TEHNIK *PHISING* (PENCURIAN DATA PRIBADI) DALAM PERSPEKTIF HUKUM PIDANA ISLAM DAN HUKUM POSITIF

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana Hukum (S.H)

Pada Jurusan Perbandingan Mazhab Fakultas Syariah

Universitas Islam Negeri (UIN) Datokarama Palu

Oleh:

AHMAD YASIR ARAFAH

NIM : 193080012

JURUSAN PERBANDINGAN MAZHAB

FAKULTAS SYARIAH

UNIVERSITAS ISLAM NEGERI (UIN) DATOKARAMA PALU

2024

PERNYATAAN KEASLIAN SKRIPSI

Dengan penuh kesadaran, penulis yang bertanda tangan di bawah ini menyatakan bahwa skripsi dengan judul " ***Fenonena phishing (pencurian data pribadi) dalam perspektif hukum pidana islam dan hukum positif*** " benar adalah hasil karya penulis sendiri. Jika dikemudian hari terbukti bahwa skripsi ini merupakan duplikat, tiruan, plagiat, atau dibuat oleh orang lain, sebagian atau sepenuhnya, maka skripsi dan gelar yang diperoleh karenanya batal demi hukum.

Palu, 22 Juli 2024 M
Palu, 16 Muharam 1446 H

Penulis

Yasir Arafah
19.30.800.12

PERSETUJUAN PEMBIMBING

Skripsi yang berjudul " Fenomena *Phising* (pencurian data pribadi) dalam perspektif hukum pidana Islam dan Hukum Positif " oleh mahasiswa atas nama Ahmad Yasir Arafah NIM : 193080012, mahasiswa Jurusan Perbandingan Mazhab, Fakultas Syariah, Universitas Islam Negeri (UIN) Datokarama Palu, setelah dengan seksama meneliti dan mengoreksi skripsi yang bersangkutan, maka masing-masing pembimbing memandang bahwa skripsi tersebut telah memenuhi syarat ilmiah dan dapat diajukan untuk diujikan.

Palu, 22 Juli 2024 M
16 Muharram 1446 H

Pembimbing I,	Pembimbing II,
Prof. Dr. Marzuki, M.H	Dr. Sitti Musyahidah, M.Th.I.
NIP.19561231 198503 1 024	NIP.19670710 199903 2 005

PENGESAHAN SKRIPSI

Skripsi mahasiswa atas nama Ahmad Yasir Arafah NIM 193080012 dengan judul **Fenomena Phishing (Pencurian Data Pribadi) dalam Perspektif Hukum Pidana Islam dan Hukum Positif** yang telah diujikan di hadapan Dewan Penguji pada tanggal 12 Agustus 2024 Masehi bertepatan dengan tanggal 01 Safar 1446 Hijriah, dipandang telah memenuhi kriteria penulisan karya ilmiah dan dapat diterima sebagai persyaratan guna memperoleh gelar Sarjana Hukum (SH) pada Fakultas Syariah, Jurusan Perbandingan Mazhab Universitas Islam Negeri (UIN) Datokarama Palu.

DEWAN PENGUJI

Jabatan	Nama	Tanda Tangan
Ketua Dewan Penguji	Yuni Amelia, S.Pd., M.Pd.	
Penguji I	Dr. M. Taufan B, S.H., M.Ag., M.H.	
Penguji II	Randy Atma R. Massi, M.H	
Pembimbing I	Prof. Dr. H. Marzuki, M.H	
Pembimbing II	Dr. Hj. Sitti Musyahidah, M.Th.I	

Mengetahui,
Ketua Jurusan,

Muhammad Syarief Hidayatullah, M.H.
NIP 199204252019031005

Mengesahkan,
Dekan,

Dr. H. Muhammad Syarief Hasyim, Lc., M.Th.I.
NIP 196512312000031030

KATA PENGANTAR

بِسْـــمِ اللهِ الرَّحْمنِ الرَّحِـيْمِ

اَلْحَمْدُ لِلّـهِ رَبِّ الْعَـا لَمِـيْن وَالصَّلاَةُ وَالسَّـلاَمُ عَلَى اَشْـرَفِ الْأَنْبِيَـاءِ والْمُرْسَلِيْنَ

سَيِّدِنَا مُحَمَّدٍ وَعَلَى آلِهِ وَاَصْحـَابِهِ اَجْمَعِـيْنَ, اَمَّـابَعْـدُ

Puji syukur kita panjatkan kehadirat Allah swt, karena berkat nikmat, rahmat dan hidayah-Nya sehingga skripsi ini dapat diselesaikan sesuai waktu yang telah direncanakan. Shalawat dan salam penulis persembahkan kepada Nabi Muhammad saw, beserta keluarga serta sahabatnya yang telah mewariskan Al-Qur'an dan hadits sebagai pedoman umatnya.

Penulis menyadari sepenuhnya bahwa dalam penulisan skripsi ini masih banyak mendapatkan bantuan moril maupun materil dari berbagai pihak. Oleh karena itu penulis mengucapkan banyak terima kasih kepada :

1. Kedua orang tua tercinta, ayah kami Hafiludin S.pd dan ibunda Suryani yang telah melahirkan, mengasuh, membesarkan mendidik dan memberi motivasi penulis sehingga dapat menyelesaikan studi jenjang pendidikan dasar sampai dengan perguruan tinggi.
2. Bapak Prof. Dr. H. Lukman S Thahir, M.Ag selaku Rektor Universitas Islam Negeri (UIN) Datokarama Palu, beserta segenap unsur pimpinan UIN Datokarama Palu, Bapak Dr. Hamka, M.Ag selaku Wakil Rektor Bidang Akademik dan Pengembangan Lembaga, Bapak Prof. Dr. Hamlan, M.Ag selaku Wakil Rektor Bidang Administrasi Umum Perencanaan dan Keuangan, dan Bapak Dr. Faisal At-Tamimi selaku Wakil Rektor Bidang Kemahasiswaan, alumni dan kerjasama beserta jajarannya, yang telah memberikan kesempatan kepada penulis sehingga dapat menuntut ilmu di kampus ini dan telah memberikan kebijakan selama perkuliahan dan penyelesaian studi hingga semuanya dapat berjalan dengan lancar.

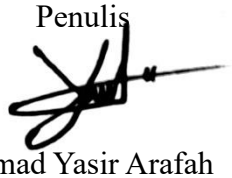
3. Bapak Dr. H. Muhammad Syarif Hasyim, Lc.M.Th.I selaku Dekan Fakultas Syariah, UIN Datokarama Palu. Ibu Dr. Mayyadah, Lc., M.H.I. selaku Wakil Dekan Bidang Akademik dan Pengembangan Kelembagaan, dan Bapak Drs. Ahmad Syafii, M.H. selaku Wakil Dekan Bidang Administrasi Umum Perencanaan dan Keuangan dan Ibu Dr. Hj. Sitti Musyahidah, M.Th.I sealaku Wakil Dekan Bidang Kemahasiswaan dan kerjasama yang telah memberikan kesempatan kepada penulis untuk menuntut ilmu pada Fakultas Syariah sehingga dapat menyelesaikan studi dengan baik.
4. Bapak Syarif Hidayatullah, S.H.I., M.H. selaku Ketua Prodi Perbandingan Mazhab dan Bapak Nursalam Rahmatullah, M.H. selaku Sekretaris Prodi Perbandingan Mazhab yang telah banyak membantu, mengarahkan, membimbing dan memberi motivasi selama proses belajar dan penyelesaian studi di Program Studi Perbandingan Mazhab.
5. Bapak Prof. Dr. H. Marzuki, M.H selaku Dosen Pembimbing 1, dan Ibu Dr. Hj. Sitti Musyahidah, M.Th.I selaku Dosen Pembimbing 2 yang telah membimbing dengan ikhlas dan memberikan masukan-masukan selama proses penulisan skripsi ini hingga selesai dengan tepat waktu dan sesuai harapan.
6. Bapak Dr. M. Taufan B, S.H., M.Ag., M.H. selaku Penguji Utama 1 dan Bapak Randy Atma R. Massi, M.H selaku Penguji Utama 2 yang telah menguji dan memberikan masukan agar skripsi yang telah dibuat bisa bermanfaat untuk agama dan bangsa
7. Seluruh Bapak/Ibu Dosen Fakultas Syariah khususnya prodi Perbandingan Mazhab yang telah membagikan ilmunya kepada penulis selama belajar di UIN Datokarama Palu.

8. Seluruh staf Akedemik Kemahasiswaan Fakultas Syariah UIN Datokarama Palu yang telah melayani penulis dalam proses pengurusan berkas-berkas selama menjadi mahasiswa Fakultas Syariah UIN Datokarama Palu.
9. Kepala Perpustakaan UIN Datokrama Palu, Bapak Rifa'I, S.E., M.M. beserta seluruh staf Perpustakaan UIN Datokarama Palu yang telah memberikan izin dan pelayanan kepada penulis dalam mencari referensi sebagai bahan dalam penulisan skripsi.
10. Kepada keluarga besar Himpunan Mahasiswa Islam (HMI) Majelis Penyelamat Organisasi (MPO) Cabang Palu yang selalu memotivasi dalam proses belajar, berdiskusi dan melakukan aksi-aksi kebaikan lainya.
11. Kepada keluarga Himpunan Mahasiswa Program Studi Perbandingan Mazhab (HMPS PM) UIN Datokaram Palu yang sudah mengamanahkan kepada penulis untuk menjadi Wakil Ketua umum HMPS PM selama satu periode, dan juga teman-teman Persatuan Perbandingan Mazhab dan Hukum Se Indonesia (PPMHSI) yang menjadi tempat belajar dalam banyak hal.
12. Kepada teman-teman seperjuangan di Program Studi Perbandingan Mazhab 2019 UIN Datokaram Palu yang telah menemani dan membantu selama belajar dikelas Perbandingan Mazhab.
13. Kepada sahabat-sahabatku, Virgiawan Listanto Ndeo, Muhammad Rafli, Muhammad Fauzan, Ahmad Reski, Jabir M yamin, Muhammad alamsyah, Africhal, Adriatman Lumayo, Fikran Hafidz, Ma'ruf , Taufik Rifal Hasbi, Hamdan Nasrullah Amin, Zainal Abidin, Rahmat Abdullah, Miftahul Jannah, Imsartina, Aisya Musdalifa, Susi Lestari, Muhammad farhat, dan ahmad Rahim yang bersama-sama penulis selama belajar di UIN Datokaram Palu.

14. Semua pihak yang tidak dapat disebutkan namanya satu persatu yang telah berjasa memberikan ilmu dan motivasi serta bantuan dalam penyusunan skripsi. Penulis sangat menyadari bahwa skripsi ini jauh dari kesempurnaan, untuk itu penulis mengharapkan kritik dan saran semua pihak. Akhirnya, penulis berharap semoga skripsi ini bermanfaat bagi seluruh pembaca dalam pengembangan disiplin ilmu Perbandingan Mazhab di masa mendatang.

Palu, 22 Juli 2024 M
Palu, 16 muharam 1446 H

Penulis



Ahmad Yasir Arafah
19.30.800.12

DAFTAR ISI

DAFTAR BAGAN

ABSTRAK

Nama : Ahmad Yasir Arafah
NIM : 19.3.080.012
Fakultas : Syariah
Jurusan : Perbandingan Mazhab
Judul : Fenomena *Phishing* (Pencurian data Pribadi) dalam Perspektif Hukum pidana Islam dan Hukum Positif

Phishing adalah bentuk kejahatan siber modern yang mengancam keamanan data pribadi. Pelakunya menyamar sebagai pihak terpercaya, menggunakan email, situs web palsu, atau pesan singkat untuk menipu korban. Tujuannya adalah membujuk korban agar secara sukarela memberikan informasi sensitif. Dengan memanfaatkan teknik rekayasa sosial, *phishing* menjadi ancaman siber yang sulit diatasi dan sangat meresahkan di era digital ini

Penelitian ini bertujuan untuk mengetahui dan mehami Fenomena serta tinjauan tinjauan Hukum Pidana islam dan Hukum positif terhadap salah satu bentuk kejahatan siber yakni *Phsihing*. Untuk mencapai tujuan tersebut, digunakan metode penelitian hukum Normatif dengan menggunakan pendekatan Perundang – undangan, Konseptual dan Teologi. Sumber data pada Penelitian ini menggunakan data primer, sekunder dan tersier

Hasil Penelitian skripsi ini menguraikan berbagai teknik phishing, termasuk *phishing scam, blind phishing, spear phishing, cloning phishing, whaling, vishing, pharming, dan smishing*, serta taktik umum seperti *e-mail phishing, website phishing, dan malware phishing*. Studi ini juga membandingkan perspektif hukum pidana Islam dan hukum positif terhadap *phishing*. Dalam hukum Islam, *phishing* disamakan dengan pencurian (*sariqah*) yang menggunakan penipuan dan dapat dikenai hukuman *ta'zir*. Sementara itu, hukum positif mengatur phishing melalui UU ITE Pasal 27-37 dan UU No. 27 tahun 2022 tentang Perlindungan Data Pribadi, khususnya Pasal 67. Penelitian ini menekankan bahwa *phishing* merupakan ancaman serius yang diakui dan diatur dalam kedua sistem hukum, menunjukkan pentingnya perlindungan data dan keamanan siber di era digital.

Dari penelitian yang dilakukan, dapat disimpulkan bahwa baik hukum pidana Islam maupun hukum positif Indonesia memiliki kerangka untuk menangani kejahatan *phishing*, meskipun dengan pendekatan yang berbeda. Hal ini menunjukkan bahwa kedua sistem hukum tersebut berupaya beradaptasi dengan tantangan kejahatan siber modern. Dalam implentasinya Penting untuk terus memperbarui kerangka hukum agar sesuai dengan perkembangan teknologi dan modus operandi kejahatan siber. Diperlukan sinergi antara pemerintah, penegak hukum, penyedia layanan internet, institusi keuangan, dan masyarakat untuk menciptakan ekosistem digital yang lebih aman. Pemerintah harus meningkatkan perhatian terhadap kejahatan komputer, terutama pencurian data pribadi, baik di instansi pemerintah maupun masyarakat umum. Penguatan pertahanan teknologi menjadi kunci dalam mengatasi masalah ini.

BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan pesat teknologi informasi, khususnya di bidang komputasi dan internet, telah terbukti membawa banyak manfaat positif bagi kemajuan hidup manusia. Namun, penting untuk dicatat bahwa di balik berbagai keunggulan dan kemudahan yang ditawarkan, terdapat potensi bahaya yang dapat mengancam kehidupan dan budaya masyarakat, teknologi informasi saat ini dapat diibaratkan sebagai "pedang bermata dua". Di satu sisi, ia berkontribusi pada peningkatan kesejahteraan, kemajuan, dan perkembangan peradaban manusia. Namun di sisi lain, teknologi yang sama juga dapat menjadi sarana yang efektif untuk melakukan tindakan melanggar hukum, termasuk berbagai bentuk kejahatan. Berbagai tindak pidana yang memanfaatkan teknologi informasi ini kemudian dikenal dengan istilah "*cybercrime"* [1]

Kejahatan siber atau *cybercrime* telah muncul sebagai bentuk baru tindak kriminal yang menarik perhatian global. *Volodymyr Golubev mengategorikannya sebagai "bentuk baru perilaku anti-sosial".* Fenomena ini tidak dapat disangkal lagi merupakan konsekuensi negatif dari kemajuan teknologi*, Cybercrime* dapat dilihat sebagai sisi gelap dari perkembangan teknologi yang memiliki dampak merugikan yang sangat luas. Pengaruhnya menyentuh hampir seluruh aspek kehidupan modern saat ini, mulai dari keamanan data pribadi hingga stabilitas ekonomi dan sosial. Kehadiran *cybercrime* menunjukkan bahwa seiring dengan manfaat yang dibawa

[1] A. Aco Agus dan Riskawati, "Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," *Jurnal Supremasi,* Vol. 10, N (2016): 56.

oleh inovasi teknologi, muncul pula tantangan-tantangan baru yang perlu diatasi oleh masyarakat global. Hal ini menegaskan pentingnya pendekatan yang seimbang dalam mengadopsi dan mengelola kemajuan teknologi di era digital.[2]

Menurut Pasal 30 Ayat (2) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi: "*Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik*".

Telah disebutkan bahwa, seiring dengan perputaran waktu dan perkembangan kehidupan masyarakat, penggunaan perangkat komputer semakin berkembang pesat. Di industri, kedokteran, pendidikan, pemerintahan, akutansi, dan perbankan, tidak ada bidang yang terlepas dari program komputerisasi. Di sisi lain, potensi keuntungan dari kemajuan teknologi informasi telah menarik perhatian pihak-pihak lain yang dengan niat jahat mencari keuntungan dengan melakukan penipuan, seperti mengirimkan *e-mail* palsu untuk mendapatkan informasi pribadi seperti User ID, PIN, nomor rekening bank, dan nomor kartu kredit seseorang secara tidak sah. Ini dikenal sebagai *phishing*[3].

