BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi telah membawa dampak positif yang signifikan bagi masyarakat, seperti kemudahan akses informasi, peningkatan efisiensi dalam berbagai sektor, dan konektivitas global yang lebih baik. Namun, sisi lain dari kemajuan teknologi juga membuka pintu bagi penyalahgunaan dan kejahatan di dunia maya. Hal ini terutama terjadi ketika individu atau kelompok dengan niat buruk memanfaatkan teknologi untuk tujuan yang tidak baik, seperti pencurian identitas, penipuan *online* dan serangan *malware*.

Dampak negatif dari perkembangan teknologi yang menyebabkan maraknya *cybercrime*[1] mencakup meningkatnya kejahatan dunia maya yang terkoordinasi, eksploitasi kelemahan sistem keamanan, dan penipuan terhadap pengguna yang kurang berpengalaman dalam menggunakan teknologi digital. *Cybercrime* adalah salah satu jenis kejahatan yang memanfaatkan kemajuan teknologi. Salah satu kelemahan kemajuan teknologi yang berdampak negatif pada setiap aspek kehidupan kontemporer adalah kejahatan dunia maya. Kejahatan dunia maya pada dasarnya adalah segala tindakan ilegal yang melibatkan penggunaan internet, teknologi mutakhir, dan telekomunikasi untuk melakukan kejahatan, seperti modus penipuan.[2]

[1] Eliasta Ketaren, Cybercrime, Cyber Space, Dan Cyber Law, *Jurnal Times* , Vol. 5 No 2 : 35-42 , 2016, H.35

[2] Bichnigauri, Avtandili, Et Al. "Unveiling Quishing: The Dark Side Of Qr Codes In Cyber Attacks." *Defence And Science* (2023): 96.

Di era digital modern, semakin banyak ditemukan berbagai jenis penipuan (*scam*). Sebagai contoh, praktik *quishing* dan *phishing* menjadi lebih umum, di mana para pelaku menggunakan teknik manipulasi untuk mendapatkan informasi sensitif dari korban, seperti kata sandi atau informasi finansial. *Quishing* adalah bentuk penipuan menggunakan teknik baru berbasis gambar. Sedangkan *phishing* adalah penipuan berbasis teks. *Quishing* dilakukan dengan cara manipulasi kode QR, yang mengubah kotak-kotak yang tampak tidak berbahaya ini menjadi pintu gerbang eksploitasi dunia maya. Penjahat dunia maya dengan cerdik menyematkan URL berbahaya ke dalam kode-kode ini, menyamarkannya dalam tautan. Kepercayaan dan kenyamanan yang melekat pada kode QR menjadi alat yang dieksploitasi oleh penyerang untuk mengatur penipuan mereka. Saat seseorang yang tidak curiga memindai kode QR ini, tanpa disadari mereka membuka pintu ke dunia situs *web* palsu yang berisi *malware* untuk tujuan jahat.

Perangkat lunak yang tidak diinginkan pada sistem komputer dikenal sebagai *malware*, atau perangkat lunak berbahaya. *Malware* biasanya dirancang untuk mencuri data atau informasi dan berpotensi menyebabkan kerusakan pada sistem komputer.[3] *Malware* memiliki kemampuan untuk memasuki perangkat, merusak sistem operasi, memanfaatkan sumber daya tanpa sepengetahuan pemiliknya, bahkan mengumpulkan data pribadi yang mungkin dibagikan kepada pihak lain tanpa izin pengguna. *Malware* sekarang dapat menginfeksi

[3] Hasanatul Munawaroh Dkk, *Bank Digital Syariah: Analisis Cyber Security Menurut Hukum Positif Di Indonesia Dan Hukum Ekonomi Syariah*, (Banjarmasin: PT Borneo Development Project, 2022), H. 56-57

hampir semua jenis sistem operasi, termasuk ponsel Android. Karena fitur akses terbuka pada sistem operasi Android, pelaku kejahatan dapat lebih mudah membuat dan mengembangkan aplikasi yang terinfeksi *malware* yang dapat menyusup ke sistem Android.[4] Berbeda dengan *smartphone* yang menggunakan sistem iOS, ia lebih *safety* karena tidak merilis kode sumbernya kepada pengembang aplikasi.[5]

