

**PERTANGGUNGJAWABAN PIDANA SIBER PHISING
DENGAN MENGGUNAKAN PLATFORM DIGITAL
WHATSAPP**

SKRIPSI

**Ditulis Untuk Memenuhi Syarat
Mendapatkan Gelar Sarjana Hukum**

Oleh:

SURYA RAMADHAN
NPM : 2106200263



UMSU
Unggul | Cerdas | Terpercaya

**FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2025**

FAKULTAS HUKUM

Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061) 6625474-6631003
🌐 <https://umsu.ac.id> ✉ rektor@umsu.ac.id 📘 umsumedan 📷 umsumedan 🐦 umsumedan 📺 umsumedan

Bila menjawab surat ini agar disebutkan
Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA I

Panitia Ujian Sarjana Strata-1 Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam Sidangnya yang diselenggarakan pada hari **Senin**, Tanggal **21 April 2025**, Jam **08.30 WIB** sampai dengan selesai, setelah Mendengar, Melihat, Memperhatikan, Menimbang:

MENETAPKAN

NAMA : SURYA RAMADHAN
NPM : 2106200263
PRODI / BAGIAN : HUKUM/ HUKUM PIDANA
JUDUL SKRIPSI : PERTANGGUNGJAWABAN PIDANA SIBER PHISING DENGAN MENGGUNAKAN PLATFORM DIGITAL WHATSAPP

Dinyatakan : (☒) Lulus Yudisium Dengan Predikat **Istimewa**
(☐) Lulus Bersyarat, memperbaiki/Ujian Ulang
(☐) Tidak Lulus

Setelah lulus dinyatakan berhak dan berwenang mendapatkan gelar **Sarjana Hukum (S.H)** Dalam **Bagian Hukum Pidana**.

PANITIA UJIAN

Ketua

Sekretaris


Assoc. Prof. Dr. FAISAL, S.H., M.Hum
NIDN. 0122087502

Assoc. Prof. Dr. ZAINUDDIN, S.H., M.H
NIDN. 0118047901

Anggota Penguji:

1. Dr. Ismail Koto, S.H., M.H
2. Assoc. Prof. Dr. Farid Wajdi, S.H., M.Hum
3. Hj. Asliani Harahap, S.H., M.H

1.
2.
3.



FAKULTAS HUKUM

Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
<https://umsu.ac.id> rektor@umsu.ac.id [f umsumedan](#) [umsumedan](#) [umsumedan](#) [umsumedan](#)

Bila menjawab surat ini agar disebutkan
Nomor dan tanggalnya

PENGESAHAN SKRIPSI

Judul : PERTANGGUNGJAWABAN PIDANA SIBER PHISING DENGAN
MENGGUNAKAN PLATFORM DIGITAL WHATSAPP
Nama : SURYA RAMADHAN
Npm : 2106200263
Prodi / Bagian : Hukum/Hukum Pidana

Skripsi tersebut diatas telah diujikan oleh Dosen Penguji Fakultas Hukum Universitas Muhammadiyah Sumatera Utara pada tanggal 21 April 2025.

Dosen Penguji

<u>(Dr. ISMAIL KOTO, S.H., M.H.)</u> NIDN:0106069401	<u>(Assoc. Prof. Dr. FARID WAJDI, S.H., M.Hum)</u> NIDN:0120028205	<u>(Hj. ASLIANI HARAHAHAP, S.H., M.H)</u> NIDN:0126066802

Disahkan Oleh :
Dekan Fakultas Hukum UMSU

Assoc. Prof. Dr. FAISAL, S.H. M.Hum.
NIDN: 0122087502



FAKULTAS HUKUM

Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/AK.Ppg/PT/II/2024

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474-6631003

<https://umsu.ac.id> rektor@umsu.ac.id [umsu](https://www.facebook.com/umsu) [umsu](https://www.instagram.com/umsu) [umsu](https://www.youtube.com/umsu) [umsu](https://www.tiktok.com/umsu)