Sutan Remy Syahdeni menjelaskan bahwa *phishing* adalah salah satu jenis kejahatan internet yang dikenal sebagai *identity theft*, di mana seseorang mengirimkan e-mail palsu kepada seseorang, perusahaan, atau organisasi dengan

[2] Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara (Cyber Crime), (Bandung: PT Refika Aditama, 2005), 451.

[3] *http://www.hukumonline.com/klinik/detail/cl5050/phising??? Diakses 28 Agustus 2023*

mengatakan bahwa pengirim adalah perusahaan nyata. Tujuan dari *phishing* adalah untuk mendapatkan informasi pribadi dari korban.[4]

Menurut Pasal 1 ayat (1) UU Perlindungan Data Pribadi (PDP) menyatakan "*Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik*".

Pada umumnya, serangan *phishing* memang terjadi melalui email dan platform media sosial seperti *Facebook, Instagram*, dan *WhatsApp*. Namun, ada juga jenis serangan *phishing* yang dilakukan melalui pesan singkat (SMS) yang diterima di ponsel. Meskipun banyak serangan *phishing* dilakukan dengan tampilan yang sangat meyakinkan, yang sering kali mencakup logo perusahaan dan tautan ke situs web yang asli, ada kasus di mana serangan ini dilakukan oleh penjahat yang kurang terampil atau amatir.

Karakteristik serangan *phishing* oleh amatir ini bisa terlihat dari beberapa hal, seperti format pesan yang acak-acakan, kesalahan tata bahasa dalam kalimat, dan kesalahan ejaan pada kata-kata yang digunakan dalam pesan. Biasanya, serangan *phishing* yang dilakukan oleh para pemula ini lebih mudah dikenali oleh korban yang waspada. Meskipun demikian, serangan semacam itu tetap dapat merugikan orang jika mereka tidak berhati-hati, sehingga tetap penting untuk selalu waspada dan tidak mengabaikan tanda-tanda yang mencurigakan, bahkan jika pesannya terlihat kurang profesional. [5]

---

[4] Syahdeini, Sutan Remy. 2009. *Kejahatan & Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafita, 63-64.

[5] Nafi"ah, Rahmawati (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. Jurnal Cybersecurity Dan Forensik Digital, 3(1), h.,7-14.

Para pelaku *phishing* memanfaatkan situs web tiruan untuk menjerat korbannya. Melalui situs palsu ini, mereka berusaha menggoda pengguna agar mengungkapkan data penting seperti identitas pengguna, *Password*, nomor PIN, detail rekening bank, serta nomor kartu kredit. Begitu korban terperdaya dan memasukkan kredensial mereka ke situs web palsu tersebut, seluruh informasi yang diinput akan segera terekam di server milik penipu. Berbekal identitas pengguna dan kata sandi yang berhasil dicuri, pelaku *phishing* kemudian memperoleh akses tak terbatas ke akun korban. Setelah berhasil menerobos, penipu memiliki keleluasaan penuh untuk memanipulasi dan mengeksploitasi akun korban sesuka hati. Situasi ini membuka peluang bagi beragam aktivitas ilegal yang dapat merugikan korban secara signifikan, Taktik ini menggambarkan betapa krusialnya bagi pengguna internet untuk selalu waspada dan berhati-hati dalam melindungi informasi pribadi mereka, khususnya ketika berhadapan dengan situs web yang meminta data sensitif.[6].

Berdasarkan data dari Indonesia *Anti-Phishing Data Exchange* (IDADX), terjadi lonjakan signifikan dalam jumlah laporan serangan *phishing* di Indonesia. Pada kuartal I 2023, IDADX mencatat 26.675 laporan serangan *phishing,* meningkat tajam dari 6.106 laporan pada kuartal IV 2022. Ini menunjukkan kenaikan sebesar 20.569 kasus. Analisis lebih lanjut untuk kuartal I 2023 menunjukkan bahwa bulan Februari menjadi puncak serangan *phishing* dengan 15.050 kasus dilaporkan. Sementara itu, Januari mencatat sekitar 7.665 kasus dan

[6] Ibid, 7-14.

Maret mengalami penurunan dengan 3.960 kasus, Peningkatan drastis ini menggambarkan semakin maraknya ancaman keamanan siber di Indonesia, khususnya dalam bentuk serangan *phishing*. Fenomena ini memerlukan perhatian serius dari berbagai pihak untuk meningkatkan kesadaran dan perlindungan terhadap ancaman siber.[7]

Dalam

Dalam syariat Islam, tidak terdapat aturan spesifik yang membahas kejahatan phishing. Hal ini disebabkan karena pada masa pembentukan hukum Islam, fenomena phishing belum dikenal. Namun demikian, para ahli hukum Islam menganalogikan phishing dengan konsep penipuan yang sudah ada dalam ajaran Islam, mengingat keduanya memiliki karakteristik yang serupa. Dalam perspektif Islam, penipuan atau tipu daya didefinisikan sebagai upaya seseorang untuk memperdaya pihak lain. Tindakan ini melibatkan penggunaan akal bulus atau strategi manipulatif, seringkali dengan menjanjikan sesuatu yang menggiurkan. Tujuan utamanya adalah memperoleh keuntungan dengan cara membuat korban menuruti keinginan pelaku. Dengan demikian, meskipun istilah phishing tidak secara eksplisit disebutkan dalam hukum Islam klasik, prinsip-prinsip yang mengatur tentang penipuan dapat diterapkan untuk menilai dan menangani kasus-kasus phishing dalam konteks hukum Islam kontemporer.

[7] https://bankjombang.co.id/serangan-phishing-di-indonesia-terus-meningkat-berikut-data-lengkapnya. Diakses 28 Agustus 2023

Orang yang memakan harta orang lain dengan cara yang bathil, seperti dilakukan dengan cara menipu, adalah sebuah perbuatan dosa, sebagaimana Allah SWT Berfirman dalam Q.S Al-Baqara/2 :188:

وَلَا تَأْكُلُوٓا اَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوْا بِهَآ اِلَى الْحُكَّامِ لِتَأْكُلُوْا فَرِيْقًا مِّنْ اَمْوَالِ النَّاسِ بِالْاِثْمِ وَاَنْتُمْ تَعْلَمُوْنَ ۝١٨٨

Terjemahnya :

"Janganlah kamu makan harta di antara kamu dengan jalan yang batil dan (janganlah) kamu membawa (urusan) harta itu kepada para hakim dengan maksud agar kamu dapat memakan sebagian harta orang lain itu dengan jalan dosa, padahal kamu mengetahui."[8]

Dalam Tafsir Syekh Nawawi Banten, ayat ini menegaskan larangan Allah kepada umat Islam untuk mengambil harta orang lain secara tidak sah. Larangan ini mencakup berbagai cara yang diharamkan dalam syariat Islam. Salah satu contohnya adalah menggunakan sistem peradilan dengan niat buruk, yaitu membawa perkara ke hadapan hakim dan bersumpah palsu untuk memenangkan klaim atas harta orang lain. Yang membuat perbuatan ini lebih tercela adalah pelakunya sadar bahwa tindakannya itu batil dan melanggar hukum agama.[9]

Senada Dengan pembahasan diatas Penipuan online atau *cyber crime* telah menjadi momok yang semakin meresahkan, tidak hanya bagi individu, tetapi juga bagi keluarga saya sendiri. Beberapa Tahun yang lalu, saya dan beberapa anggota keluarga mengalami kerugian besar akibat serangkaian penipuan online yang ternyata menggunakan teknik *phishing.* Modus ini begitu canggih dan terstruktur

[8] Kementerian Agama, Al-Quran QS. Al Baqarah/2:188

[9] Muhammad Nawawi Al-Jawi, *At-Tafsirul Munir li Ma'alimt Tanzil*, (Beirut, Darul Fikr), juz II Terjemahan, 44

sehingga tanpa sadar kami menjadi korban. *Phishing* adalah salah satu bentuk kejahatan dunia maya di mana pelaku menyamar sebagai pihak yang sah atau terpercaya, seperti perbankan, perusahaan besar, atau penyedia layanan digital. Dengan berbagai cara, mereka memancing korbannya untuk memberikan informasi sensitif, seperti nomor kartu kredit, *password*, atau data pribadi lainnya. Dalam kasus kami, para pelaku *phishing* menggunakan metode yang sangat meyakinkan melalui email dan situs palsu yang tampak resmi, mengarahkan kami untuk memasukkan data sensitif. Akibatnya, sejumlah besar uang dari rekening kami berhasil diambil tanpa sepengetahuan kami hingga kerugian itu menjadi nyata. Kejadian ini sangat menghancurkan, terutama karena kami merasakan dampak material yang signifikan. Berbulan-bulan lamanya kami berusaha pulih dari kerugian tersebut, tetapi trauma dan rasa ketidakpercayaan terhadap transaksi online tetap menghantui kami. Sebagai individu yang tidak hanya merasakan kerugian materi, tetapi juga kehilangan rasa aman dalam berinteraksi di dunia digital, kejadian ini membuka mata saya akan betapa lemahnya perlindungan sebagian masyarakat dari serangan siber seperti ini. Setelah kejadian tersebut, saya merasa terdorong untuk mendalami lebih jauh mengenai teknik *phishing* dan bagaimana aspek hukum bisa berperan dalam mencegah serta menindak pelakunya. Hal ini menjadi dasar pemikiran saya dalam memilih topik skripsi: "**Teknik Phishing dalam Perspektif Hukum Positif dan Hukum Pidana Islam**."

B. Rumusan Masalah

1. Rumusan Masalah

Bersarkan latar belakang diatas, maka masalah dalam penelitian ini dapat di rumuskan dalam beberapa bentuk bertanyaan sebagai berikut :

a. Bagaimanakah Tehnik dan Taktik yang digunakan Dalam serangan *Phishing* (Pencurian Data Pribadi) ?
b. Bagaimanakah pandangan hukum positif dan Hukum Pidana Islam Tentang *Phishing* (Pencurian Data Pribadi) ?

C. Tujuan dan Kegunaan Penelitian

Sesuai Rumusan masalah diatas, maka tujuan penelitian sebagai berikut:

1. Tujuan Penelitian
   a. Untuk mengetahui tinjauan hukum positif UU ITE dan UU PDP terhadap penanganan tindak pidana *Phishing* (pencurian data Pribadi)
   b. Untuk menganalisis kajian komparatif mengenai tindak pidana *phishing* (pencurian data pribadi) menurut hukum Islam dan hukum positif, untuk dicari persamaan dan perbedaan dalam tindak pidana tersebut
2. Kegunaan Penelitian

   Setiap penelitian diharapkan dapat memberikan manfaat yang baik untuk penulis sendiri maupun bagi masyarakat umum tentunya. Adapun manfaat yang diharapkan penulis dalam penelitian yakni :

a. Diharapkan hasil studi ini dapat memberikan kontribusi berarti bagi aparat penegak hukum dalam upaya mewujudkan keadilan. Lebih lanjut, penelitian ini bertujuan untuk menyediakan perspektif yang dapat dijadikan sebagai bahan pertimbangan oleh para hakim dalam proses pengambilan keputusan yang adil dan bijaksana. Dengan kata lain, kajian ini diharapkan dapat menjadi sumber referensi yang berharga dalam sistem peradilan, membantu meningkatkan kualitas penegakan hukum, serta mendukung terciptanya putusan-putusan pengadilan yang mencerminkan rasa keadilan yang tinggi di masyarakat.
b. Diharapkan bahwa penelitian ini akan meningkatkan pengetahuan umat muslim tentang ide-ide tentang hukum pidana islam dan hubungannya dengan perubahan hukum yang terjadi saat ini, khususnya tentang subjek penelitian terkait, yaitu kejahatan phishing dalam penelitian hukum pidana islam.

D. Penegasan istilah

1. *Phishing*

Bentuk serangan siber di mana penyerang mencoba untuk mendapatkan informasi sensitif, seperti nama pengguna, kata sandi, informasi kartu kredit, atau data pribadi lainnya, dengan menyamar sebagai entitas yang tepercaya atau lembaga yang sah. Penyerang menciptakan tampilan yang menipu dan meyakinkan, seringkali dalam bentuk email palsu, situs web palsu, atau pesan teks palsu, untuk memancing korban agar memberikan informasi pribadi atau data keuangan.

Dalam serangan phishing, penyerang berupaya memanipulasi kepercayaan korban dengan membuatnya yakin bahwa mereka berinteraksi dengan entitas yang sah. Teknik ini sering digunakan untuk meretas akun online, mencuri informasi finansial, atau bahkan mencuri identitas. Dengan cara ini, penyerang mencoba mendapatkan akses ilegal ke informasi penting atau mencuri dana korban[10].

2. Pencurian

Ditinjau dari aspek etimologis, istilah "pencurian" berasal dari kata dasar "curi" yang dilengkapi dengan awalan "pe-" dan akhiran "-an". Kata "curi" sendiri mengandung makna tindakan mengambil kepemilikan orang lain secara tidak sah atau tanpa izin, umumnya dilakukan secara diam-diam atau sembunyi-sembunyi.

Dalam terminologi hukum, pencurian didefinisikan sebagai tindakan mengambil harta milik pihak lain tanpa persetujuan atau secara ilegal, biasanya dilakukan dengan cara tersembunyi. Sementara itu, Kamus Besar Bahasa Indonesia (KBBI) memberikan definisi yang serupa untuk kata "curi", yaitu tindakan mengambil barang milik orang lain tanpa izin atau dengan cara yang tidak sah, umumnya dilakukan secara sembunyi-sembunyi.

Adapun "pencurian" diartikan sebagai proses, cara, atau perbuatan mencuri. Definisi-definisi ini menekankan unsur-unsur kunci dalam tindakan pencurian, yaitu pengambilan tanpa izin, ketidaksahan, dan upaya untuk menyembunyikan tindakan tersebut.

3. Fiqih jinayat

[10] Andi Abdul Muis, Indonesia di Era Dunia Maya Teknologi Informasi dalam Dunia Tanpa Batas, (Bandung:PT Remaja Rosdakarya Offset,2001), 3

Fiqih jinayah juga dikenal sebagai hukum pidana Islam. Dalam bahasa, "fiqih" berarti memahami maksud pembicara. Fiqih adalah ilmu yang didasarkan pada pemikiran dan ijtihad (penelitian), dan memerlukan pemikiran dan perenungan..[11]

4. Data Pribadi

Data pribadi mengacu pada informasi yang bisa dihubungkan dengan individu tertentu, baik secara langsung maupun tidak langsung, dan dapat digunakan untuk mengidentifikasi individu tersebut. Informasi ini meliputi berbagai jenis data yang berkaitan dengan kehidupan, identitas, dan karakteristik individu, termasuk namun tidak terbatas pada nama, alamat, nomor telepon, alamat email, tanggal lahir, nomor identifikasi pribadi (seperti KTP atau paspor), nomor kartu kredit, dan banyak informasi lain yang berkaitan dengan seseorang.[12]

E. Garis-Garis Besar Isi

Agar proposal ini mudah di pahami, maka penulis membagi penulisan menjadi lima bab, yaitu:

Pada Bab I Merupakan bab pendahuluan memuat latar belakang, Rumusan masalah, Tujuan dan Kegunaan Penelitian, dan Garis-garis Besar isi

Pada Bab II merupakan bab Kajian Pustaka memuat Penelitian Terdahulu, Kajian teori, dan Kerangka Pemikiran

---

[11] Djazuli, Ilmu Fiqih: Penggalian, Perkembangan, dan Penerapan Hukum Islam (Ponorogo: Pustaka Setia, 2010).

[12] KBBI. “Pengertian Data”. https://kbbi.web.id/data diakses pada 21 Agustus 2023

Pada Bab III merupakan Metode Penelitian memuat Pendekatan dan Desain Penelitian, Definisi Operasional, instrumen penelitian, Tehnik Pengumpulan Data, dan Tehnik Analisis Data

Pada Bab IV merupakan Hasil dan Pembahasan Penelitian yang memuat pandangan hukum Islam tentang tindakan *phishing* sebagai pelanggaran hukum, Analisis definisi dan ketentuan UU ITE terkait dengan tindakan *phishing*, Tinjauan tentang perlindungan data pribadi dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), Korelasi dan perbedaan Hukum perlindungan data pribadi dalam hukum Islam, hukum positif (UU ITE), dan UU PDP.