Hadirnya *smartphone* sebagai alat transaksi atau pembayaran dianggap sebagai peluang bagi para *hacker* untuk mencuri data menggunakan metode *quishing* dan *phishing*. Mereka membuat kode *QR* palsu yang berisi *malware* untuk mendapatkan informasi seperti *username,* PIN bahkan nomor rekening korban agar dapat diakses secara ilegal. Sifat seseorang seperti pelaku *quishing* dan *phishing* yang ingin menguasai hak milik orang lain tersebut masuk dalam perbuatan *moral hazard* yang dapat menimbulkan kerugian.

Moral hazard adalah situasi yang berkaitan dengan sifat, watak, dan sifat manusia yang dapat meningkatkan besarnya kerugian dengan risiko rata-rata.[6] Hal tersebut sama dengan tujuan utama pelaku *quishing* dan *phishing* yakni sengaja mencuri data untuk menguasai harta orang lain. Mereka memanfaatkan teknologi untuk kepentingan pribadi dan rela menghalalkan segala cara agar keinginannya terpenuhi. *Moral hazard* atau bahaya moral disebabkan oleh

---

[4] Aris Rsafael Tambunan, Implementasi Static Analysis Dan Background Process Untuk Mendeteksi Malware Pada Aplikasi Android Dengan Mobile Security Framework, *Ledger: Journal Informatic And Information Technology,* Vol.1, No.2, 2024, H.2

[5] Olga Knezevick, Android vs iPhone security: which is safer? Dalam https://us.norton.com/blog/mobile/android-vs-ios-which-is-more-secure, Diakses Pada 28 Juni 2024.

[6] Indah Piliyanti & Afrilianti Romadhon , "Assessing Factors Influencing Moral Hazard Of Mudharaba And Musyaraka Financing In Islamic Banking; Case Study In Surakarta", *Jurnal Ekonomi Dan Bisnis Islam*, Vol. 1, No. 2, 2016, H.84

sejumlah faktor, termasuk penerapan sanksi yang tidak terlalu berat, kelalaian dalam memberi tanggung jawab kepada pihak lain dan kurangnya pengawasan dari pihak yang berwenang.[7] Akibatnya akan ada pihak mengalami kerugian dengan adanya ketidakjujuran yang dilakukan seseorang.

Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) menyatakan bahwa transaksi elektronik tidak boleh mengandung sesuatu yang menyesatkan atau merugikan orang lain[8]. Sedangkan menurut definisinya, *quishing* dan *phishing* diartikan sebagai upaya memperoleh informasi pribadi seseorang, seperti nama, umur, alamat, nama pengguna, dan kata sandi suatu akun, serta informasi keuangan tentang nomor kartu kredit atau rekening menggunakan teknik manipulasi. Sehingga dalam praktiknya *quishing* dan *phishing* mengandung unsur *ghish* (penipuan) untuk melakukan pencurian. Pada saat pengguna *smartphone* melakukan transaksi, sistem tersebut disalahgunakan untuk melakukan *quishing* dan *phishing.* Sehingga transaksi tersebut yang awalnya memberikan manfaat ini kemudian dapat membahayakan jika disalahgunakan sebagai alat untuk melakukan *quishing* dan *phishing.*

Ancaman *quishing* harus dihilangkan karena dapat mendatangkan kemudharatan dan berpotensi membawa kerugian serta dampak negatif bagi kehidupan manusia. Sebagaimana dalam kaidah fikih yang berbunyi:

[7] Nur Anisha, "Indikasi Moral Hazard Dan Adverse Selection Dalam Penyaluran Dana Pihak Ketiga", Skripsi Uin Syarif Hidayaullah, Jakarta, 2016 H 119-120

[8] Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Ite)

الضَّرار يزالُ

"*kemudharatan itu harus dihilangkan".*

Kaidah tersebut menunjukkan bahwa menghilangkan kemudharatan adalah wajib.[9] Kegiatan muamalah atau transaksi dalam islam tidak boleh membahayakan dan tidak boleh saling merugikan.