Bila mendapat surat ini agar diberikan
Nomor dan tanggapannya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PENETAPAN HASIL UJIAN SKRIPSI MAHASISWA FAKULTAS HUKUM UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

Berdasarkan Berita Acara Ujian Skripsi yang dilaksanakan pada hari **Senin tanggal 21 April 2025**. Panitia Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dengan ini menetapkan bahwa:

Nama : SURYA RAMADHAN
NPM : 2106200263
Prodi/ Bagian : HUKUM/ HUKUM PIDANA
Judul Skripsi : PERTANGGUNGJAWABAN PIDANA SIBER PHISING DENGAN MENGGUNAKAN PLATFORM DIGITAL WHATSAPP

Penguji :

1. Assoc. Prof. Dr. Farid Wajdi, S.H., M.Hum.	NIDN. 0102087002
2. Hj. Asliani Harahap, S.H., M.H.	NIDN. 0126066802
3. Dr. Ismail Koto, S.H., M.H.	NIDN. 0106069401

Lulus, dengan nilai A, Predikat Istimewa

Oleh karenanya dinyatakan berhak menggunakan gelar **Sarjana Hukum (SH)**.

PANITIA UJIAN

Ketua

Assoc. Prof. Dr. FAISAL, S.H.M.Hum.
NIDN. 0122087502

Sekretaris

Assoc. Prof. Dr. ZAINUDDIN, S.H., M.H.
NIDN. 0118047901



UMSU

Unggul | Cerdas | Terpercaya

Belajarlah untuk meningkatkan kualitas diri

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

UMSU Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 1913/SK/BAN-PT/Ak.KP/PT/XI/2022

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

<https://fahum.umsu.ac.id>

fahum@umsu.ac.id

[fahum@umsu.ac.id](#)

[umsu.ac.id](#)

[umsu.ac.id](#)

[umsu.ac.id](#)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BUKTI PENDAFTARAN UJIAN SKRIPSI

Panitia Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara telah menerima Pendaftaran Ujian Skripsi :

NAMA : SURYA RAMADHAN
NPM : 2106200263
PRODI/BAGIAN : HUKUM/ HUKUM PIDANA
JUDUL SKRIPSI : PERTANGGUNGJAWABAN PIDANA SIBER PHISING
DENGAN MENGGUNAKAN PLATFORM DIGITAL
WHATSAPP
PEMBIMBING : Dr. ISMAIL KOTO, S.H., M.H

Selanjutnya layak untuk diujikan.

Medan, 16 April 2025

PANITIA UJIAN

Ketua

Sekretaris

Assoc.Prof.Dr. Faisal, S.H., M.Hum
NIDN : 0122087502

Assoc.Prof.Dr. Zainuddin, S.H., M.H
NIDN : 0118047901

Unggul | Cerdas | Terpercaya



UMSU
Unggul | Cerdas | Terpercaya

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS HUKUM

Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https://umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan
Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Strata 1 Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, bagi:

NAMA : SURYA RAMADHAN
NPM : 2106200263
PRODI/ BAGIAN : HUKUM/ HUKUM PIDANA
**JUDUL SKRIPSI : PERTANGGUNGJAWABAN PIDANA SIBER PHISING
DENGAN MENGGUNAKAN PLATFORM DIGITAL
WHATSAPP**
PENDAFTARAN : TANGGAL 16 APRIL 2025

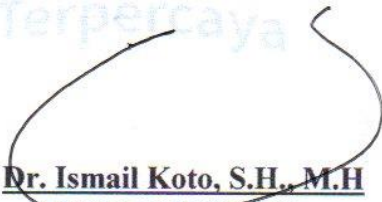
Dengan diterimanya skripsi ini, sesudah lulus dari Ujian Skripsi Penulis berhak memakai gelar:

SARJANA HUKUM (S.H)