Pada Bab V Penutup Memuat simpulan yang berisi jawaban dari pokok permasalahan dan saran-saran. [13]

[13] Sulistyo Irianto dkk, *Metode Penelitian Hukum*, cet. Ke-1 (Jakarta: Obor, 2009),142

BAB II

KAJIAN PUSTAKA

A. Penelitian Terdahulu

Kajian pustaka yang akan dilakukan oleh penulisadalah dari berbagai karya ilmiah selain berbentuk buku yang berbentuk jurnal, dan skripsi-skripsi yang sudah ada. Berikut pemaparanya :

1. Abdurrobbi Rijaluddin Sabbala dengan judul penelitian "Perlindungan Hukum Bagi Korban Pencurian Data Pribadi di Internet dalam Sistem Hukum Pidana di Indonesia". Penelitian Abdurrobbi Rijaluddin Sabbala bertujuan mengkaji perlindungan hukum bagi korban pencurian data pribadi melalui internet dan implementasinya dalam sistem hukum pidana Indonesia. Hasil penelitiannya menunjukkan bahwa perlindungan hukum yang tersedia bagi korban kejahatan ini masih sangat terbatas. Saat ini belum ada regulasi khusus yang dirancang untuk melindungi korban pencurian data pribadi.Meskipun demikian, Sabbala berpendapat bahwa tindakan pelaku kejahatan pencurian data pribadi di internet dapat mempengaruhi bentuk perlindungan hukum yang akan diterima korban. Berdasarkan Undang-Undang Perlindungan Saksi dan Korban yang berlaku, korban pencurian data pribadi melalui internet hanya berhak mendapatkan satu bentuk perlindungan hukum, yaitu restitusi.

   Dari hasil penelitian diatas, persamaan yang di dapat yakni sama-sama meneliti mengenai pencurian data pribadi di internet, namun perbedaannya dalam penelitian yang akan diangkat penulis yakni fenomena *Phishing* dalam perspektif hukum pidana islam dan hukum positif

2. Penelitian yang dilakukan oleh Azhar Triadhi Sofyan (2021), berjudul "Tindak Pidana Kejahatan Siber Pasal 30 ayat 2 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Perspektif Hukum Pidana Islam". Penelitian ini bertujuan untuk mengetahui sanksi kejahatan siber, faktor penyebab kejahatan siber dan untuk mengetahui analisis hukum pidana Islam terhadap sanksi tindak pidana siber.

   Dari hasil penelitian diatas, membahas mengenai Undangan-undang No. 11 tahun 2008 tentang informasi dan transaksi elektronik pada pasal 30 ayat 2 dalam pandangan hukum pidana islam. Persamaannya sama-sama menggukan pasal 30 UU ITE sebagai alat analisis tulisan. Perbedaannya penelitian terdahulu ini hanya terkhusus pada pasal 30 ayat 2 UU ITE

3. Skripsi Rizki Arfah, dengan judul, "Sanksi Tindak Pidana *Hacking* (Studi Analisis Undang-Undang ITE dan Hukum Pidana Islam". Penelitian tersebut membahas mengenai kejahatan hacking yang diatur dalam UU ITE dan hukum pidana Islam, serta sanksi hacking menurut UU ITE dan hukum pidana Islam.[14]

   Dari hasil penelitian diatas, membahas tentang sanksi dari tindak pidana hacking pada analisis UU ITE dan hukum pidana islam, Persamaanya yakni sama-sama menggunakan UU ITE sebagai dasar hukum pada penelitian perbedaan nya penelitian terdahulu membahas sanksinya sedangkan penelitian ini membahas fenomena *phishing*

[14] Rizki Arfah, "Sanksi Tindak Pidana Hacking (Studi Analisis Undang-Undang ITE dan Hukum Pidana Islam," *Angewandte Chemie International Edition, 6(11), 951–952.* (UIN Sumatera Utara, 2018).

4. Skripsi Sulham Akbar Hidayat,[15] dengan judul, "Tinjauan Yuridis Pencurian Data Pribadi di Online Shop Menggunakan Malware (Studi Kasus Putusan Nomor 252/Pid.Sus/2020/PN.Smn". Penelitian tersebut membahas mengenai kualifikasi tindak pidana pencurian data pribadi di online shop menggunakan *malware* serta penerapan hukum pidana materiil terhadap kasus pencurian data pribadi di online shop menggunakan malware berdasarkan putusan nomor 252/Pid.Sus/2020/PN.Smn, sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

   Dari penelitian di atas, fokus penelitiannya tentang tinjauan yuridis pencurian data dari putusan pengadilan, sedangkan pada penelitian ini membahas tentang fenomena dari salah satu bentuk dari *cyber crime* yakni *Phishing* pada persamaannya yakni sama-sama kajiannya tentang kejahatan dalam internet atau *Cybercrime*

5. Artikel Jaenudin dan Rasyida Rofiatun Nisa, dengan judul, "*Islamicu Criminal LawuAnalysisoof Cyber Crimes on Consumen in E-CommerceiTransactions*". Penelitian tersebut membahas mengenai *cybercrime* yang, menurut analisis Hukum Pidana Islam, dapat dikategorikan sebagai *ta'zir* karena tindakan ini merusak nilai-nilai sosial dalam dunia teknologi informasi dan berdampak pada masyarakat baik di dalam maupun luar negeri.

   Dapat di perhatikan bahwa penelitian ini berbeda dengan Penelitian terdahulu di atas penelitian yang disusun oleh peneliti ini berfokus pada

[15] Sulham Akbar Hidayat, "TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI ONLINE SHOP MENGGUNAKAN MALWARE (Studi Kasus Putusan Nomor: 252/Pid.Sus/2020/PN. SMN)" (Universitas Hasanudin, 2021).

perbandingan hukum islam dan hukum positif mengenai fenomena Phishing agar dapat memberikan pemahaman yang lebih tentang perbedaan dan persamaan Phishing dalam kacamata hukum islam dan hukum positif persamaan yang dapat diperhatikan dalam penelitian ini yakni kajian nya sama-sama merupakan kejahatan siber atau *Cybercrime*

No	Penelitian Terdahulu	Persamaan	Perbedaannya
1	Abdurrobbi Rijaluddin Sabbala dengan judul penelitian "Perlindungan Hukum Bagi Korban Pencurian Data Pribadi di Internet dalam Sistem Hukum Pidana di Indonesia"	persamaan yang di dapat yakni sama-sama meneliti mengenai pencurian data pribadi di internet	dalam penelitian yang akan diangkat penulis yakni fenomena *Phishing* dalam perspektif hukum pidana islam dan hukum positif
2	Penelitian yang dilakukan oleh Azhar Triadhi Sofyan (2021), berjudul "Tindak Pidana Kejahatan Siber Pasal 30 ayat 2 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Perspektif Hukum Pidana Islam".	sama-sama menggukan pasal 30 UU ITE sebagai alat analisis tulisan	penelitian terdahulu ini hanya terkhusus pada pasal 30 ayat 2 UU ITE
3	Skripsi Rizki Arfah "Sanksi Tindak Pidana Hacking (Studi Analisis Undang-Undang ITE dan Hukum Pidana Islam".	sama-sama menggunakan UU ITE sebagai dasar hukum pada penelitian	penelitian terdahulu membahas sanksinya sedangkan penelitian ini membahas fenomena *phishing*
4	Skripsi Sulham Akbar Hidayat "Tinjauan Yuridis Pencurian	sama-sama kajiannya	membahas tentang

	Data Pribadi di Online Shop Menggunakan Malware (Studi Kasus Putusan Nomor 252/Pid.Sus/2020/PN.Smn"	tentang kejahatan dalam internet atau *Cybercrime*	fenomena dari salah satu bentuk dari *cyber crime* yakni *Phishing*
5	Artikel Jaenudin dan Rasyida Rofiatun Nisa, dengan judul, "*IslamicuCriminal LawuAnalysisoof Cyber Crimes on Consumen in E-CommerceiTransactions*".	persamaan yang dapat diperhatikan dalam penelitian ini yakni kajian nya sama-sama merupakan kejahatan siber atau *Cybercrime*	Pada penelitian ini berfokus pada perbandingan hukum islam dan hukum positif mengenai fenomena Phishing

B. Kajian Teori

a. Efektivitas Hukum

Setiap regulasi, baik yang memiliki hierarki tinggi maupun rendah, dirancang dengan tujuan menciptakan kepatuhan yang setara di antara masyarakat dan pejabat pemerintah. Prinsip ini didasarkan pada konsep kesetaraan di hadapan hukum, di mana setiap individu diperlakukan sama tanpa diskriminasi. Keberhasilan suatu peraturan perundang-undangan dapat diukur dari tingkat implementasinya. Kegagalan dalam penerapan hukum sering kali disebabkan oleh sikap apatis, baik dari masyarakat maupun dari aparatur negara. Dalam konteks ini, "efektif" merujuk pada kemampuan untuk menghasilkan dampak yang diinginkan. Sementara itu, efektivitas, sebagaimana didefinisikan oleh Mulyasa, mengacu pada kapasitas suatu

organisasi untuk memperoleh dan memanfaatkan sumber daya secara optimal dalam rangka mencapai tujuan yang telah ditetapkan.[16]

Hans Kelsen mendefinisikan efektivitas hukum sebagai kondisi di mana perilaku individu dalam masyarakat sejalan dengan norma-norma yang berlaku. Lebih lanjut, efektivitas hukum tercapai ketika aturan-aturan tersebut tidak hanya ada di atas kertas, tetapi benar-benar diterapkan dan dipatuhi dalam kehidupan sehari-hari. Interpretasi dari definisi ini menunjukkan bahwa suatu peraturan perundang-undangan dapat dianggap efektif ketika dua komponen utama masyarakat - yaitu warga negara dan aparatur pemerintah - menyelaraskan perilaku mereka dengan ketentuan hukum yang ada. Dengan kata lain, efektivitas hukum terwujud ketika ada keselarasan antara aturan tertulis dan implementasinya dalam praktik sosial.[17] Teori efektivitas hukum memiliki 3 kajian yang meliputi:

1. Keberhasilan Dalam Pelaksanaan Hukum

Efektivitas peraturan perundang-undangan dapat dinilai dari tingkat kepatuhan yang ditunjukkan oleh dua kelompok utama: masyarakat umum dan aparat penegak hukum. Ketika norma-norma hukum yang dirancang untuk melindungi dan mengatur kepentingan publik berhasil dipatuhi secara menyeluruh, baik oleh warga negara maupun oleh pejabat pemerintah, maka

[16] Mulyasa, *Management Berbasis Sekolah Konsep Strategi Dan Implementasi*, (Bandung: PT Remaja Rosdakarya, 2006), 82

[17] Jimly Asshiddiqie Dan Ali Safaat, *Teori Hans Kalsen Tentang Hukum*, (Jakarta: Sekjen MK RI,2006), 9

dapat dikatakan bahwa penerapan hukum tersebut telah mencapai tingkat keberhasilan dan efektivitas yang diharapkan.

2. Kegagalan Dalam Pelaksanaan

Bahwa peraturan perundang-undangan yang dibuat tidak menunjukkan keberhasilan pada implementasinya

3. Faktor Yang Berpengaruh

Dalam implementasi dan penegakan hukum, terdapat berbagai elemen yang berperan penting dalam menentukan tingkat efektivitasnya. Faktor-faktor yang berkontribusi pada keberhasilan penerapan hukum mencakup dua aspek utama: muatan atau isi dari hukum itu sendiri (substansi hukum) dan nilai-nilai serta sikap masyarakat terhadap hukum (kultur hukum). Di sisi lain, kegagalan dalam pelaksanaan hukum sering kali bersumber dari dua komponen kunci dalam sistem hukum: masyarakat sebagai subjek hukum dan aparat penegak hukum. Sikap dan perilaku kedua kelompok ini dapat menjadi penentu utama apakah suatu aturan hukum akan berjalan efektif atau mengalami hambatan dalam penerapannya.

b. Phishing

1. Pengertian *Phishing*

Phishing adalah salah satu bentuk kejahatan internet yang masuk dalam kategori pencurian identitas. Istilah *"phishing"* sebenarnya berasal dari kata "*fishing"* yang merujuk pada penggunaan umpan yang semakin canggih

dengan tujuan untuk mendapatkan informasi keuangan dan kata sandi dari target yang dituju.[18]

Senator Patrick Leahy dalam pidatonya saat memperkenalkan rancangan undang-undang *Anti-Phishing Act* pada tahun 2005 menjelaskan bahwa istilah *"phishing"* berasal dari olahraga *"fishing,"* yang merupakan analogi dari teknik melempar umpan pancing dalam olahraga memancing. Dalam konteks *phishing*, "umpan" yang digunakan adalah surel atau pesan elektronik yang dirancang sedemikian rupa sehingga meyakinkan korban untuk mengungkapkan informasi pribadi atau rahasia mereka. Tujuan utama dari teknik ini adalah untuk berhasil "memanen" informasi yang diinginkan dari korban.[19]

2. Ciri-ciri *Phishing*

Ancaman terhadap keamanan data pribadi semakin meningkat seiring dengan pesatnya perkembangan teknologi dan internet. Hal ini menuntut kita untuk lebih waspada terhadap berbagai taktik manipulatif yang digunakan dalam ancaman siber. Salah satu bentuk kejahatan siber yang perlu diwaspadai adalah *phishing*. Untuk melindungi diri dari *phishing*, penting bagi kita untuk mengenali ciri-ciri umum dari kejahatan ini. *Phishing* sering kali dilakukan melalui email, pesan teks, atau situs web palsu yang dirancang untuk mencuri informasi pribadi seperti kata sandi, nomor kartu kredit, dan

---

[18] Syahdeini, Sutan Remy. 2009. *Kejahatan & Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafita, . 63.

[19] Syahdeini, Sutan Remy. 2009. *Kejahatan & Tindak Pidana Komputer.* Jakarta: Pustaka Utama Grafita., . 65.

data sensitif lainnya. Dengan memahami tanda-tanda *phishing*, kita dapat mengambil langkah-langkah preventif untuk menghindari menjadi korban kejahatan siber tersebut. Beberapa ciri-ciri umum *phishing* meliputi pesan yang mengandung tautan mencurigakan, permintaan informasi pribadi secara mendadak, dan penggunaan bahasa yang mendesak atau menakut-nakuti. Mengedukasi diri sendiri dan orang lain tentang bahaya *phishing* serta cara mengenalinya dapat membantu meningkatkan keamanan data pribadi kita di dunia digital.. Berikut ciri -cirinya:

1. Email atau pesan yang tidak diinginkan
2. Alamat email atau URL yang tampak resmi
3. Ancaman atau tekanan mendesak
4. Permintaan informasi pribadi
5. Tautan ke situs web yang mencurigakan
6. Kesalahan tata bahasa atau ejaan yang mencolok
7. Tidak adanya informasi kontak yang jelas
8. Tawaran yang terlalu bagus untuk menjadi kenyataan, seperti penawaran yang terlalu menggiurkan untuk menarik perhatian Anda
9. Spoofing dan teknologi pemalsuan
10. Identitas pengirim yang disamarkan [20]

a. Landasan Hukum

Peraturan mengenai tindak pidana *cyber crime* termuat dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi

[20] Sabrina tabrani dan vivi safitri, "*Kejahatan Phishing ditinjau dari prespekktif hukum dan kejahatan siber*", vol 3 (2024). 4

Elektronik Pasal 30 Ayat (2) yang berbunyi: "*Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik*".

c. Fiqih Jinayah

1. Pengertian

Hukum pidana dalam Islam, atau yang dikenal sebagai Fiqih Jinayah, adalah bagian dari syariat Allah yang membawa manfaat bagi kehidupan manusia, baik di dunia maupun di akhirat. Syariat Islam, dalam konteks substansial, menegaskan bahwa setiap individu memiliki kewajiban mendasar untuk mematuhi ketentuan syariat. Konsep kewajiban mendasar syariah ini menempatkan Allah sebagai otoritas yang memiliki hak tertinggi, baik dalam hubungannya dengan diri sendiri maupun dengan orang lain. Setiap individu bertanggung jawab sebagai pelaksana, yang berkewajiban untuk mematuhi perintah Allah. Perintah Allah ini harus dilaksanakan untuk kebaikan pribadi serta kebaikan bersama. Dengan kata lain, mematuhi hukum-hukum Allah adalah langkah yang diambil untuk memastikan kesejahteraan dan kebaikan, baik bagi individu itu sendiri maupun bagi masyarakat lebih luas.[21]

Secara terminologi, fiqih mengacu pada ilmu yang membahas berbagai hukum syariat yang memiliki karakter praktis, dan hukum-hukum ini ditemukan melalui analisis mendalam terhadap dalil-dalil yang terperinci.

[21] Zainuddin Ali,*Hukum Pidana Islam* (Jakarta : Sinar Grafika, 2007), . 1.

Dengan kata lain, fiqih merupakan kajian ilmiah tentang hukum-hukum syariat yang dapat diterapkan dalam kehidupan sehari-hari. Ilmu ini merupakan hasil pemahaman dan interpretasi seorang mujtahid terhadap dalil-dalil yang rinci, termasuk yang terdapat dalam Al-Quran dan hadis.[22]

Jinayah adalah tindakan atau perbuatan yang dapat mengancam keselamatan fisik dan tubuh seseorang serta berpotensi menimbulkan kerugian pada diri dan harta benda. Oleh karena itu, tindakan semacam ini dianggap terlarang dalam Islam, dan pelakunya harus dikenai sanksi hukum. Sanksi tersebut diberikan untuk mencegah terulangnya perbuatan serupa dan menjaga ketertiban serta keamanan masyarakat.