Berdasarkan latar belakang di atas maka penulis tertarik untuk melakukan kajian lebih lanjut mengenai **Studi Analisis Teori *Moral Hazard* dan Hukum Ekonomi Syariah Terhadap *Quishing* dan *Phishing* dalam Transaksi Digital**

B. Definisi Operasional

1. Analisis adalah membedah suatu pemeriksaan ke dalam kejadian-kejadian (tindakan, karangan, dan lain-lain) untuk menyajikan situasi dan pemahaman nyata (masalah, sebab-sebab, dan lain-lain).[10]
2. *Moral hazard* merupakan istilah yang digunakan untuk menggambarkan perilaku tidak jujur atau sifat negatif yang meningkatkan frekuensi dan besarnya kerugian[11]
3. Hukum ekonomi syariah adalah sekumpulan hukum berdasarkan kaidah hukum Islam yang mengatur bagaimana individu berinteraksi satu sama lain

[9] Ade Dedi Rohayana, *Ilmu Qawa'id Fiqhiyyah Kaidah-Kaidah Hukum Islam* (Jakarta: Gaya Media Pratama, 2008) Hlm. 215.

[10] Kamus Besar Bahasa Indonesia, "Analisis", Https://Kbbi.Kemendikbud.Go.Id/Entri/Analisis, Diakses Pada 10 Mei 2022.

[11] Ade Heryana, *Moral Hazard Dalam Asuransi Kesehatan*, Universitas Esa Unggul (2020), H.1.

ketika melakukan kegiatan ekonomi dalam bentuk perjanjian ataupun akad muamalah.[12]

4. *Quishing* adalah sebuah taktik berbahaya yang memanfaatkan kode-kode yang ada di mana-mana ini sebagai saluran serangan dunia maya.[13] Dalam hal ini *quisher* menerapkan *quishing* dalam proses transaksi atau pembayaran nontunai melalui kode *QR* (*Quick Response*) yang mengandung *malware.*
5. *Phishing* adalah praktik penipuan dengan situs *web* palsu yang dapat diandalkan dalam interaksi elektronik untuk mencuri informasi pribadi, termasuk nama pengguna, kata sandi, dan nomor kartu kredit.[14]

C. Identifikasi dan Batasan Masalah

Identifikasi dan batasan masalah adalah langkah yang diambil dalam penelitian untuk mengidentifikasi dan mencatat sebanyak mungkin kemungkinan yang dapat dianggap sebagai masalah.[15] Berdasarkan latar belakang yang telah dijelaskan di atas, dapat diidentifikasi beberapa masalah sebagai berikut:

---

[12] Arifin Hamid, *Membumikan Ekonomi Syariah Di Indonesia*, (Jakarta: Pemuda Jakarta, 2008), 73.

[13] Bichnigauri, Avtandili, Et Al. "Unveiling Quishing: The Dark Side Of Qr Codes In Cyber Attacks." *Defence And Science* (2023): 96.

[14] Saputra Gulo And Others, „Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik" (2020) *Pampas: Journal Of Criminal*, H.70.

[15] Tim Penyusun Fakultas Syari'ah Dan Adab Universitas Nahdlatul Ulama' Sunan Giri, Buku Panduan Skripsi, (Bojonegoro : Fakultas Syari'ah Dan Adab Universitas Nahdlatul Ulama' Sunan Giri, 2022), 9.

1. Identifikasi Masalah

   a. Adanya penipuan ketika pengguna mengarahkan *smartphone* untuk *scan qr code* dalam melakukan pembayaran ternyata diarahkan ke *web* situs palsu.

   b. Adanya penyalahgunaan *scan qr code* dalam transaksi dengan menggunakan situs palsu yang mengandung *malware* khusus untuk mencuri informasi dan data.

   c. Adanya pengelabuhan untuk mengunduh sesuatu ke dalam perangkat yang digunakan pada saat melakukan transaksi melalui *scan qr code* sehingga membahayakan perangkat milik korban.

   d. Adanya pihak yang dirugikan akibat pencurian data melalui *quishing* dan *phishing* dalam transaksi digital