Diketahui
DEKAN FAKULTAS HUKUM

Disetujui
DOSEN PEMBIMBING


Assoc. Prof. Dr. FAISAL, S.H., M.Hum
NIDN. 0122087502


Dr. Ismail Koto, S.H., M.H
NIDN. 0106069401

FAKULTAS HUKUM

Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
 <https://umsu.ac.id>  rektor@umsu.ac.id  [umsumedan](#)  [umsumedan](#)  [umsumedan](#)  [umsumedan](#)

Bila menjawab surat ini agar disebutkan
Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA : SURYA RAMADHAN
NPM : 2106200263
PRODI/BAGIAN : HUKUM / HUKUM PIDANA
JUDUL SKRIPSI : PERTANGGUNGJAWABAN PIDANA SIBER PHISING DENGAN
MENGGUNAKAN PLATFORM DIGITAL WHATSAPP

Disetujui untuk disampaikan kepada
Panitia ujian skripsi

Medan, 23 April 2025

Disetujui:
Dosen Pembimbing

Dr. Ismail Koto, S.H., M.H
NIDN: 0106069401

Unggul | Cerdas | Terpercaya



UMSU

Unggul | Cerdas | Terpercaya

Bila mengawat surat di agar disebutkan
nama dan ungganya

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS HUKUM

UMSU Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 1913/SK/BAN-PT/Ak.KP/PT/XI/2022

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

<https://fahum.umsu.ac.id>

fahum@umsu.ac.id

[fahum@umsu.ac.id](#)

[umsu.ac.id](#)

[umsu.ac.id](#)

[umsu.ac.id](#)

PERNYATAAN KEASLIAN PENELITIAN

Saya Mahasiswa Fakultas Hukum Universitas Muhamadiyah Sumatera Utara yang bertanda tangan di bawah ini:

Nama : Surya Ramadhan
NPM : 2106200263
Prodi/Bagian : Hukum/Hukum Pidana
Judul Skripsi : Pertanggungjawaban Pidana Siber Phising Dengan
Menggunakan Platform Digital WhatsApp

Dengan ini menyatakan sesungguhnya bahwa skripsi yang saya tulis secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya. Apabila ternyata di kemudian hari skripsi ini diketahui merupakan hasil plagiat atau merupakan karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik sesuai dengan ketentuan yang berlaku.

Medan, 14 April 2025

Saya yang menyatakan



Surya Ramadhan
2106200269

KATA PENGANTAR



Assalamu'alaikum Warahmatullahi Wabarkatuh

Puji syukur saya atas kehadiran Allah SWT, Tuhan Yang Maha Esa, atas limpahan rahmat, taufik, dan hidayah-Nya, sehingga dalam hal ini penulis dapat menyelesaikan sebuah penyusunan skripsi ini dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan program studi pada Fakultas Hukum, Universitas Muhammadiyah Sumatera Utara.

Secara khusus, dengan penuh rasa hormat dan penghargaan setinggi-tingginya, penulis ingin menyampaikan terimakasih sebesar-besarnya kepada Ayahanda Hery Supriyadi dan Ibunda tercinta Suprapti selaku orang tua penulis yang penuh dengan kasih sayang yang telah membesarkan dan membimbing, dan terimakasih atas doa yang tulus tanpa henti, cinta yang tak terbatas serta dukungan dan motivasi sebagai sumber kekuatan dalam menyelesaikan proses ini. Juga kepada Zaky, Lela, Jopan selaku Abang, Adik-Adik Kandung Penulis, Terima kasih atas doa yang tulus tiada henti, motivasi dan cinta yang diberikan. Serta tak luput juga rasa terimakasih penulis yang sebesar-besarnya kepada seluruh anggota keluarga yang tak dapat disebut satu persatu atas segala bentuk dukungan dan doa serta semangat yang telah diberikan selama penyusunan skripsi ini.