2. Dalil-dalil Fiqih jinayat

Adapun dalil-dalil yang menjadi dasar hukum jinayah adalah firman allah swt. dalam QS. Al-Baqarah (2):178.

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ كُتِبَ عَلَيۡكُمُ ٱلۡقِصَاصُ فِي ٱلۡقَتۡلَىۖ ....

Terjemahnya :

"Hai orang-orang yang beriman, diwajibkan atad kamu qishaash berkenaan dengan orang-orang yang dibunuh"

Firman Allah swt. dalam QS. Al-Baqarah (2):179.

وَلَكُمۡ فِي ٱلۡقِصَاصِ حَيَوٰةٞ يَٰٓأُوْلِي ٱلۡأَلۡبَٰبِ لَعَلَّكُمۡ تَتَّقُونَ ١٧٩

Terjemahnya :

" Dan dalam qishosh itu ada (jaminan keberlangsungan) hidup bagimu, hai orang-orang yang berakal, supaya kamu bertakwa"

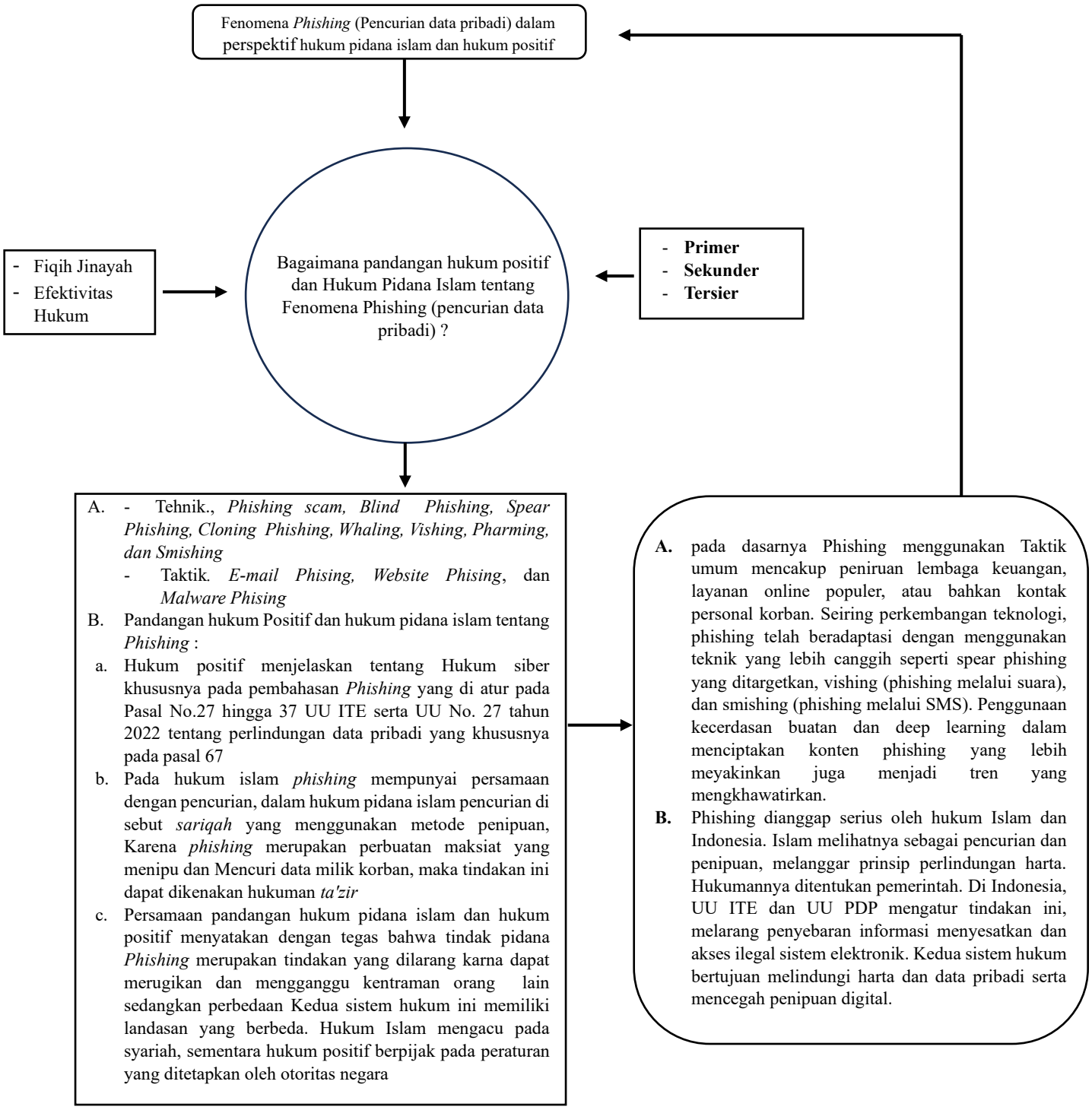
[22] Zainuddin Ali,*Hukum Pidana Islam* (Jakarta : Sinar Grafika, 2007), . 67

C. Kerangka Pemikiran

Kerangka pemikiran adalah dasar penelitian yang melibatkan penggabungan teori, observasi, fakta, dan kajian pustaka sebagai landasan dalam penulisan karya ilmiah. Kerangka berpikir penelitian memberikan arahan yang dapat dijadikan pedoman bagi para peneliti dalam melaksanakan penelitiannya, dimulai dari munculnya suatu fenomena.. [23]

Penelitian ini bertitik tolak dari adanya fenomena *phishing* atau pencurian data pribadi yang marak terjadi di internet dengan menipu si korban untuk mendapatkan data pribadi dari korban itu sendiri, fenomena ini memantik munculnya pertanyaan (*research question)* tentang mengapa hal tersebut bisa terjadi. Selanjutnya fenomena ini di telaah dengan menggunakan teori hukum islam dan hukum positif. Untuk menompang hasil penelitian ini menggunakan sumber data primer, sumber data sekunder dan sumber data tersier. Dari telaah teori dan sumber – sumber data, ditemukanlah hasil penelitian yang diakhiri dengan kesimpulan. Input, proses, dan output penelitian ini digambarkan dalam bagan sebagai berikut.

[23] Riduawan, *Metode dan taktik menyusun proposal penelitian*, ed. Zainal Arifin (cet. II ;Bandung: Alfabeta,CV, 2009) 33.



Bagan 1: Kerangka pemikiran Fenomena Phishing (pencurian data pribadi) menurut perespektif hukum pidana islam dan hukum positif

BAB III

METODE PENELITIAN

A. *Pendekatan dan desain penelitian*

Untuk mendapatkan data dan penjelasan terkait segala hal yang berkaitan dengan pokok permasalahan, diperlukan sebuah panduan penelitian yang disebut Pendekatan Penelitian.

1. Jenis penelitian

   Jenis penelitian yang dilakukan adalah Penelitian Penelitian hukum normatif, juga dikenal sebagai penelitian kepustakaan, adalah jenis penelitian yang berfokus pada studi dokumen dengan menggunakan berbagai data sekunder. Data sekunder ini mencakup peraturan perundang-undangan, keputusan pengadilan, teori hukum, dan pandangan para ahli. Dalam penelitian ini, analisis dilakukan secara kualitatif, yang berarti peneliti menjelaskan dan menginterpretasikan data dalam bentuk narasi atau kata-kata, bukan angka atau statistik.[24]

2. Sifat Penelitian

   Penelitian ini bersifat deskriptif komparatif, yang berarti objek penelitian disajikan dan dijelaskan secara sistematis. Penelitian ini mengidentifikasi dan menyajikan informasi tentang fenomena phishing (pencurian data pribadi)

[24] Bambang Sunggono, Metodologi Penelitian Hukum, cet. ke-1 (Jakarta: Raja Grapindo Persada, 2007),35-38.

dalam hukum Islam dan hukum positif. Penelitian komparatif melibatkan perbandingan dua subjek penelitian untuk memberikan perspektif baru dan menjelaskan komponen dari perspektif tersebut.[25] Dalam hal ini, penulis berusaha membandingkan fenomena *phishing* atau pencurian data pribadi dari perspektif hukum positif dan hukum Islam. Penulis akan melihat keabsahan data serta kekuatan hukum terkait fenomena *phishing* dalam kedua sistem hukum tersebut. Penelitian komparatif melibatkan perbandingan dua objek kajian untuk memberikan pandangan baru dan menjelaskan unsur-unsur dari pandangan tersebut. Dengan membandingkan kedua perspektif ini, penelitian ini bertujuan untuk mengungkap bagaimana masing-masing sistem hukum menangani dan merespons ancaman *phishing*, serta menyoroti perbedaan dan persamaan yang ada antara hukum positif dan hukum Islam dalam mengatasi kejahatan siber ini.

Penelitian terkait Fenomena *phishing* (pencurian data pribadi) ini menggunakan pendekatan penelitian sebagai berikut:

a. Penekatan Perundang-Undangan *(Statute Approach)*

Salah satu metode penelitian yang digunakan oleh penulis adalah pendekatan perundang-undangan. Dalam metode ini, penulis meninjau dan menganalisis peraturan perundang-undangan yang relevan dengan masalah hukum yang sedang dibahas. Pendekatan ini melibatkan pemeriksaan

[25] Anton Bakker dan Ahmad Zubeir, Metodologi Penelitian Filsafat (Yogyakarta:Kanisius, 1990), 85-87.

terhadap berbagai undang-undang, regulasi, dan kebijakan yang berlaku untuk memahami bagaimana hukum mengatur dan merespons isu-isu terkait, seperti fenomena *phishing* atau pencurian data pribadi. Dengan cara ini, penulis dapat memberikan wawasan yang mendalam tentang kerangka hukum yang ada serta mengevaluasi efektivitas dan kelemahan dari peraturan-peraturan tersebut dalam konteks kejahatan siber.[26]

b. Pendekatan Konseptual (*Conceptual Approach)*

Dengan menggunakan pendekatan konseptual, peneliti meneliti teori-teori yang berkembang dalam ilmu hukum untuk menemukan gagasan-gagasan yang membentuk pemahaman hukum, serta mengidentifikasi konsep-konsep dan asas-asas hukum yang relevan dengan masalah yang dibahas. Pendekatan ini melibatkan analisis mendalam terhadap literatur hukum, pemikiran para ahli, dan doktrin hukum untuk menggali dasar-dasar teoretis yang mendukung interpretasi dan penerapan hukum dalam konteks tertentu. Melalui pendekatan konseptual, peneliti dapat menghubungkan teori hukum dengan praktik hukum yang ada, serta mengembangkan wawasan yang lebih komprehensif tentang bagaimana prinsip-prinsip hukum dapat diterapkan untuk menangani isu-isu kontemporer, seperti *phishing* dan kejahatan siber lainnya. [27]Pendekatan ini digunakan untuk mencermati dan melakukan kajian konsep atau gagasan hukum tentang Fenomena *phishing* atau Pencurian data

[26] Peter Mahmud Marzuki, Penelitian Hukum, Penerbit Kencana, Jakarta, 2007, 96.

[27] Ibid,d 135.

pribadi, karena peraturan yang ada saat ini belum secara tegas memberi perlindungan kepada korban *phishing* yang terjadi di dunia maya.

c. Pendekatan Teologi

Penelitian agama sering kali menggunakan pendekatan teologis untuk menjawab pertanyaan-pertanyaan terkait kemungkinan penelitian dalam bidang agama. Menurut Noeng Muhadjir, ilmu dan wahyu memiliki otonomi masing-masing dalam bidangnya. Ketidakseimbangan dalam memandang keduanya dapat menyebabkan para ulama terjebak dalam filsafat yang abstrak, sementara ilmuwan bisa menjadi terlalu empiris dan kehilangan aspek sensasional dari agama.

Pendekatan teologis dalam penelitian agama beroperasi di dua kawasan: *naqli* (wahyu) dan *aqli* (produk budaya manusia). Tujuan pendekatan ini adalah menjembatani kesenjangan antara para ulama, yang ahli dalam ilmu agama, dengan ilmuwan dari bidang lain. Dengan metode ini, diharapkan dapat tercapai pemahaman yang lebih komprehensif dan integratif. Dalam konteks penelitian mengenai *phishing* atau pencurian data pribadi, metode teologis digunakan untuk mendapatkan pemahaman dari perspektif hukum Jinayah Islam. Pendekatan ini melibatkan analisis teks-teks wahyu serta pemikiran ulama untuk menilai bagaimana hukum Islam mengatur dan merespons kejahatan siber, serta bagaimana prinsip-prinsip hukum Jinayah dapat diterapkan dalam menghadapi tantangan keamanan data pribadi di era

digital.[28] Pendekatan ini digunakan untuk memahami fenomena *phishing* atau pencurian data pribadi dalam pandangan hukum *Jinayah* islam.

B. Data dan Sumber data

Penelitian hukum normatif bertujuan untuk memahami dan mengevaluasi hukum dari sudut pandang teoritis dan praktis. Dengan menggunakan metode ini, peneliti dapat mengidentifikasi dan menganalisis prinsip-prinsip hukum, serta bagaimana hukum diterapkan dalam berbagai kasus. Selain itu, penelitian ini juga memungkinkan peneliti untuk mengkritisi dan merekomendasikan perubahan atau perbaikan dalam sistem hukum yang ada. Dalam konteks yang lebih luas, penelitian hukum normatif berfungsi sebagai alat penting untuk memahami dinamika hukum dalam masyarakat, serta bagaimana hukum berinteraksi dengan aspek-aspek sosial, politik, dan ekonomi. Dengan demikian, penelitian ini tidak hanya memberikan wawasan tentang struktur hukum, tetapi juga tentang bagaimana hukum dapat digunakan untuk mencapai keadilan dan ketertiban dalam masyarakat.

Penelitian hukum normatif meliputi beberapa aspek kajian, yaitu:

1. Asas-asas hukum
2. Sistematika hukum
3. Sinkronisasi hukum
4. Perbandingan hukum
5. Sejarah hukum

[28] Jurnal Hunafa Vol. 3 No. 2, Juni 2006:129-140

Seperti halnya penelitian pada umumnya yang membutuhkan sumber data, penelitian hukum normatif juga bergantung pada sumber-sumber hukum tertentu. Sumber-sumber ini menjadi dasar analisis dan pembahasan dalam penelitian hukum normatif. seperti:

a) Sumber hukum primer adalah bahan-bahan hukum yang memiliki kekuatan mengikat dalam kaitannya dengan masalah yang sedang diteliti. Sumber-sumber ini mencakup Undang-Undang Dasar 1945, Undang-Undang, Peraturan Pemerintah, Pancasila, Yurisprudensi, Sumber hukum mengikat lainnya. Bahan-bahan hukum ini bersifat otoritatif dan menjadi acuan utama dalam penelitian hukum normatif. Mereka memberikan landasan hukum yang kuat dan relevan untuk analisis masalah yang sedang dikaji.
b) Sumber hukum sekunder adalah materi yang menjelaskan bahan hukum primer, seperti RUU, hasil penelitian, dan karya ilmiah dari para ahli.
c) Sumber hukum tersier adalah materi yang memberikan informasi mengenai hukum primer dan sekunder. Contohnya termasuk kamus hukum, ensiklopedia, majalah, media massa, dan internet. [29]

C. Tehnik Pengumpulan Data

Adapun Untuk mengumpulkan data untuk penelitian ini, metode yang digunakan adalah meninjau literatur. Sumber data primer termasuk Al-Quran dan As-Sunnah, Kitab-Kitab Fiqih Jinayah, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, dan KUHPidana. Sumber data

[29] https://idtesis.com/pengertian-penelitian-hukum-normatif-adalah/ diakses pada tanggal 21 Agustus 2023

sekunder termasuk kitab ushul fiqh, buku, dan artikel yang membahas fenomena *phishing* atau pencurian data pribadi. Selanjutnya, bahan data tersier adalah kamus yang dapat menjelaskan arti, maksud, dan istilah yang relevan.

D. Tehnik Analisis Data

Untuk menganalisis data yang dikumpulkan, digunakan analisis yuridis kualitatif dan penarikan kesimpulan dari data kepustakaan. Analisis yuridis digunakan karena data kepustakaan yang dikumpulkan dalam penelitian ini berfokus pada Peraturan Perundang-undangan sebagai hukum materiil. Analisis kualitatif digunakan karena tujuan analisis data yang dikumpulkan adalah untuk menemukan asas-asas hukum dari unsur-unsur yang ada dalam objek penelitian tanpa menggunakan analisis yuridis.