2. Batasan Masalah

   Berdasarkan identifikasi masalah yang telah dijelaskan sebelumnya, dan untuk menjaga agar uraian observasi dalam penelitian tetap fokus, penulis akan membatasi permasalahan pada:

   a. Mekanisme *quishing* dan *phishing* dalam transaksi digital

   b. Analisis *moral hazard* ter*had*ap *quishing* dan *phishing* dalam transaksi digital

   c. Tinjauan hukum ekonomi syariah ter*had*ap *quishing* dan *phishing* dalam transaksi digital

D. Rumusan Masalah

1. Bagaimana mekanisme *quishing* dan *phishing* dalam transaksi digital *?*
2. Bagaimana analisis teori *moral hazard* terhadap *quishing* dan *phishing* dalam transaksi digital *?*
3. Bagaimana tinjauan hukum ekonomi syariah terhadap *quishing* dan *phishing* dalam transaksi digital *?*

E. Tujuan Penelitian

Tujuan penelitian yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk mengetahui mekanisme *quishing* dan *phishing* dalam transaksi digital
2. Untuk menganalisis *moral hazard* ter*had*ap *quishing* dan *phishing* dalam transaksi digital
3. Untuk mengetahui tinjauan hukum ekonomi syariah ter*had*ap *quishing* dan *phishing* dalam transaksi digital

F. Kegunaan Penelitian

Penelitian ini diharapkan dapat memberikan manfaat minimal dalam dua bidang, yaitu teoritis dan praktis. Berikut gambaran kedua aspek tersebut:

1. Segi Teoritis

   Penelitian ini diharapkan memberikan kontribusi signifikan terhadap pengembangan ilmu pengetahuan, terutama di bidang Hukum Ekonomi Syariah. Temuan penelitian ini akan membantu dalam membangun, memperkuat, memperluas, dan menyempurnakan teori-teori yang sudah

ada, serta menjadi sumber referensi penting dalam menangani permasalahan yang berkaitan. Selain itu, data yang diperoleh dari penelitian ini diharapkan mampu memberikan penjelasan mendalam mengenai kejahatan dunia maya, khususnya *quishing* dan *phishing* dalam transaksi digital.

2. Segi Praktis

Dalam penelitian ini, penulis berusaha memberikan jawaban atas permasalahan terkait *quishing* dan *phishing* dalam transaksi digital, dengan tujuan agar pengguna dapat lebih memahami istilah-istilah tersebut dalam konteks kejahatan dunia maya pada transaksi digital, Misalkan:

a. Bagi Penulis

Penelitian ini bermanfaat bagi penulis dalam memberikan solusi terhadap permasalahan yang dihadapi dan memperluas wawasan mengenai istilah *quishing* dan *phishing* dalam transaksi digital. Selain itu, penelitian ini akan meningkatkan pengetahuan penulis tentang mekanisme serangan dan strategi pencegahannya, serta memberikan kontribusi signifikan pada literatur akademis di bidang keamanan siber dan Hukum Ekonomi Syariah.

b. Bagi Pemerintah

Hasil dari penelitian ini diharapkan dapat membantu pemerintah dalam merumuskan dan memperbaiki kebijakan yang terkait *quishing* dan *phishing* dalam transaksi digital. Penelitian ini dapat menyediakan data dan analisis yang mendalam untuk meningkatkan efektivitas regulasi dan perlindungan hukum, sehingga masyarakat lebih

terlindungi dari kerugian akibat serangan siber. Selain itu, penelitian ini juga dapat menjadi acuan dalam pengembangan strategi keamanan nasional dan edukasi publik untuk meningkatkan kesadaran serta kewaspadaan terhadap ancaman *quishing* dan *phishing*.

c. Bagi Masyarakat

Penulis berharap dapat memberikan edukasi kepada masyarakat, sehingga meningkatkan kesadaran mereka tentang istilah *quishing* dan *phishing* dalam transaksi digital. Dengan pemahaman yang lebih baik, masyarakat akan lebih waspada dan mampu mengambil langkah-langkah pencegahan untuk melindungi diri mereka dari ancaman tersebut.