Dengan selesainya skripsi ini, diucapkan terimakasih yang sebesar-besarnya kepada: Rektor Universitas Muhammadiyah Sumatera Utara Bapak Prof. Dr. Agussani., M.AP atas kesempatan dan fasilitas yang diberikan kepada kami untuk mengikuti dan menyelesaikan pendidikan program sarjana ini. Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Bapak Assoc. Prof. Dr. Faisal, S.H., M.Hum atas kesempatan menjadi mahasiswa Fakultas Hukum

Universitas Muhammadiyah Sumatera Utara. Demikian juga halnya kepada Wakil Dekan I Bapak Assoc. Prof. Dr. Zainuddin, S.H., M.H dan Wakil Dekan III Ibu Dr. Atikah Rahmi, S.H., M.H. Terimakasih yang tak terhingga dan penghargaan yang setinggi-tingginya diucapkan kepada Bapak Dr. Ismail Koto, S.H., M.H selaku Pembimbing, yang dengan penuh perhatian telah memberikan dorongan, bimbingan dan arahan sehingga skripsi ini selesai. Disampaikan juga penghargaan kepada seluruh staf pengajar Fakultas Hukum Universitas Muhammadiyah Sumatera Utara (UMSU).

Tiada hal yang paling indah kecuali persahabatan, untuk itu, penulis dalam kesempatan ini ingin mengucapkan terimakasih terhadap sahabat-sahabat penulis yang telah banyak berperan. Ucapan terimakasih yaang istimewa penulis tunjukkan terkhususnya kepada Walaa Dhyaa Abd Aljaleel atas segala dukungan dan motivasi yang diberikan selama proses penyusunan skripsi ini dan kepada teman-teman seperjuangan dalam menyelesaikan tugas akhir di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Terima kasih atas semua kebaikannya semoga Allah SWT membalas kebaikan kalian semua dan semoga semuanya selalu dalam lindungan Allah SWT, Aamiin.

Assalamu'alaikum Warahmatullahi Wabarkatuh

Medan.....2025

Hormat Saya
Penulis

**SURYA RAMADHAN
NPM; 2106200263**

ABSTRAK

**PERTANGGUNGJAWABAN PIDANA SIBER PHISING DENGAN
MENGUNAKAN PLATFORM DIGITAL WHATSAPP**

SURYA RAMADHAN
NPM: 2106200263

Teknologi informasi semakin mempermudah para penggunanya baik dalam hal semua bidang, teknologi mendukung aktivitas manusia dengan keefesiensannya memberikan dampak positif akan tetapi diiringi dengan banyaknya penyalahgunaan teknologi tersebut munculnya kejahatan baru yang disebut cybercrime dalam ruang lingkup jaringan internet. kejahatan tersebut salah satunya disebut phising (penipuan) dengan menggunakan sebuah platform digital WhatsApp (APK), mengirimkan sebuah pesan berupa, link, undangan pdf, maupun Aplikasi (apk), yang merujuk ke sebuah website ataupun Malware (virus), minimnya pengetahuan pengguna menjadi pendorong terjadinya cybercrime dalam bentuk phising.

Penelitian ini merupakan penelitian yuridis normatif, Dengan menggunakan data sekunder serta data yang bersumber dari Al-Qur'an dan Hadist. Kemudian alat pengumpulan data yaitu: Metode studi kepustakaan dengan melakukan telaah mendalam serta dengan pengumpulan bahan literatur yang cukup relevan berupa perundang-undangan, jurnal ilmiah, dan buku yang secara khusus membahas aspek hukum.

Pengaturan tindak pidana cybercrime berupa phising berdasarkan undang-undang No 1 tahun 2024 perubahan kedua atas undang-undang no 11 tahun 2008 tentang informasi dan transaksi elektronik, di atur dalam pasal 28 ayat (1) Jo pasal 45A (1) tentang perbuatan informasi bohong, pasal 30 ayat (3) Jo pasal 46 ayat (3), tentang perbuatan penerobos sistem elektronik, pelaku mengirimkan pesan berupa aplikasi Malware (virus) tanpa sepengetahuan pengguna, pasal 35 Jo pasal 51 ayat (1), tentang Perbuatan memalsukan/manipulasi dokumen elektronik, Pelaku juga dapat dijerat Pasal 65 ayat (1) dan (3) Jo pasal 67 ayat (1) dan (3), UU perlindungan data pribadi (PDP) tentang larangan memperoleh atau mengumpulkan data pribadi orang lain secara melawan hukum.