BAB IV

HASIL DAN PEMBAHASAN

A. Hasil Penelitian

a. Asal Mula Istilah *Phishing*

Istilah "*Phishing*" pertama kali digunakan dalam "*newsgroup Usenet alt.online-service.america-online"* pada 2 Januari 1996, meskipun mungkin telah muncul sebelumnya dalam edisi cetak majalah hacker 2600. Pada tahun 1987, teknik *phishing* diuraikan secara komprehensif dalam makalah dan presentasi yang diberikan kepada *Interex*, grup pengguna HP internasional. Istilah "*pheaking*" berasal dari kata "*pheaking*", yang berasal dari kata "*freaking*", di mana huruf "*f*" digantikan oleh "*ph*", dan merujuk pada penggunaan umpan yang lebih canggih yang bertujuan untuk mendapatkan *password* dan informasi keuangan dari pihak yang dituju.[30]

b. Pengertian *Phishing*

Phishing adalah metode penipuan yang dilakukan dengan cara menipu pelanggan menggunakan alamat situs palsu untuk mencuri data pribadi mereka. Biasanya, pelaku menyebarkan *phishing* melalui email korban, yang digunakan untuk mengarahkan korban ke situs web palsu guna menjebak mereka. Istilah "*phishing*" sendiri berasal dari kata Inggris "*fishing*," yang berarti "memancing."[31]

---

[30] Akbar Galih hariyono dan Frans Simangusong. " Perlindungan Hukum Korban Pencurian Data Pribadi (*Phishing Cybercrime*) dalam Perspektif Kiriminilogi" Jurnal Of Law and Social, Volume 3, nomor 1. (2023). 429

[31] Dian Rachmawati, 'Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber' (2014) 13 Jurnal SAINTIKOM. 21

Menurut Dendy Eka Puspawadi, seorang ahli informasi dan teknologi elektronik, *phishing* adalah tindakan penipuan yang bertujuan untuk mencuri akun target dengan cara mengelabui mereka. Ini biasanya dilakukan dengan menyebarkan pesan siaran, seringkali melalui email palsu yang berisi informasi menyesatkan, yang mengarahkan target ke halaman palsu untuk menjebak mereka, sehingga pelaku dapat memperoleh akses ke akun korban.[32]

Hewlett Packard (HP) Group *Interex*, sebuah perusahaan teknologi di Amerika Serikat, pertama kali menggunakan teknik *phishing* pada tahun 1987. Namun, pada tahun 1990-an, seorang *hacker* bernama Khan C. Smith menggunakan teknik *phishing* untuk mendapatkan data akun bank pengguna *American Online* (AOL), dengan tujuan mendapatkan *username* dan *password* dari pengguna akun tersebut. *Phishing*, juga disebut sebagai "*brand spoofing*" atau "*carding*", yang mana berarti jenis layanan yang menipu seseorang dengan mengatakan bahwa transfer data mereka aman dan sah.

Menurut Felten et al. (1997), *phishing* adalah metode yang digunakan oleh *hacker* untuk mendapatkan akses secara *ilegal* ke komputeryang menimbulkan ancaman. Adapun aspek ancaman dari sebuah *web* terkena *virus* yang di berikan oleh pelaku *Phishing* antara lain[33] :

---

[32] Ibid. 212

[33] Ibid. 213

1. Manipulasi Link, di mana pelaku *phishing* membuat link yang mirip dengan sumber asli tetapi menggunakan ejaan yang salah untuk memberi kesan bahwa itu adalah situs web asli.
2. *Website Forgery*, Teknik ini menggunakan celah keamanan pada sebuah website untuk memasang link pada file multimedia. Salah satu celah yang digunakan pelaku adalah *cross site scripting* (css), yang memungkinkan mereka membuat link yang tidak sah ke website yang sebenarnya.
3. *Filter Evasion*, mengalihkan perhatian pengguna melalui email yang mengandung tautan yang mengarah ke situs web yang sebenarnya, meskipun situs tersebut sebenarnya dibuat oleh pelaku phising, memaksa pengguna atau korban phising untuk memberikan informasi pribadi mereka.

c. **Tehnik dan Taktik *Phishing***

Beberapa penyebab utama kejahatan siber di Indonesia termasuk akses internet yang tidak terbatas, pengguna komputer yang lalai, tingkat keamanan yang rendah, dan kurangnya perhatian terhadap kejahatan siber itu sendiri.[34] Dengan kata lain, pendidikan masyarakat Indonesia sangat buruk, yang memungkinkan peretas dengan mudah masuk ke sistem komputer orang lain dan merusaknya.

Karena mereka menguasai sistem komputer dan mahir menemukan celah keamanan, pelaku kejahatan dalam dunia siber dianggap sangat pintar. Selain itu, pelaku kejahatan siber berasal dari latar belakang yang sangat

[34] Nudirman Munir, *Pengantar Hukum Siber Indonesia*, Rajawali Pers (2017). 10

beragam dan tidak terkategorikan; para hacker tidak terbatas pada usia dan memiliki status sosial yang sangat beragam, seperti pelajar, ibu rumah tangga, pejabat perusahaan, dan lain-lain. Namun terdapat beberapa karakter khusus umum yang selalu menjadi ciri khas para *hacker*, antara lain :[35]

1. Pemuja kesenangan, Hal ini dievaluasi berdasarkan kesenangan yang mereka peroleh saat berhasil membobol pertahanan atau keamanan sistem komputer yang telah dirancang sedemikian rupa. Hal ini dianggap sebagai sarana untuk menguji kemampuan dan mengasah otak mereka.
2. Manusia – manusia kreatif, Kebanyakan *hacker* tidak memiliki sumber daya yang memadai, sehingga mereka harus memikirkan ulang cara untuk mengatasi masalah sistem yang ada.
3. Tidak mudah bosan, Hal ini dinilai dari kecenderungan mereka untuk duduk berjam-jam di depan layar komputer untuk melakukan tugas yang sama berulang kali, yang cenderung membosankan. Biasanya, membutuhkan waktu 48 jam untuk mengamati lalu lintas data atau kegiatan dalam jaringan komputer.
4. Menginginkan kebebasan absolut, Para hacker adalah orang yang akan melakukan apa yang dilarang, jadi musuh utama mereka adalah birokrasi dan otoritas pemerintah yang selalu merahasiakan informasi dan

[35] Maskun, *Kejahatan Siber (Cyber Crime) : Suatu Pengantar*, Kencana (2013).50

menegaskan bahwa mereka tidak akan berhenti sampai mereka mendapatkan akses bebas ke sistem yang mereka inginkan.

Para peretas selalu mencari celah keamanan dalam sistem komputer, namun tidak semua peretas memiliki niat yang sama. *Phishing*, meskipun dianggap sebagai tindakan yang merugikan pengguna internet, tidak selalu dilakukan dengan niat buruk. Seperti dalam kasus Steven Haryanto, dia hanya ingin menguji tingkat keamanan internet *banking* bank BCA. Dengan kata lain, *phishing* dibagi menjadi beberapa kategori berdasarkan motivasi yang berbeda dari para pelaku.

Seperti yang telah dijelaskan sebelumnya, *phishing* dibagi ke dalam berbagai jenis berdasarkan motivasi pelaku dan target yang ingin dituju, yaitu :

1. *Spear Phishing*, di mana pelaku memiliki target yang jelas, dengan kata dasar *Spear*, yang berarti tombak, sehingga mereka memiliki peluang yang lebih besar untuk berhasil.
2. *Whaling,* adalah teknik *Phishing* ini yang menargetkan individu berpengaruh dalam suatu organisasi. Metode ini menyasar eksekutif tingkat tinggi atau pejabat senior. Para penipu biasanya menggunakan taktik intimidasi, seperti mengirimkan surat panggilan pengadilan palsu, untuk menekan korban agar memberikan informasi sensitif atau melakukan tindakan tertentu.

3. *Clone Phishing*, *Phishing* tradisional melibatkan penggunaan email palsu untuk mengirimkan pesan yang mirip dengan isi email asli kepada korban, hanya dengan mengubah file lampiran isi dalam email.
4. *Blind Phishing ,*Ini adalah jenis *phishing* yang paling umum. Serangan ini menggunakan metode tunggal, yaitu email atau pesan massal. Karena pesan dikirim ke banyak orang sekaligus, ciri khas utama dari penipuan jenis ini adalah tidak menyebutkan nama penerima secara spesifik.
5. *Phishing scam,* Pelaku kejahatan *cyber* berusaha memperdaya Anda dengan meminta informasi pribadi seperti kata sandi, nomor rekening bank, dan nomor kartu kredit. Mereka seringkali mengirimkan pesan atau email dengan lampiran atau tautan yang berbahaya, yang bisa menyebabkan pencurian data. Dengan informasi yang mereka dapatkan, mereka bisa masuk ke akun Anda, mengambil uang, atau bahkan melakukan transaksi tanpa izin Anda. Penipuan semacam ini bisa datang melalui telepon, email, pesan teks, atau media sosial. Oleh karena itu, pastikan Anda selalu waspada terhadap pesan atau panggilan yang mencurigakan dan jangan pernah memberikan informasi pribadi kepada orang yang tidak dikenal atau tidak dipercayai
6. *Covert Redirect,* merupakan metode yang sangat rumit di mana pelaku merubah *link* yang tampaknya resmi tetapi sebenarnya menuju *pop-up* login yang dibuat oleh pelaku. Teknik ini membuat target lebih sulit dikenali karena pelaku menggunakan kedua *link* dan situs resmi dengan

pop-up yang telah dimodifikasi, sehingga sulit untuk mengidentifikasi apakah *pop-up* tersebut benar-benar form login asli.[36]

7. *Vishing,* singkatan dari "*voice phishing*", adalah taktik penipuan yang menggunakan komunikasi suara. Para penipu menelepon korban potensial, sering kali menyamar sebagai anggota keluarga atau kenalan. Mereka biasanya menciptakan skenario darurat atau menggiurkan, seperti kecelakaan palsu atau kemenangan undian fiktif. Tujuan akhirnya adalah membujuk korban untuk mengirimkan uang. Untuk menyembunyikan identitas mereka, para pelaku *vishing* sering menggunakan teknologi seperti nomor telepon palsu atau sistem VoIP (*Voice over Internet Protocol*) yang sulit dilacak. Teknik ini membuat penipuan lebih meyakinkan dan sulit dideteksi oleh korban.
8. *Pharming,* adalah teknik serangan siber yang memanipulasi navigasi online pengguna. Berbeda dengan *phishing* yang mengandalkan penipuan langsung, *pharming* bekerja dengan mengalihkan pengguna secara diam-diam dari situs web yang sah ke situs tiruan yang tampak identik. Proses ini biasanya dimulai dengan penyebaran *malware (malicious software)* melalui email. Setelah terinstal di perangkat korban, *malware* ini memodifikasi pengaturan sistem untuk mengubah rute lalu lintas internet. Akibatnya, ketika pengguna mencoba mengakses situs web tertentu, mereka tanpa sadar diarahkan ke versi palsu yang dikontrol oleh penyerang. Tujuan utama pharming adalah pengumpulan data sensitif

[36] Sabrina tabrani dan vivi safitri, "Kejahatan Phishing ditinjau dari prespekktif hukum dan kejahatan siber", vol 3 (2024). 30

seperti kredensial login, informasi keuangan, atau data pribadi lainnya. Karena sifatnya yang tersembunyi, pharming dapat sangat berbahaya dan sulit dideteksi oleh pengguna biasa.

9. *Smishing, Phishing*, gabungan dari "SMS" dan "*phishing*", adalah bentuk penipuan digital yang memanfaatkan pesan teks atau SMS. Metode ini sangat populer di Indonesia dan negara-negara dengan tingkat penggunaan ponsel yang tinggi. Para penipu mengirimkan pesan SMS yang tampak meyakinkan, sering kali dengan tawaran yang menggiurkan. Pesan-pesan ini biasanya berisi janji palsu tentang kemenangan lotere, hadiah undian, atau kesempatan mendapatkan uang dalam jumlah besar. Tujuannya adalah memancing korban untuk melakukan tindakan tertentu, biasanya berupa transfer uang atau pemberian informasi pribadi. Efektivitas *smishing* terletak pada sifat langsung dan personal dari SMS, serta kecenderungan orang untuk lebih mempercayai pesan yang diterima di ponsel mereka. Penipuan ini memanfaatkan harapan akan keuntungan cepat dan mudah, yang membuat banyak orang lengah terhadap tanda-tanda penipuan.[37]

Salah satu cara untuk menentukan apakah seseorang telah melakukan *phishing* adalah dengan menentukan motif pelaku. Selain motif pelaku, tentu adanya sarana atau media juga penting apabila seseorang melakukan *phishing*. Dari definisi *phishing* yang telah dijelaskan sebelumnya, *phishing*

[37] https://www.hostinger.co.id/tutorial/ Phishing-adalah#1_Scam_ Phishing di akses 23 juni 2024

membutuhkan sarana seperti komputer dan internet, serta bahwa para pelaku *phishing* juga kadang-kadang membutuhkan dana untuk melakukan *phishing* mereka. Adapun cara kerja *phishing* dibedakan dalam berbagai bentuk:[38]

1. *E-mail Phising,* adalah taktik penipuan siber yang umum digunakan. Dalam skenario ini, penipu memulai serangan dengan mengirimkan email yang tampak resmi. Email ini dirancang untuk menyerupai komunikasi dari organisasi yang dikenal dan dipercaya oleh penerima, seperti bank, perusahaan, atau institusi pemerintah. Isi email biasanya mencakup permintaan yang tampak mendesak atau penting untuk memperbarui informasi pribadi. Untuk memfasilitasi ini, penipu menyertakan tautan URL di dalam email. Tautan ini dirancang untuk terlihat sah, tetapi sebenarnya mengarah ke situs web palsu yang dikontrol oleh penipu.
2. *Website Phising,* Pelaku *phishing* membuat domain yang terlihat seperti situs web asli perusahaan atau organisasi. Tujuannya adalah untuk mengelabui korban dengan meminta informasi pribadi seperti *password* dan rekening bank mereka.
3. *Malware Phising, Malware* adalah program komputer yang dibuat untuk menginfeksi sistem komputer tanpa diketahui pengguna. Pelaku *phishing* mengirimkan file kepada korban agar mereka mengunduh file yang berisi

[38] Cyber Crime",JOEICT (jurnal Of Education And Information Communication Technology).[urnal Of Education And Information Communication Technology),(2017). 3

virus, sehingga mereka dapat dengan mudah mengakses sistem komputer korban.

Beberapa modus yang digunakan oleh para pelaku *Phishing* adalah dengan menjebak sehingga korban secara tidak sadar memberikan data pribadinya, Para pelaku *Phishing* ini selalu menggunakan tipu muslihat dan rangkaian kebohongan, adapun ciri-ciri dari tipu muslihat yang terjadi pada *E-mail phishing* dalam rangka untuk menjebak korbannya yakni dengan memainkan kata-kata dalam *Subject* dan juga *Content E-mail* tersebut sehingga korban tertipu bahwa email tersebut adalah email yang asli, Sebagai contoh, mereka meminta verifikasi akun dan kemudian mengancam bahwa akun akan ditutup jika mereka tidak menjawab dalam jangka waktu tertentu. Yang ketiga menggunakan kata-kata sopan seperti "*Dear Valued Costumer*" karena kebanyakan pelaku *phishing* memiliki target yang acak dan bahkan mungkin menggunakan nama korban secara langsung, dan contoh terakhir, di mana korban diminta untuk mengklik tautan untuk mengakses akun korban.[39]

Dalam *phishing web*, istilah "*forgery web*" digunakan untuk menggambarkan bahwa situs web tersebut dibuat dengan tujuan hanya untuk menipu penggunanya. Untuk melakukan *phishing* ini, pelaku memilih untuk membangun domain di internet untuk menjadi hostnya, yang disebut sebagai *web hosting*. Selama proses pembuatan domain, pelaku dapat

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

memilih untuk menggunakan domain yang berbayar atau gratis. Setelah mendapatkan domain yang diinginkan, pelaku akan mulai membangun *website*nya sendiri. Tampilannya akan sebisa mungkin mirip dengan *website* asli, mulai dari penataan *layout*, logo perusahaan, pewarnaan, dan elemen yang disertakan, hingga detail terkecil, sehingga korban akan tertipu dan memberikan data pribadi seperti *password* dan *username* ke dalam formulir, yang secara otomatis akan disimpan dalam *database* web.[40]

Suatu tindakan dapat disebut sebagai tindak pidana apabila tindakan tersebut dilakukan dalam bentuk delik atau tindak pidana, dan bagi pelanggarnya dapat di jatuhi hukuman yang berlaku. Contoh delik dalam KUHP yang dapat dijatuhkan sanksi terhadap pelaku *Phishing*, contohnya kasus penipuan yang teratur dalam KUHP pasal 378, Karena *phishing* pada dasarnya merupakan jenis penipuan online di mana pelaku menggunakan *e-mail* atau *website* palsu untuk mengirimkan konten berisi kebohongan atau tipu muslihat yang bertujuan untuk mengecoh korban untuk memberikan data pribadi mereka, ketentuan dalam Pasal ini dapat diterapkan pada mereka yang melakukan *phishing*.[41]

B. PEMBAHASAN

a. *Phishing* dalam hukum positif

[40] Ki Jagad Tomara, "Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs Phising", (2011). 56

[41] Ibid. 59

Perundang-undangan yang mengatur hukum siber di Indonesia dianggap "seumur jagung", yang membuatnya menjadi tantangan tersendiri dalam praktiknya. Kedudukan hukum siber berdampak pada perubahan masyarakat, seperti peningkatan kecanggihan teknologi komputer yang telah membuat kehidupan sehari-hari lebih mudah bagi orang-orang, terutama di bidang pekerjaan. Namun, penggunaan teknologi komputer sebagai sarana untuk melakukan kejahatan telah menimbulkan masalah yang cukup rumit, terutama dalam hal proses pembuktian pidana karena kejahatan yang dilakukan.[42]

Klasifikasi kejahatan pada Pasal 27 hingga 37 UU ITE menetapkan kategori kejahatan siber. Misalnya, Pasal 27 mengatur tentang pelanggaran perjudian, pencemaran nama baik, kesusilaan, serta pengancaman dan pemerasan . Unsur-unsur dalam Pasal 27 mencakup pengembangan modus kejahatan seperti yang diatur dalam KUHP, tetapi dalam UU ITE, modus kejahatan tersebut dilakukan menggunakan perangkat komputer.