G. Penelitian Terdahulu

Tabel 1.1 Penelitian Terdahulu

No.	Penelitian	Hasil	Persamaan	Perbedaan
1.	Fazwi Aswin *Had*ist yang berjudul "Sanksi Pelaku Pidana *Phishing* (Komparasi Undang-Undang ITE dan Teori *Qiyas*)". (Fakultas Syariah dan Hukum Universitas Islam Negeri Sunan Kalijaga	Penelitian ini membahas tentang sanksi bagi pelaku pidana *phising* dalam UU ITE dan teori *qiyas*. Hasil dari penelitian ini adalah perbuatan *phising* termasuk bentuk kejahatan penipuan, baik itu dilakukan secara konvensional maupun melalui media internet, dalam hal ini kasus peretasan, dengan menggunakan jenis *qiyas awla*. Tindak pidana mengakses komputer/sistem elektronik milik orang	Persamaan dari penelitian ini, terletak pada satu objek penelitian yang sama yaitu kejahatan elektronik (*cybercrime*) dalam bentuk penipuan menggunakan metode *phishing*.	Sedangkan perbedaannya terletak pada metode baru dalam kejahatan elektronik (*cybercrime*) yaitu *quishing* serta terdapat perbedaan pada teori yang digunakan penulis.

	Yogyakarta: 2022).[16]	lain tanpa izin (melawan hukum) dapat disamakan dengan memasuki rumah tanpa izin dikarenakan keduanya terdapat persamaan *illat*, yaitu tanpa izin. Perbedaannya ialah: meskpiun sama-sama dikenakan *Jarimah Ta'sir*, namun dalam pengaturannya masih memiliki keterbatasan, yaitu terletak kepada hubungan transaksi elektronik, yaitu antara produsen dan konsumen serta dalam lingkup pemberitaan bohong dan penyesatan melalui internet.		
2.	Farid Nabila dengan judul "Perlindungan Hukum Ter*had*ap Korban Penipuan Melalui Sms (*Short Message Service*)". Program Studi Hukum Pidana Islam Fakultas Syariah Universitas Islam Negeri Kiai Haji Achmad Siddiq	Penelitian membahas tentang perlindungan hukum positif dan hukum pidana islam ter*had*ap korban penipuan melalui SMS. Hasil penelitian ini menyatakan bahwa Untuk melindungi hak pertanggung jawaban, diantaranya: KUHP BUKU II BAB XXV Pasal 378 Tentang penipuan, yang dapat dijadikan sebagai dasar hukum untuk melindungi hak pertanggung jawaban korban dan mengadili para tersangka. Sedangkan hak jaminan perlindungan dan ganti rugi dapat ditemukan dalam beberapa aturan	Persamaan dari penelitian ini, sama-sama membahas kejahatan elektronik (*cybercrime*) dalam bentuk penipuan.	Perbedaannya, penelitian yang ditulis oleh Farid Nabila ini berfokus pada perlindungan hukum ter*had*ap korban penipuan melalui SMS, sedangkan penulis memfokuskan penelitian ini pada mekanisme *phishing* dan *quishing* dalam *cybercrime*

[16] Fazwi Aswin Hadist, "Sanksi Pelaku Pidana *Phishing* (Komparasi Undang-Undang Ite Dan Teori *Qiyas*)", (Skripsi Universitas Islam Negeri Sunan Kalijaga Yogyakarta, 2022)

