Sciencetech Research*, Volume 8, Nomor 1. Medan : Universitas Potensi Utama

Internet

Erlina F. Santika. *Indonesia Masuk 3 Besar Negara dengan Pengguna Whatsapp Terbanyak di Dunia pada 2022*. Dalam <https://databoks.katadata.co.id/datapublish/2023/05/11/indonesia-masuk-3-besar-negara-dengan-pengguna-whatsapp-terbanyak-di-dunia-pada-2022>, diakses pada tanggal 22 November 2023 pukul 11.12 WIB

Kementerian Komunikasi dan Informatika. *Kominfo, Whatsapp Kenalkan Literasi Privasi dan Keamanan Digital*. Dalam https://www.kominfo.go.id/content/detail/22824/kominfo-whatsapp-kenalkan-literasi-privasi-dan-keamanan-digital/0/sorotan_media, diakses pada tanggal 22 November 2023 pukul 10.46 WIB

Kepolisian Republik Indonesia. *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*. Dalam https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat, diakses pada tanggal 22 November 2023 pukul 10.15 WIB