Dalam merumuskan tindak pidana *phishing*, beberapa pasal dalam KUHP yang dijadikan acuan adalah Pasal 378, Pasal 263, dan Pasal 362. Pasal 378 KUHP mengatur tentang penipuan, yang menyatakan bahwa siapa pun yang secara melawan hukum menggunakan nama atau identitas palsu untuk menguntungkan diri sendiri atau orang lain dengan tipu muslihat atau rangkaian kebohongan dengan tujuan menggerakkan orang tersebut untuk menyerahkan atau memberikan sesuatu, diancam dengan pidana penjara

[42] Ayu Putriyanti, "*Yurisdiksi di Internet/Cyberspace*",9 Media Hukum (2009).15

maksimal empat tahun. Oleh karena itu, pembahasan berikutnya akan menganalisis unsur-unsur dalam Pasal 378 KUHP yang menjadi salah satu acuan dalam menjatuhkan pidana untuk kasus *phishing*.[43]

Pertama, unsur "barangsiapa" mengacu pada subjek hukum, yang dapat berupa individu atau badan hukum yang dianggap bertanggung jawab menurut hukum atas tindakannya, Unsur kedua adalah menguntungkan diri sendiri. Dalam konteks tindak pidana *phishing*, dapat disimpulkan bahwa sebagian besar pelaku *phishing* menggunakan kemampuan mereka untuk meraih keuntungan dari orang lain, meskipun sering kali bukan dalam bentuk uang atau barang.

Unsur menggunakan nama atau identitas palsu dengan tipu muslihat atau rangkaian kebohongan sering ditemukan pada pelaku tindak pidana *phishing*. Pelaku *phishing* biasanya menggunakan nama atau identitas palsu untuk menipu korbannya. Seperti yang telah dijelaskan, pelaku *phishing* bertujuan untuk memancing korban, dengan cara menggunakan nama atau identitas organisasi atau perusahaan besar. Isi email atau situs web palsu tersebut juga dirancang agar menyerupai aslinya, dengan tujuan agar korban mudah percaya akan keaslian email atau situs web palsu tersebut.

Unsur terakhir adalah menggerakkan orang lain untuk menyerahkan sesuatu. Meskipun dalam konteks *phishing* yang menjadi sasaran bukan barang, melainkan data pribadi korban, hal ini tetap dianggap memenuhi

[43] Ibid. 18

unsur Pasal 378 KUHP. Pada dasarnya, data pribadi juga merupakan benda tak berwujud yang dapat dibuktikan keberadaannya. [44]

Adapun pasal 263 KUHP mengatur tentang pemalsuan surat. Seperti yang telah dijelaskan sebelumnya, *phishing* adalah tindakan penipuan di mana pelaku membuat *email* atau situs web palsu yang terlihat asli. Karena belum ada pengaturan khusus mengenai *phishing*, Pasal 263 mengalami perluasan makna, karena email juga dianggap sebagai surat dalam bentuk elektronik. Unsur-unsur dalam pasal tersebut juga sesuai dengan definisi *phishing* yang telah dijelaskan sebelumnya.

Pasal 362 KUHP tentang pencurian juga menjadi salah satu acuan bagi penuntut umum dalam mendakwakan pelaku tindak pidana *phishing*. Tindak pidana *phishing* merupakan rangkaian perbuatan yang bertujuan mengambil sesuatu milik korban secara melawan hukum untuk dimiliki. Pelaku *phishing* umumnya bertujuan mencuri data pribadi milik korban untuk kepentingan pribadi mereka. [45]

Dalam KUHP, pengaturan hukum terkait siber masih dibahas secara umum. Di Indonesia, dikenal asas *Lex Specialis derogat legi Generalis,* yang berarti bahwa undang-undang khusus mengesampingkan undang-undang umum. Dengan demikian, ada undang-undang yang lebih spesifik mengatur hukum siber, yaitu Undang-Undang Informasi dan Transaksi

[44] vikran Fassyadhiyaksa putra, "Modus Operandi tindakan pidana Phishing Menurut UU ITE" Jurist-Diction Vol. 4 (2021). 25

[45] Ibid. 26

Elektronik (UU ITE). UU ITE mengatur berbagai perbuatan yang dilarang terkait penggunaan teknologi informasi dan dijadikan acuan dalam merumuskan tindak pidana *phishing* di Indonesia. Meskipun tidak mengatur *phishing* secara rinci, pasal-pasal dalam UU ITE digunakan oleh penegak hukum dalam menyusun dakwaan. [46]

UU ITE memberikan pengaturan yang lebih rinci mengenai perbuatan yang dilarang dalam penggunaan teknologi informasi. Beberapa pasal dalam UU ITE yang dapat diterapkan pada pelaku tindak pidana *phishing*, sesuai dengan pengertian *phishing* yang telah dijelaskan sebelumnya, antara lain adalah Pasal 28 ayat (1), Pasal 45A ayat (1), Pasal 30 ayat (2), Pasal 46 ayat (2), Pasal 35, dan Pasal 51 ayat (1).

Perbuatan pelaku *phishing* tidak hanya sebatas memanipulasi website atau email untuk menipu korban, tetapi juga melibatkan kebohongan yang bertujuan untuk menyesatkan korban dan mengakibatkan kerugian. Pasal 28 ayat (1) UU ITE melarang tindakan yang dapat menyesatkan orang lain dan mengakibatkan kerugian dalam transaksi elektronik. Kerugian ini timbul karena pelaku memperoleh dan menyalahgunakan informasi pribadi korban. Berbeda dengan penipuan yang diatur dalam KUHP, tindak pidana *phishing* secara khusus mencakup perbuatan menyesatkan dalam transaksi elektronik. Dengan demikian, Pasal 28 ayat (1) UU ITE tidak berlaku untuk transaksi yang bersifat konvensional.[47]

---

[46] Ibid. 27

[47] Ardi Saputra Gulo, "Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang

Sedangkan Pasal 30 ayat (2) UU ITE secara khusus membahas tindakan mengakses sistem elektronik secara ilegal untuk memperoleh informasi atau dokumen elektronik, yang merupakan esensi dari *phishing*. Pasal ini juga mencakup tindakan penyebaran informasi yang diperoleh secara tidak sah kepada pihak yang tidak berwenang. Dalam konteks *phishing*, pelaku sering menggunakan dokumen palsu untuk memancing informasi sensitif dari korban. Sanksi untuk pelanggaran ini diatur dalam Pasal 46 ayat (2) UU ITE. Bila dibandingkan dengan tindak pidana pencurian dalam KUHP, *phishing* memiliki perbedaan signifikan dalam hal objek yang dicuri. *Phishing* berfokus pada pencurian data digital dan informasi elektronik, bukan barang fisik. Oleh karena itu, *phishing* dapat dianggap sebagai bentuk khusus dari pencurian yang disesuaikan dengan era digital, memerlukan pendekatan hukum yang lebih spesifik dibandingkan dengan pencurian konvensional..[48]

Selanjutnya dalam upaya menindak pelaku *phishing*, aparat penegak hukum sering mengandalkan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pasal ini menjadi dasar hukum utama untuk menjatuhkan sanksi yang sesuai terhadap para pelaku kejahatan siber jenis ini. Penggunaannya yang luas dalam berbagai kasus *phishing* menunjukkan relevansi dan efektivitas pasal ini dalam menghadapi bentuk penipuan

Informasi dan Transaksi Elektronik" PAMPAS: Journal of Criminal Vol.1 (2020). 75

[48] Ibid. 76

digital yang semakin canggih. Pasal ini terdapat beberapa unsur sebagaimana 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 informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik

Pasal 51 ayat (1) UU ITE juga akan mengenakan sanksi pidana terhadap individu yang melanggar ketentuan dalam pasal tersebut, Pelaku *phishing* tidak akan lepas dari identitasnya dan akan melakukan manipulasi seperti yang disebutkan di atas. Pertama, mereka akan membuat situs web palsu atau e-mail palsu untuk mengecoh korbannya, dan tujuan mereka adalah untuk membuat korban percaya bahwa situs web atau e-mail palsu adalah data sebenarnya.

Selain diatur dalam UU ITE, *phishing* juga diatur oleh Undang-Undang Perlindungan Data Pribadi. Perlindungan data pribadi sangat penting di era digital saat ini. Pemerintah memiliki peran utama dalam menjaga data pribadi melalui Undang-Undang Perlindungan Data Pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah peraturan baru yang mengatur perlindungan dan pemrosesan data pribadi di Indonesia. Ini merupakan langkah krusial untuk memastikan

privasi dan hak-hak individu terkait pengumpulan, penggunaan, dan pembagian data pribadi.

Pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memainkan peran penting dalam menanggulangi *phishing* di Indonesia. UU PDP memberikan perlindungan terhadap data pribadi individu dan menetapkan sanksi tegas bagi pelaku kejahatan siber, termasuk *phishing*. Pemerintah bertanggung jawab untuk memastikan bahwa peraturan dalam UU PDP diterapkan dan dipatuhi dengan baik guna melindungi data pribadi masyarakat. [49]

Pada Pasal 58 UU PDP menyatakan bahwa lembaga yang bertanggung jawab atas pelaksanaan UU PDP adalah Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) yang dibentuk oleh pemerintah. Lembaga ini bertugas untuk mengawasi dan memastikan pelaksanaan UU PDP berjalan dengan baik dan juga lembaga ini ditetapkan oleh Presiden dan diatur lebih lanjut melalui Peraturan Presiden.[50] Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) mempunyai tugas serta wewenang yang begitu penting dalam melindungi data pribadi seseorang. Berikut merupakan tugas dan wewenang dari LOPDP berdasarkan UUPDP :

1. Tugas LOPDP :

[49] Evelyn Angelita Pinondang Manurung, dan Emmy Febriani Thalib. "Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022." Jurnal Hukum Saraswati (JHS), Volume 4, Nomor 2, (2022). 15

[50] Ananta Fadli Sutarli dan Shelly Kurniawan. “Peran Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi *Phishing* di Indonesia” Jurnal Of Social Science Research, Volume 3, Nomor 2, (2023). 6

a) Mengembangkan kebijakan yang berkaitan dengan perlindungan data pribadi untuk memastikan keamanan dan kerahasiaan data individu secara efektif. Tugas ini mencakup merancang dan menyusun kebijakan yang tidak hanya memenuhi standar hukum yang berlaku, tetapi juga menyesuaikan diri dengan perkembangan teknologi terbaru serta dinamika bisnis yang terus berubah. Ini termasuk mengidentifikasi risiko baru yang muncul seiring dengan kemajuan teknologi dan memastikan bahwa kebijakan yang diterapkan dapat mengatasi tantangan tersebut secara proaktif.

b) Memberikan sanksi administratif kepada pihak-pihak yang melanggar ketentuan perlindungan data pribadi. Langkah ini bertujuan untuk menimbulkan efek jera dan mendorong kepatuhan terhadap peraturan yang berlaku.

c) Berkolaborasi dengan aparat penegak hukum untuk menangani kasus pidana yang melibatkan data pribadi. Mereka memberikan bantuan dan dukungan yang diperlukan selama proses penyelidikan dan penuntutan terhadap pelanggaran data pribadi.

d) Bertanggung jawab untuk mengevaluasi kepatuhan terhadap persyaratan terkait transfer data pribadi ke luar wilayah hukum Indonesia. Mereka memastikan bahwa transfer data dilakukan dengan memperhatikan tingkat perlindungan yang memadai.

2. Wewenang LOPDP :

a) Menginspeksi organisasi dan perusahaan yang diduga melanggar peraturan perlindungan data pribadi, serta menetapkan sanksi administratif dan denda yang sesuai.

b) Memberikan perintah untuk menghentikan penggunaan atau pengolahan data pribadi oleh individu, kelompok, atau perusahaan yang tidak sah atau tidak diizinkan.

Dalam melaksanakan tugas dan wewenangnya, Lembaga Otoritas Perlindungan Data Pribadi harus menjaga independensi, memiliki keahlian yang memadai, dan beroperasi dengan transparansi. Lembaga ini perlu memastikan bahwa fungsi dan kewenangannya tidak tumpang tindih dengan lembaga pemerintah lainnya di Indonesia, serta menjalin kerja sama yang efektif dengan lembaga-lembaga pemerintah lainnya.[51]

Berdasarkan Pasal 67 UU PDP, pelaku kejahatan siber yang melanggar undang-undang perlindungan data pribadi, termasuk *phishing*, dapat dikenakan sanksi administratif dan pidana. Sanksi administratif dapat termasuk teguran, peringatan, denda administratif, pencabutan izin usaha, dan/atau pembekuan kegiatan usaha. *Phishing* adalah jenis pencurian *online* yang dilakukan dengan metode penipuan yang mana memalsukan identitas atau data pribadi seseorang untuk memperoleh keuntungan atau data pribadi korban. Tindakan *phishing* ini dapat dianggap melanggar Pasal 67 Undang-Undang Perlindungan Data Pribadi Tahun 2022 dapat dikenakan hukuman

[51] Ibid. 7

penjara hingga 5 tahun dan/atau denda maksimal jika melibatkan pengumpulan atau penerimaan data pribadi korban secara ilegal. [52]

b. *Phishing* Dalam Hukum Pidana Islam

Hukum pidana Islam, yang dikenal sebagai fiqh jinayah, merupakan bagian integral dari syariat Allah. Sistem hukum ini dirancang untuk memberikan manfaat bagi umat manusia, tidak hanya dalam kehidupan duniawi tetapi juga untuk kehidupan akhirat. Dalam perspektif Islam, syariat ini bukan sekadar aturan hukum, melainkan kewajiban mendasar yang harus dipatuhi oleh setiap Muslim. Konsep ini menempatkan Allah sebagai sumber utama dari segala hak, baik yang berkaitan dengan individu maupun masyarakat. Setiap Muslim dianggap sebagai pelaksana yang bertanggung jawab untuk mematuhi dan menjalankan perintah Allah. Kepatuhan terhadap hukum syariah ini dipandang sebagai kewajiban yang membawa kebaikan, tidak hanya bagi diri sendiri tetapi juga bagi masyarakat luas..[53]

Dalam konteks hukum Islam, tindak pidana diartikan sebagai perilaku yang bertentangan dengan syariat, yang dapat dikenai hukuman *hudud* atau *ta'zir* sesuai ketentuan Allah SWT. Cakupan pelanggaran syariat ini luas, meliputi baik tindakan yang dilarang maupun kelalaian dalam melaksanakan kewajiban yang diperintahkan. Istilah "*syara*" dalam konteks

[52] Ibid. 19

[53] Sofyan Maulana, *Hukum Pidana Islam dan Pelaksanaan*, (Jakarta, Rineka Cipta, 2004). 83

ini memiliki makna penting. Ia mengindikasikan bahwa suatu perbuatan baru dapat dikategorikan sebagai tindak pidana jika secara eksplisit dilarang oleh syariat Islam. Dengan kata lain, definisi tindak pidana dalam hukum Islam sangat terikat pada apa yang ditetapkan oleh syariat.