	Jember: 2023).[17]	diantaranya adalah: Undang-Undang No. 31 tahun 2014 Perubahan Undang-Undang No 13 tahun 2006 tentang perlindungan saksi dan korban serta Kitab Undang-Undang Hukum Pidana pasal 98 sampai 101 yang secara teknis dapat diajukan melalui penggabungan gugatan acara perdata atau melalui Kitab Undang-Undang Hukum Acara Pidana. Adapun menurut Hukum Pidana Islam, penipuan SMS tergolong dalam *jarimah ta'zir*. Dalam kasus ini hukuman yang diberikan kepada tindak pidana penipuan dalam Hukum Islam yang mana hukuman ini dapat berupa hukam penjara, jilid, diasingkan, diperingati, dibunuh dan lain sebagainya.		transaksi digital untuk dianalisis dengan teori *moral hazard* dan hukum ekonomi syariah.
3.	Rifki Ihza Mahendra yang berjudul Tindak Pidana *Skimming* Melalui Mesin Atm Dalam Hukum Positif Dan Hukum Pidana Islam (Studi Kasus Tindak Pidana	Penelitian ini juga membahas tentang pandangan hukum positif dan juga hukum islam ter*had*ap pelaku kejahatan *skimming* ter*had*ap nasabah bank BCA. Hasil penelitian ini menjelaskan mengenai modus operandi yang digunakan oleh pelaku kejahatan *skimming* yang mana kasus kejahatan *skimming* ini masuk dalam kategori	Persamaan dari penelitian ini terletak pada kejahatan elektronik (*cybercrime*) dengan cara mencuri data informasi seseorang untuk kepentingan pribadi.	Perbedaan keduanya terletak pada teori dan tinjauan hukum yang digunakan penulis.

[17] Farid Nabila, "Perlindungan Hukum Terhadap Korban Penipuan Melalui Sms (*Short Message Service*)", (Skripsi Universitas Islam Negeri Kiai Haji Achmad Siddiq, Jember, 2023)

	Skimming Ter*had*ap Nasabah Bank BCA). Prodi Hukum Pidana Islam Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta: 2020).[18]	*Infringements of privacy* melihat kepada objek kejahatan yaitu informasi dan data pribadi seseorang seperti pin ATM dan data dari kartu ATM nasabah. Selanjutnya hasil penelitian ini juga menjelaskan pasal-pasal yang dapat digunakan untuk menjerat pelaku kejahatan skimming dalam kasus ini seperti Pasal 362 KUHP dan atau pasal 30 jo pasal 46 UU ITE, serta Pasal 81 UU Transfer Dana dan atau Pasal 3, 4, dan 5 UU TPPU. Kemudian dalam perspektif hukum pidana Islam tindak Pidana *skimming* masuk kedalam kategori *jarimah takzir*, walaupun unsur-unsur tindak pidana *skimming* memiliki kesamaan dengan *jarimah sariqah* dan *hirabah* akan tetapi modus operandi nya berbeda dengan kedua *jarimah* itu.		

H. Kerangka Teori

1. Moral Hazard

Moral hazard adalah praktik ekonomi yang memaksimalkan utilitas diri sendiri dengan mengorbankan orang lain. Hal ini terjadi ketika para pihak

[18] Rifki Ihza Mahendra, "Tindak Pidana *Skimming* Melalui Mesin Atm Dalam Hukum Positif Dan Hukum Pidana Islam (Studi Kasus Tindak Pidana *Skimming* Terhadap Nasabah Bank Bca)", (Skripsi Universitas Islam Negeri Syarif Hidayatullah, Jakarta, 2020)

mengadakan kontrak dengan penyelesaian yang tidak lengkap atau terbatas sehingga menghalangi mereka untuk membayar agen yang bertanggung jawab atas tindakan mereka atau untuk memperoleh manfaat penuh dari tindakan mereka.[19]

Moral hazard terjadi ketika seseorang atau sesuatu bertindak tidak bertanggung jawab untuk mengalihkan kesalahan atas hasil kegiatannya kepada orang lain, dan tidak bertanggung jawab atas tindakannya.

Teori ini digunakan untuk menganalisis teori *moral hazard* terhadap *quishing* dan *phishing* dalam transaksi digital.