Tindak pidana *Phishing* memiliki banyak kesamaan dengan konsep pencurian dalam islam, dengan menggunakan metode penipuan atau tipu muslihat untuk memperdaya korbannya, dengan liciknya menggiring korbannya untuk masuk ke website atau mengelik aplikasi yang dibuat oleh *Phisher* (pelaku *Phishing*) sehingga si korban terperdaya mengikuti kemauannya, dengan demikian *Phisher* (pelaku *Phishing*) bisa menjalankan rencananya dengan mengambil data pribadi korbannya. Pencurian dengan menggunakan metode penipuan ini merupakan sebuah perbuatan dosa yang merugikan orang lain.

Dalam Hukum islam pencurian disebut dengan *Sariqah*, pencurian (*Sariqah*) adalah mengambil harta milik seseorang dengan sembunyi – sembunyi dan tipu daya, Sedangkan pengertian Terminologis Pencurian (*sariqah*) adalah mengambil harta orang lain dengan sembunyi – sembunyi dari tempat penyimpanannya.[54] Adapun Menurut Wahbah al-Zuhaili, pencurian diartikan sebagai mengambil harta milik orang lain di luar penjualannya, dan harus dilakukan secara sembunyi-sembunyi dengan niat untuk memilikinya. Dari penjelasan diatas tentang pencurian dapat diuraikan unsur dari *sariqah* atau pencurian sebagai berikut :

[54] Fitri Wahyuni, *Hukum Pidana Islam*, Tangerang; PT Nusantara Persada, (2018). 26

1. Mengambil barang seseorang secara sembunyi – sembunyi
2. Barang curian yang diambil tersebut merupakan barang yang berharga
3. Yang diambil merupakan milik orang lain
4. Dengan sengaja memiliki niat untuk memiliki atau untuk keuntungan pribadi

Dasar hukum pencurian atau *sariqah* dalam hukum pidana islam diatur dalam Al-Qur'an, sebagai mana firman Allah SWT. dalam QS. Al-Maidah (5): 38.

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوْٓا اَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَالًا مِّنَ اللّٰهِ ۗوَاللّٰهُ عَزِيْزٌ حَكِيْمٌ

Terjemahnya :

"Laki-laki maupun perempuan yang mencuri, potonglah tangan keduanya sebagai balasan atas perbuatan yang mereka lakukan dan sebagai siksaan dari Allah. Allah Maha perkasa lagi Maha bijaksana."[55]

Dari penjelasan di atas, dikatakan bahwa pencurian atau *sariqah* terjadi jika yang diambil merupakan barang berharga milik orang lain. Sama halnya dalam kasus *phishing* tetapi yang diambil adalah data dan hal ini terjadi di dunia maya. dalam *Phishing* memiliki teknik untuk mengambil hak orang lain dengan mengelabui orang lain. Ini memungkinkan pelaku *phishing* untuk mendapatkan data pribadi seperti *password, username,* ID (*Identity*

[55] Kementerian Agama, Al-Quran QS.Al-maidah/5:38

Document), PIN (*Personal Identification Number*), nomor rekening, nomor kartu kredit, dan lain-lain dari korban penipuan. [56]

Dengan demikian, tindakan *phishing* memiliki sejumlah kesamaan dengan pencurian yang mana *phisher* (pelaku *Phishing)* melakukan aksinya secara sembunyi – sembunyi, data pribadi dianggap sebagai "harta" dalam konteks digital, *Phisher* (pelaku *phishing*) memiliki niat jelas untuk menggunakan atau memanfaatkan data yang diambil untuk keuntungan pribadi, serta sistem digital atau akun online dapat dianggap sebagai "tempat penyimpanan" modern untuk data pribadi.

Selain *phishing* memiliki kesamaan dengan pencurian Tindak pidana *phishing* ini juga menggunakan metode penipuan atau tipu muslihat di mana seseorang berupaya memperdaya orang lain dengan menggunakan akal licik atau strategi untuk mengiming-imingi sesuatu demi meraih keuntungan, sehingga korban mengikuti keinginan pelaku. Seseorang yang Memakan harta orang lain dengan cara yang batil, seperti melalui penipuan, adalah perbuatan dosa, sebagaimana firman Allah SWT. dalam QS. Al-Baqarah (2): 42.

وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ وَتَكْتُمُوا الْحَقَّ وَاَنْتُمْ تَعْلَمُوْنَ

Terjemahnnya :

[56] Hendra Gunawan, "Tindakan Kejahatan Cyber Crime dalam Prespektif Fiqih Jinayah " Jurnal Ilmu Kesyariahan, volume 6 ,nomor 1 (2020). 44

"Janganlah kamu campuradukkan kebenaran dengan kebatilan dan (jangan pula) kamu sembunyikan kebenaran, sedangkan kamu mengetahui(-nya)."[57]

Penipuan dapat juga dikatakan sebagai sebuah kebohongan / kedustaan (berdusta), sesuai dengan firman allah dalam QS. An-Nahl (6) 105 :

اِنَّمَا يَفْتَرِى الْكَذِبَ الَّذِيْنَ لَا يُؤْمِنُوْنَ بِاٰيٰتِ اللّٰهِۚ وَاُولٰۤىِٕكَ هُمُ الْكٰذِبُوْنَ

Terjemahnnya :

> "Sesungguhnya yang mengada-adakan kebohongan hanyalah orang-orang yang tidak beriman kepada ayat-ayat Allah. Mereka itulah para pembohong."[58]

Dari penjelasan diatas, Karena *phishing* merupakan perbuatan maksiat yang menipu dan Mencuri data milik korban, maka tindakan ini dapat dikenakan hukuman *ta'zir*. Menurut *syara'*, *Ta'zir* merupakan bentuk sanksi yang diterapkan untuk pelanggaran atau tindak kriminal yang tidak termasuk dalam kategori yang diancam dengan hukuman *hudud* atau *kafarat.* Sanksi ini berfungsi sebagai tindakan disipliner untuk perilaku yang dianggap melanggar norma agama atau hukum, namun tidak memiliki ketentuan hukuman yang spesifik dalam syariat Islam. *Ta'zir* memberikan fleksibilitas bagi hakim atau otoritas yang berwenang untuk menentukan hukuman yang sesuai dengan tingkat keseriusan pelanggaran dan kondisi pelaku, dengan tujuan untuk mencegah pengulangan tindakan dan memperbaiki perilaku pelanggar.

---

[57] Kementerian Agama, Al-Quran QS.Al-Baqarah/2 :42

[58] Kementerian Agama, Al-Quran QS.An-Nahl/16:105

Adapun Macam-macam hukuman *ta'zir* sangat beragam. Di antaranya adalah: Pertama, sanksi yang berkaitan dengan tubuh, seperti hukuman mati dan cambuk; Kedua, sanksi yang berkaitan dengan kebebasan, seperti penjara dan pengasingan; Ketiga, sanksi yang berkaitan dengan harta, seperti denda, penyitaan, atau perampasan, dan penghancuran barang; dan Keempat, sanksi tambahan yang ditetapkan oleh ulil amri untuk kepentingan umum. [59]

Perbuatan *cyber crime* dalam bentuk *phishing* termasuk dalam *jarimah ta'zir*, sehingga hukuman bagi pelaku *phishing* ditentukan oleh *ulil amri* (Pemerintah). Di Indonesia, kejahatan *cyber crime* diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang -undang Nomor 27 tahun 2022 tentang Perlindungan data pribadi.

Dalam hukum pidana Islam, Jenis-jenis hukuman yang termasuk dalam jarimah *ta'zir* meliputi hukuman penjara, skorsing atau pemecatan, ganti rugi, pukulan, teguran lisan, dan jenis hukuman lain yang dianggap sesuai dengan pelanggaran pelakunya. Dalam hukum Islam, jenis hukuman *ta'zir* sepenuhnya diserahkan kepada keputusan manusia. Menurut Imam Abu Hanifah, pelanggaran ringan yang dilakukan berulang kali dapat dikenakan hukuman mati oleh hakim. Misalnya, jika seorang pencuri yang telah

[59] Ahmad Djazuli, *Fiqh Jinayah (Upaya Menanggulangi Kejahatan Dalam Islam)*, Jakarta: PT RajaGrafindo, (1997), 192.

dipenjara terus mengulangi perbuatannya, hakim memiliki wewenang untuk menjatuhkan hukuman mati kepadanya. [60]

Jadi, untuk mencapai kemaslahatan, apabila tindak pidana pencurian dengan modus penipuan ini jelas mendatangkan bahaya bagi orang lain, maka bahaya tersebut harus dihilangkan menurut hukum Islam.

Oleh karena itu, dalam tinjauan Fiqh Jinayah, tindak pidana *phishing* merupakan jarimah yang dapat dikenakan sanksi atau hukuman. *Phishing* termasuk dalam kategori jarimah t*a'zir*, di mana perbuatan tersebut tidak dilarang karena substansinya, melainkan karena sifatnya. Sifat yang menjadi alasan (*illat*) dijatuhkannya hukuman adalah dampaknya yang berbahaya atau merugikan kepentingan umum. Karena *phishing* memiliki unsur yang merugikan kepentingan umum, perbuatan ini dianggap sebagai jarimah, dan hukuman untuk pelakunya diserahkan kepada hakim atau penguasa.

c. Persamaan dan Perbedaan Pandangan Hukum Positif Dan Hukum Pidana Islam

1. Persamaan

Phishing sebagai bentuk kejahatan siber yang melibatkan pencurian data pribadi melalui manipulasi dan penipuan, telah menjadi perhatian serius baik dalam konteks hukum Islam maupun hukum positif di berbagai negara, termasuk Indonesia. Menariknya, meskipun berasal dari latar belakang dan tradisi hukum yang berbeda, kedua sistem hukum ini

[60] Zainuddin, *Hukum Islam: Pengantar Ilmu Hukum Islam di Indonesia*, Jakarta: Sinar Grafika, (2006). 129

menunjukkan korelasi yang signifikan dalam mengakui *phishing* sebagai suatu tindak pidana yang perlu ditangani dengan tegas.

Hukum Islam, dengan prinsip-prinsip universal dan fleksibilitasnya, telah mampu beradaptasi dengan tantangan era modern.[61]Sementara itu, hukum positif Indonesia, melalui berbagai peraturan perundang-undangan, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), secara eksplisit mengatur tentang kejahatan siber. Korelasi antara kedua sistem hukum ini dalam memandang *phishing* sebagai tindak pidana tidak hanya mencerminkan kesepahaman dalam mengidentifikasi ancaman, tetapi juga menunjukkan komitmen bersama untuk melindungi masyarakat dari bahaya kejahatan siber.[62]

Dalam hukum pidana islam *phishing* tidak disebutkan secara eksplisit dalam sumber-sumber hukumnya, tetapi *phishing* dikategorikan sebagai pencurian modern dengan menggunakan metode penipuan sehingga berdasarkan prinsip *maqashid syariah* khususnya dalam prinsip perlindungan harta, *phishing* dianggap sebagai pelanggaran terhadap tujuan syariah. Pada fatwa-fatwa kontemporer dari berbagai lembaga fatwa islam telah menegaskan bahwa *phishing* adalah tindakan yang tidak terpuji karna merugikan orang lain. [63]senada dengan ini dalam peraturan

---

[61] Ahmad Wardi Muslich, *Hukum Pidana Islam*, Jakarta : Sinar Grafika, (2005),29.

[62] Barda Nawawi,. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta : Raja Grafindo Persada, 2006. 27

[63] Sofwan Jannah & M. Naufal, "Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam", Jurnal Al-Mawarid Fakultas Ilmu Agama Islam UII Yogyakarta, Volume XII Nomor 1, 2012. 82.

perundang-undangan diindonesia dengan tegas melarang tindakan *phishing* tersebut melalui undang-undang no. 11 tahun 2008 tentang informasi dan tranksaksi elektronik (UU ITE), yang telah di perbarui dengan UU no. 19 tahun 2016 serta UU no 27 tahun 2022 tentang perlindungan data pribadi (UU PDP), mengatur secara spesifik tentang kejahatan siber, termaksud *phishing.*[64]

Dari penjelasan diatas bahwa korelasi dari pandangan hukum pidana islam dan hukum positif menyatakan dengan tegas bahwa tindak pidana *Phishing* merupakan tindakan yang dilarang karna dapat merugikan dan mengganggu kentraman orang lain

2. Perbedaan

Perbedaan yang cukup besar antara cara hukum pidana Islam dan hukum positif memandang tindakan *phishing*. Dalam perspektif hukum pidana Islam, *phishing* dianggap sebagai tindakan mencuri dan menipu yang bertentangan dengan prinsip Perlindungan Harta (*hifz al-mal*).[65] Konsekuensinya adalah hukuman *ta'zir* yang dapat disesuaikan berdasarkan kebijaksanaan hakim. Di sisi lain, hukum positif umumnya menempatkan *phishing* dalam kategori *cybercrime* atau penipuan digital,

[64] Budi Suhariyanto,*Tindak PidanaTeknologi Informasi; Cybercrime; Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: Rajawali Pers, (2012), 124.

[65] Sofwan Jannah & M. Naufal, "Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam", Jurnal Al-Mawarid Fakultas Ilmu Agama Islam UII Yogyakarta, Volume XII Nomor 1, 2012. 85.

dengan hukuman yang telah ditetapkan dalam undang-undang, biasanya berupa denda finansial dan/atau kurungan penjara.[66]

Kedua sistem hukum ini memiliki landasan yang berbeda. Hukum Islam mengacu pada syariah, sementara hukum positif berpijak pada peraturan yang ditetapkan oleh otoritas negara. Dalam hal penerapan hukuman, hukum Islam menawarkan fleksibilitas melalui konsep *ta'zir,* sedangkan hukum positif cenderung memiliki ketentuan hukuman yang lebih kaku dan telah ditentukan sebelumnya.[67]

[66] Ibid. 86

[67] Ibid. 89

BAB V
PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah disajikan diatas, maka penulis dapat menarik kesimpulan dari hasil penelitian ini sebagai berikut:

1. *Phishing* adalah teknik penipuan untuk mencuri data pribadi menggunakan situs web palsu atau komunikasi elektronik yang tampak resmi. Istilah ini berasal dari "*fishing*" (memancing) dalam bahasa Inggris. Tujuannya adalah memperoleh informasi sensitif untuk keuntungan finansial atau pencurian identitas. Karakteristik utama phishing yakni Menggunakan manipulasi psikologis dan rekayasa sosial, Memanfaatkan rasa urgensi atau ketakutan korban, Menggunakan teknik seperti peniruan situs web dan manipulasi tautan, Berkembang menjadi metode lebih canggih (*spear phishing, vishing, smishing*) dan Memanfaatkan AI dan *deep learning* untuk konten yang lebih meyakinkan. Untuk menghadapi ancaman phishing yang terus berkembang, diperlukan kewaspadaan, edukasi berkelanjutan, dan pengembangan teknologi keamanan yang adaptif.

2. *Phishing* adalah kejahatan siber yang kompleks, dianggap serius dalam hukum Islam dan hukum Indonesia. dalam Hukum Islam Dianggap sebagai pencurian modern (*sariqah*) dan penipuan (*ghish*), Melanggar prinsip perlindungan harta (*hifz al-mal*)dan Dikenakan hukuman *ta'zir* sesuai tingkat kejahatan. pada Hukum Positif Indonesia Diatur dalam UU ITE dan UU PDP, UU ITE: mengatur tindakan menyesatkan dan akses tanpa hak dan UU PDP: memperkuat perlindungan data pribadi dan menetapkan sanksi. Kedua sistem hukum menganggap *phishing* sebagai ancaman serius terhadap keamanan data,

3. privasi, dan ekonomi digital. Penanganan *phishing* memerlukan Penegakan hukum yang kuat, Kerjasama internasional, Edukasi masyarakat, Pengembangan teknologi keamanan siber dan Peningkatan kapasitas aparat penegak hukum. Kombinasi penegakan hukum efektif, edukasi berkelanjutan, dan teknologi keamanan mutakhir diperlukan untuk melindungi masyarakat dari risiko *phishing.*

B. Implikasi Penelitian

Dengan adanya Fenomena tindak pidana Phishing yang semakin marak di tengah masyarakat dengan menggunakan metode atau tehnik juga yang semakin berkembang , maka implikasi penelitin ini sebagai berikut:

1. Menghadapi ancaman kejahatan siber yang terus berkembang, khususnya phishing dan pencurian data pribadi, diperlukan pendekatan komprehensif yang melibatkan berbagai aspek. Hal ini mencakup pembaruan kerangka hukum agar tetap relevan dengan perkembangan teknologi, sinergi antara pemerintah, penegak hukum, penyedia layanan internet, institusi keuangan, dan masyarakat untuk menciptakan ekosistem digital yang lebih aman. Pemerintah perlu meningkatkan perhatian terhadap kejahatan komputer, terutama pencurian data pribadi, baik di instansi pemerintah maupun masyarakat umum. Penguatan pertahanan teknologi menjadi kunci dalam mengatasi masalah ini, disertai dengan edukasi masyarakat tentang risiko kejahatan siber dan cara melindungi diri. Dengan pendekatan holistik ini, diharapkan dapat tercipta lingkungan digital yang lebih aman dan terlindungi, sambil tetap mengikuti perkembangan teknologi dan modus operandi kejahatan yang terus berubah.
2. Perlu meningkatkan kewaspadaan terhadap email dan tautan website yang meminta informasi pribadi atau perbankan, terutama yang menjanjikan hadiah

atau menggunakan ancaman. Penting untuk memastikan bahwa data hanya dikirim ke situs resmi yang terpercaya. Mengenai pelaku phishing yang tertangkap, ada baiknya mereka tidak hanya dihukum tapi juga dibina selama masa tahanan. Mengingat keahlian mereka di bidang teknologi informasi, Indonesia sebenarnya membutuhkan keterampilan tersebut jika diarahkan untuk hal-hal yang positif.

DAFTAR PUSTAKA

A.Aco Agus dan Riskawati, "Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," Jurnal Supremasi, Vol. 10, N, 2016

Abdul Wahid, Mohammad Labib, Kejahatan Mayantara (Cyber Crime), (Bandung: PT Refika Aditama, 2005

Abdul Muis Andi , Indonesia di Era Dunia Maya Teknologi Informasi dalam Dunia Tanpa Batas, (Bandung:PT Remaja Rosdakarya Offset,2001)

Ahmad Djazuli, Fiqh Jinayah (Upaya Menanggulangi Kejahatan Dalam Islam), Jakarta: PT RajaGrafindo, 1997.

Ahmad Wardi Muslich, Hukum Pidana Islam, Jakarta : Sinar Grafika, (2005).

Anton Bakker dan AhmadZubeir, Metodologi Penelitian Filsafat (Yogyakarta:Kanisius, 1990),

Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nabawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik.", PAMPAS: Journal Of Criminal, Volume 1, Nomor 2, (2020)

Ardi Saputra Gulo, "Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik" PAMPAS: Journal of Criminal Vol.1 (2020).

Ardhiwisastra Yudha Bhakti , Hukum Internasional, (Bandung, Bunga Rampat, 2003)

Arief, Barda Nawawi,. Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, Jakarta : Raja Grafindo Persada, 2006.

Arfah Rizki , "Sanksi Tindak Pidana Hacking (Studi Analisis Undang-Undang ITE dan Hukum Pidana Islam," Angewandte Chemie International Edition, 6(11), 951–952. (UIN Sumatera Utara, 2018).

Atmasasmita Romli , Sistem Peradilan Pidana ; Perspektif Eksistensialisme dan Abilisionisme, Cet II revisi, Bina Cipta, Bandung, 1996

Ayu Putriyanti, "Yurisdiksi di Internet/Cyberspace",9 Media Hukum (2009).

Barda Nawawi,. Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, Jakarta : Raja Grafindo Persada, 2006.

Budi Suhariyanto,Tindak PidanaTeknologi Informasi; Cybercrime; Urgensi Pengaturan dan Celah Hukumnya, Jakarta: Rajawali Pers, (2012).

Dikdik M. Arief Mansur dan Elisatris Gulto, Cyber law Aspek Hukum Teknologi Informasi dan Komunikasi, (Bandung:PT Refilka Aditama, 2009)

Djazuli, Ilmu Fiqh: Penggalian, Perkembangan, dan Penerapan Hukum Islam (Ponorogo: Pustaka Setia, 2010).

Fitri Wahyuni,Hukum Pidana Islam,Tanggerang;TPT Nusantara Persada, (2018).

Hasan, Mustofa dan Saebani, Beni Ahmad,. Hukum Pidana Islam; Fiqh Jinayah, Bandung: Pustaka Setia, 2013.

Hendra Gunawan, "Tindakan Kejahatan Cyber Crime dalam Prespektif Fiqih Jinayah " Jurnal Ilmu Kesyariahan, volume 6 ,nomor 1 (2020).

Hidayat Sulham Akbar , "TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI ONLINE SHOP MENGGUNAKAN MALWARE (Studi Kasus Putusan Nomor: 252/Pid.Sus/2020/PN. SMN)" (Universitas Hasanudin, 2021).

Indrajit, Richardus Eko,. Konsep dan Strategi Kemanan Informasi di Dunia Cyber, Yogyakarta: Graha Ilmu, 2014.

Irfan M. Nurul , Hukum Pidana Islam (Jakarta : Amzah, 2016)

Irfan, M. Nurul dan Masyrofah,. Fiqih Jinayat, cet ke-1, Jakarta: Amzah, 2013.

Jaenudin Jaenudin dan Rasyida Rofiatun Nisa, "Islamic Criminal Law Analysis of Cyber Crimes on Consumers in E-Commerce Transactions," Islamic Criminal Law Analysis of Cyber Crimes on Consumers in E-Commerce Transactions, 1.4 (2021), .

Maulia Jayantina Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," Jurnal Masyarakat Telematika Dan Informasi, Vol. 8 No. (2017)

Maskun, Kejahatan Siber (Cyber Crime) : Suatu Pengantar, Kencana (2013).

Mahmud Marzuki Peter , Penelitian Hukum, Penerbit Kencana, Jakarta, 2007

Muslich, Ahmad Wardi,. Hukum Pidana Islam, Jakarta : Sinar Grafika, 2005.

Margareta Rosa Anjani dan Budi Santoso. "Urgensi Rekonstruksi Hukum E-commerce di Indonesia", Jurnal Law Reform, Volume 14, Nomor 1, (2018).

Mia Haryati Wibowo dan Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime", Journal of Education and Information Communication Technology, Volume 1, Nomor 1, (2017).

Nudirman Munir, Pengantar Hukum Siber Indonesia, Rajawali Pers (2017).

Naskah Akademik Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik, 2008

Nasution, Muhammad Arsad,. Hoax Sebagai Bentuk Hudud, Jurnal Yurispudentia; Jurnal Hukum Ekonomi Syariah Fakultas Syariah dan Ilmu Hukum IAIN Padangsimpuan, Volume 3 Nomor 1, Edisi Januari-Juni Tahun 2017.

Nur Khalimatus Sa'diyah, "Modus Operandi Tindak Pidana Cracker Menurut Undang-Pemilik Domain Situs Phising", (2011).

Panjaitan, Hinca IP dkk,. Membangun Cyber Law Indonesia yang Demokratis, Jakarta: IMLPC, 2005.

Purnamawati, Dian,. Mengenal Dunia Cyber, Surakarta : CV. Mediatama, 2007.

Santoso, Topo, Membumikan Hukum Pidana Islam; Penegakan Syariat dalam Wacana dan Agenda, cet ke-1, Jakarta : Gema Insani Press, 2003.

Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia.", Yustisia Jurnal Hukum, Volume 5, Nomor 1 (2016).

Sitompul, Josua,. Cyberspace, Cybercrimes, Cyberlaw; Tinjauan Aspek Hukum Pidana, Jakarta: Tatanusa, 2012.

Sisi Wardani, siti kalilah dan deden najmudin, "Perbandingan hukuman jarimah sariqah dalam hukum pidana islam dengan hukum Indonesia" jurnal kajian agama, vol. 1 no. 2 (2023).

Sofyan Maulana, Hukum Pidana Islam dan Pelaksanaan, (Jakarta, Rineka Cipta, 2004).

Suhariyanto, Budi,.Tindak PidanaTeknologi Informasi; Cybercrime; Urgensi Pengaturan dan Celah Hukumnya, Jakarta: Rajawali Pers, 2012.

Sunggono Bambang , Metodologi Penelitian Hukum, cet. ke-1 (Jakarta: Raja Grapindo Persada, 2007)

Syahdeini, Sutan Remy. Utama Grafita, hlm 63-64.2009. *Kejahatan & Tindak Pidana Komputer*. Jakarta: Pustaka

Tabrani Sabrina dan safitri vivi, "Kejahatan Phishing ditinjau dari prespekktif hukum dan kejahatan siber", vol 3 (2024).

Undang Informasi Dan Transaksi Elektronik",(2012).

vikran Fassyadhiyaksa putra, "Modus Operandi tindakan pidana Phishing Menurut UU ITE" Jurist-Diction Vol. 4 (2021).

Zainuddin, Hukum Islam: Pengantar Ilmu Hukum Islam di Indonesia Jakarta: Sinar Grafika, (2006).

DAFTAR LAMPIRAN

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI DATOKARAMA PALU
جامعة داتوكاراما الإسلامية الحكومية بالو
STATE ISLAMIC UNIVERSITY DATOKARAMA PALU
FAKULTAS SYARIAH
Jl. Diponegoro No. 23, Lere, Kec. Palu Barat, Kota Palu, Sulawesi Tengah 94221
Website [illegible] email : [illegible] (mailto [illegible]) Telepon (0451-460798

PENGAJUAN JUDUL SKRIPSI

Nama	: Ahmad Yasir arafah	NIM	: 193080012
TTL	: Palu, 15 maret 2000	Jenis Kelamin	: Laki - Laki
Prodi	: Perbandingan mazhab	Semester	: VII (Tujuh)
Alamat	: Jl. beringin Lr. Damai	HP	: 081342065070 (WA)

Judul :

1. Judul I
   Fenomena Phising (Pencurian data pribadi dalam Perspektif hukum Islam dan hukum positif
2. Judul II
   Hukuman mati bagi pengedar Narkoba dalam tinjauan hukum islam dan ham
3. Judul III
   analisis hukum islam terhadap tradisi baboliq dari suku kaili kota palu

Palu, 8 November 2022
Mahasiswa,

(a yasir arafah)
NIM. 193080012

Telah disetujui penyusunan skripsi dengan catatan :

Pembimbing I : Prof. Dr. Marzuki, MH.
Pembimbing II : Dr. Sitti Mawaliah, M.Th.I

an. Dekan
Wakil Dekan Bidang Akademik, Kemahasiswaan,
Kelembagaan & Kerjasama,

Dr. M. Taufan B, S.H., M.Ag
NIP. 19710827200003 1 002

Ketua Program Studi,

Hafiyani, M.H
NIP. 198911202018012002

KEPUTUSAN DEKAN FAKULTAS SYARIAH
UNIVERSITAS ISLAM NEGERI DATOKARAMA PALU
NOMOR : 590 TAHUN 2022

TENTANG

PENUNJUKAN DOSEN PEMBIMBING SKRIPSI MAHASISWA
FAKULTAS SYARIAH UIN PALU
TAHUN AKADEMIK 2022/2023

Membaca : Surat saudara : **Ahmad Yasir Arafah** / NIM **19.3.08.0012** mahasiswa Program Studi **Perbandingan Mazhab** Fakultas Syariah UIN Datokarama Palu, tentang pembimbingan penulisan skripsi pada program Strata Satu (S1) Fakultas Syariah UIN Datokarama Palu dengan judul skripsi : **Fenomena Phising (Pencurian Data Pribadi Dalam Perspektif Hukum Islam Dam Hukum Positif**

Menimbang :
a. bahwa untuk kelancaran pelaksanaan pembimbingan skripsi tersebut, dipandang perlu untuk menunjuk dosen pembimbing mahasiswa yang bersangkutan.
b. bahwa mereka yang namanya tercantum dalam keputusan ini dipandang cakap dan mampu melaksanakan tugas pembimbingan tersebut.
c. bahwa berdasarkan pertimbangan sebagaimana pada huruf a dan b tersebut, dipandang perlu menetapkan Keputusan Dekan dan Fakultas Syariah UIN Datokarama Palu.

Mengingat :
1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
2. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi;
3. Peraturan Pemerintah Nomor 32 Tahun 2013 tentang Standar Pendidikan Nasional
4. Peraturan Presiden Nomor 61 Tahun 2021 tentang Perubahan Bentuk Institut Agama Islam Negeri (IAIN) Palu Menjadi Universitas Islam Negeri (UIN) Datokarama Palu;
5. Peraturan Menteri Agama Repuplik Indonesia Nomor 7 Tahun 2016 Tentang Perubahan Atas Peraturan Menteri Agama Nomor 47 Tahun 2015 Tentang Statuta Institut Agama Islam Negeri Palu.
6. Peraturan Menteri Agama Nomor 30 Tahun 2021 Tentang Susunan Organisasi dan Tata Kerja Universitas Agama Islam Negeri Palu.
7. Keputusan Mentri Agama RI Nomor: 455/Un.24/KP.07.6/12/2021 Tanggal 27 Desember 2021 Tentang Pengangkatan Dekan Fakultas Syariah Universitas Islam Negeri Datokaramna Palu.

MEMUTUSKAN

Menetapkan : KEPUTUSAN DEKAN FAKULTAS SYARIAH UNIVERSITAS ISLAM NEGERI (UIN) DATOKARAMA PALU TENTANG PENUNJUKAN DOSEN PEMBIMBING SKRIPSI MAHASISWA FAKULTAS SYARIAH UNIVERSITAS ISLAM NEGERI (UIN) DATOKARAMA PALU TAHUN AKADEMIK 2022/2023

Pertama	:	1. **Prof. Dr. Marzuki, M.H.** 2. **Dr. Sitti Musyahidah, M.Th.I.**	(Pembimbing I) (Pembimbing II)
Kedua	:	Pembimbing I bertugas memberikan bimbingan berkaitan dengan substansi/isi skripsi. Pembimbing II bertugas memberikan bimbingan berkaitan dengan metodologi penulisan skripsi.	
Ketiga	:	Segala biaya yang timbul sebagai akibat dikeluarkannya Keputusan ini, dibebankan pada anggaran DIPA UIN Datokarama Palu Tahun Anggaran 2022.	
Keempat	:	Jangka waktu penyelesaian skripsi dimaksud selambat-lambatnya 6 (enam) bulan terhitung mulai tanggal ditetapkannya Keputusan ini.	
Kelima	:	Segala sesuatu akan diubah dan diperbaiki sebagaimana mestinya, apabila di kemudian hari terdapat kekeliruan dalam penetapan Keputusan ini.	

SALINAN : Keputusan ini disampaikan kepada yang bersangkutan untuk diketahui dan dilaksanakan sebagaimana mestinya.

Ditetapkan di : Palu
Pada Tanggal : 9 November 2022

Dekan,

Dr. Ilhamuddin, S.Ag., M.SI
NIP. 19700720 199903 1 008

Tembusan :
1. Rektor UIN Datokarama Palu;
2. Wakil Dekan Bidang Akademik, Kemahasiswaan dan Pengembangan Kelembagaan Fakultas Syariah UIN Datokarama Palu;
3. Dosen Pembimbing yang bersangkutan;
4. Mahasiswa yang bersangkutan;

NO.	HARI/TANGGAL KONSULTASI	MATERI BIMBINGAN SKRIPSI / SARAN	TANDA TANGAN		KETERANGAN
			PEMBIMBING I	PEMBIMBING II	
1	Senin, 22/07/2024	menambah ayat pada hasil	✓		
2	Selasa, 23/07/2024	menambah Perbedaan dan Persamaannya	✓		
3	rabu, 24/07/2024	menambah Daftar Pustaka	✓		
4			✓		
5					
6	Senin, 8/07/2024	Perbaikan Penulisan Pada Pendahuluan			
7	selasa, 9/07/2024	menambah ayat Pada kajian teori			
8	rabu, 10/07/2024	merapikan kembali margin Pada hasil			
9					
10					

Telah diperiksa dan disetujui

Pembimbing I,

NIP.

Pembimbing II,

NIP.

DAFTAR RIWAYAT HIDUP

A. Identitas Diri

Nama	: Ahmad Yasir Arafah
NIM	: 193080012
Tempat Tgl. Lahir	: Palu, 15 Maret 2000
Alamat	: Jl. Beringin Lr. Damai No. 20, Kelurahan Nunu Kecamatan Tatanga, Kota Palu
No. Hp	: 0821-9379-4973
E-Mail	: yasir.arafad.8@gmail.com
Nama Ayah	: Hafiludin, S.Pd
Nama Ibu	: Suryani

B. Riwayat Pendidikan

1. SD/MI, Tahun Lulus : SDN 14 Palu, 2012
2. SMP/MTS, Tahun Lulus : MTS Al-Khairaat Pusat Palu, 2015
3. SMA/MA, Tahun Lulus : MAN 2 Kota Palu, 2019

C. Pengalaman Organisasi

1. Anggota Kewirausahaan HMJ PM, 2020
2. Anggota Komisariat FSEI IAIN Palu HMI MPO Cabang Palu, 2020
3. Kabid Humas Komisariat FSEI HMI MPO Cabang Palu, 2021

4. Wakil Ketua HMJ PM, 2021
5. Sekertaris Umum Senat Fakultas Syariah, 2022
6. Ketua Umum HMI MPO Cabang Palu, 2023
7. Sekertaris KPC HMI MPO Cabang Palu, 2024

Palu, 22 Juli 2024 M
Palu, 16 Muharam 1446 H
Penulis

Ahmad Yasir Arafah
19.30.800.12