2. *Ḍarar*

Secara etimologi, *al-Ḍarar* (bahaya) adalah lawan dari *al-Naf'u* (manfaat). Juga bisa diartikan bahwa *al-Ḍarar* adalah segala segala jenis keadaan yang tidak menguntungkan, kelangkaan, tantangan, atau kemalangan. Sedangkan secara terminologi, maknanya tidak jauh dari pengertiannya secara bahasa, yaitu kekurangan atau kerusakan yang menimpa sesuatu.[20]

Dalam Syariah Islam, segala jenis kerugian hukum dilarang. Seseorang tidak boleh merugikan dirinya sendiri atau orang lain terhadap jiwa, harta benda, atau kehormatannya. Dan hukum wajib mencegah terjadinya suatu

[19] Kotowitz, Moral Hazard. J. Eatwell Et Al. (Eds.), Allocation, Information And Markets, London. 1989, H.207

[20] Wildan Jauhari, *Kaidah Fikih; Adh-Dhararu Yuzal*, (Jakarta: Rumah Fiqih Publishing, 2018), H.6

kerugian (preventif), karena syariat ini juga mewajibkan penghapusan kerugian setelah terjadi (represif).

Teori ini digunakan untuk mengetahui bagaimana tinjauan hukum ekonomi syariah terhadap *quishing* dan *phishing* dalam transaksi digital menggunakan teori *ḍarar*.

3. *Ghish*

Yang dimaksud dengan *ghish* adalah penjual menampilkan barang tidak sesuai dengan hakikatnya, atau ia menyembunyikan cacat barang, jika pembeli mengetahui hakikat barang sesungguhnya ia tidak akan membeli barang dengan harga yang diinginkan penjual.[21]

Dari definisi di atas jelas bahwa penjual menggunakan *ghish* untuk meraup untung yang lebih besar dari harga biasa dengan cara berbohong atau melakukan penipuan.

Awalnya, *ghish* memang merupakan bentuk penipuan dalam konteks jual beli, di mana penjual menipu pembeli dengan cara menampilkan barang tidak sesuai dengan hakikatnya atau menyembunyikan cacat barang. Tujuannya adalah untuk mendapatkan keuntungan yang lebih besar dari harga sebenarnya dengan cara berbohong atau melakukan penipuan.

Namun, dalam konteks *quishing* dan *phishing*, *ghish* merupakan bentuk penipuan untuk melakukan pencurian informasi, data pribadi dan uang dalam rekening. *Quishing* menggunakan kode QR palsu atau pesan teks palsu untuk menipu korban, sedangkan phishing menggunakan email palsu

[21] Abdullah Assulami, Al Ghish wa atsaruhu fil uqud, Jilid 1, H.33

atau pesan teks yang meniru entitas yang sah untuk mencuri informasi pribadi korban. Kedua teknik ini memanfaatkan kepercayaan dan ketidaktahuan korban untuk mendapatkan akses ke informasi yang kemudian dapat disalahgunakan untuk tujuan kriminal seperti pencurian identitas atau penipuan finansial.

Teori ini digunakan untuk mengetahui tinjauan Hukum Ekonomi Syariah terhadap *quishing* dan *phishing* dalam transaksi digital menggunakan teori *ghish*.

I. Metode Penelitian

1. Jenis Penelitian

Untuk mendukung penelitian yang berkualitas dan dapat dipertanggungjawabkan secara ilmiah, peneliti menjelaskan metode penelitian yang digunakan untuk menginvestigasi dan menganalisis permasalahan yang terkait dengan *Quishing* dan Phishing Dalam Transaksi Digital: Studi Analisis Teori *Moral Hazard* dan Hukum Ekonomi Syariah. Oleh karena itu, metode penelitian yang diterapkan dalam skripsi ini adalah sebagai berikut:

1. Jenis Penelitian

Penelitian yang dilakukan oleh peneliti merupakan jenis penelitian kualitatif yang cenderung bersifat deskriptif dan sering menggunakan analisis.[22] Berdasarkan pada jenis penelitian tersebut, metode pendekatan

[22] Muhammad Ramdhan, *Metode Penelitian*, (Surabaya : Cipta Media Nusantara, 2021), H. 6.

yang digunakan ialah penelitian pustaka (*Library Research*). Dikarenakan ini adalah penelitian pustaka, data dikumpulkan dari literatur-literatur atau sumber-sumber kepustakaan yang relevan dengan topik penelitian.

2. Sumber Data

Untuk mengidentifikasi sumber data penelitan, maka penulis mengklasifikasikannya menjadi dua sumber, sebagai berikut:

a. Data Primer

Menurut Moh. Pabundu Tika yang dikutip oleh A'imatul Rosyidah dalam skripsinya menjelaskan bahwa data primer ialah sumber data yang didapat secara langsung dari objek atau responden penelitian.[23] Dalam hal ini sumber data primer didapatkan dari hasil studi pustaka pada APWG (*Anti Phishing Working Group*) dan *Infosecurity Magazine* serta artikel-artikel yang berhubungan dengan penelitian.

b. Data Sekunder

Data sekunder yang dimanfaatkan oleh peneliti berasal dari berbagai sumber seperti teori-teori, laporan penelitian sebelumnya, buku-buku, berita, dan jurnal-jurnal yang relevan dengan fokus penelitian.

[23] A'imatul Rosyidah, "Analisis Penyaluran Dana *Crowdfunding* Di Aplikasi Kitabisa Perspektif Hukum Positif Dan Hukum Ekonomi Syariah", (Skripsi, Universitas Nahdlatul Ulama Sunan Giri (Unugiri), Bojonegoro, 2023), H. 16.

3. Teknik Pengumpulan Data dan Analisis Data

Teknik awal yang dilakukan oleh peneliti adalah dengan menggumpulkan tulisan-tulisan ilmiah yang membahas tentang *quishing* dan *phishing* setelah data-data terkumpul, langkah kedua adalah melakukan kajian atas beberapa tulisan ilmiah untuk menemukan data yang dibutuhkan oleh penulis. Sebagai data tambahan, peneliti juga mengumpulkan data lainnya, seperti konten-konten vidio, berita, artikel dan bahan-bahan lainnya yang ada kaitannya dengan fokus penelitian.

Setelah data terkumpul, langkah berikutnya adalah melakukan analisis data. Peneliti menggunakan metode analisis kualitatif, yang melibatkan analisis data dengan memberikan komentar menggunakan teori-teori yang relevan terhadap objek penelitian. Yakni dengan cara menganalisis teori *moral hazard, darar, ghish* dengan *quishing* dan *phishing* dalam transaksi digital.

J. Sistematika Pembahasan

Sistematika pembahasan penelitian skripsi ini penulis akan membagi dalam lima bab sebagai berikut:

Bab I Pendahuluan merupakan gambaran menyeluruh dari isi penelitian yang dijelaskan melalui beberapa sub-bab, termasuk latar belakang masalah, definisi operasional, identifikasi dan batasan masalah, rumusan masalah, tujuan penelitian, kegunaan penelitian, penelitian terdahulu, kerangka teori, metode penelitian dan sistematika pembahasan.

Bab II Kerangka teori, pada bab ini akan memuat teori-teori yang berkaitan dengan penelitian meliputi teori *moral hazard, ḍarar* dan *ghish.* Pertama, teori *moral hazard* menguraikan definisi *moral hazard*, jenis-jenis dan tingkatan *moral hazard*. Kedua, teori *ḍarar* menguraikan: pengertian *ḍarar* dan dasar hukum *ḍarar*. Ketiga, teori *ghish* meliputi: definisi, landasan hukum, bentuk-bentuk *ghish*.

Bab III Deskripsi Lapangan, menjelaskan tentang transaksi digital, gambaran umum dan mekanisme *quishing* serta gambaran umum dan mekanisme *phishing.*

Bab IV Temuan dan Analisis. Temuan mengenai perilaku *quishing* menurut teori *moral hazard* dan hukum ekonomi syariah. Dalam analisis ini, nantinya akan diuraikan masing-masing pandangan hukum dalam menilai hal tersebut.

Bab V Penutup yang berisi rangkuman dari seluruh bab yang telah disajikan oleh penulis, menggambarkan kesimpulan yang ditarik dari analisis yang telah dilakukan, serta memberikan solusi terhadap permasalahan yang telah diidentifikasi. Selain itu, penutup juga berfungsi sebagai platform untuk menyampaikan rekomendasi dari peneliti berdasarkan temuan yang telah diungkapkan dalam penelitian tersebut. Daftar pustaka serta lampiran untuk memberikan dukungan lebih lanjut terhadap argumen yang telah dibahas dalam penelitian.