Kata Kunci: Tindak Pidana, Phising, WhatsApp, Cybercrime

DAFTAR ISI

KATA PENGANTAR	viii
ABSTRAK.....	xi
DAFTAR ISI.....	xii
BAB I PENDAHULUAN.....	1
A. Latar Belakang	1
1. Rumusan Masalah	8
2. Tujuan Penelitian	9
3. Manfaat Penelitian.....	9
B. Definisi Operasional.....	10
C. Keaslian Penelitian	12
D. Metode Penelitian.....	14
1. Jenis Penelitian	15
2. Sifat Penelitian	15
3. Pendekatan Penelitian.....	15
4. Sumber Data Penelitian	16
5. Alat Pengumpul Data.....	17
6. Analisis Data.....	18
BAB II TINJAUAN PUSTAKA.....	19
A. Pertanggungjawaban pidana.....	19
B. WhatsApp	22
C. Cyber Crime	25
D. Cyber Phising	30
BAB III HASIL PENELITIAN DAN PEMBAHASAN	37
A. Penyebab Terjadinya Tindak Pidana Siber Phising Dengan Menggunakan Platform Digital WhatsApp.....	37
B. Pengaturan Hukum Tindak Pidana Siber Phising Dengan Menggunakan Platform WhatsApp.....	46
1. Menurut Undang-undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi.....	46
2. Menurut Undang-undang No 1 Tahun 2024 Perubahan Kedua Atas Undang-undang No 11 Tahun 2008 Tentang Transaksi Dan Informasi Elektronik.....	51

3. Pengaturan Hukum Menurut Pandangan Islam	59
C. Perlindungan Hukum Dalam Bentuk Preventif Terhadap Korban	
Tindak Pidana Siber Phising Dengan Menggunakan Platform Digital	
WhatsApp.....	69
BAB IV KESIMPULAN DAN SARAN	79
A. KESIMPULAN	79
B. SARAN	80
DAFTAR PUSTAKA.....	82

BAB I

PENDAHULUAN

A. Latar Belakang

Di era digital saat ini, hampir setiap aspek kehidupan manusia tak terlepas dari yang namanya sebuah teknologi. Dalam hal bersosialisasi, informasi, bahkan hingga melakukan strategi promosi secara terukur dengan menggunakan digital. Seiring perkembangan jaman, bentuk daripada sebuah platform digital terus beragam macam, mencakup seperti situs web maupun aplikasi mobile, dengan kehadiran kecanggihan teknologi yang terus berkembang ini menjadi berbagai macam aspek kegiatan dapat dilakukan dengan cepat.¹

Dalam memanfaatkan platform digital dapat dijadikan sebagai penunjang kebutuhan dan perkembangan baik oleh pemerintah, individu, maupun perusahaan yang diyakini mampu memberikan sebuah dampak positif yang signifikan. Selain itu perlu juga kita sadari bahwa platform digital memiliki potensi untuk membentuk kita menjadi pribadi yang lebih berarti, namun harus dimanfaatkan secara positif dan bertanggung jawab, pemanfaatan Platform Digital secara positif diyakini akan memperoleh dukungan yang luas dalam berbagai kalangan, mengingat bahwa kontribusinya yang signifikan dalam mendorong kemajuan dan memberikan dampak positif bagi masyarakat.²

¹Ratna Patria, 2023. *"Platform Digital adalah: Pahami Jenis-Jenis Platform Digital"* <https://www.dominesia.com/berita/platform-digital-adalah/>, diakses 3 Januari 2025, Pukul 23:11 WIB.

²Priatna, *et.al.* (2022). "Pengaruh Efektivitas Platform Digital Terhadap Kinerja Pegawai Dinas Arsip Dan Perpustakaan Kabupaten Sumedang". *JRPA-Journal of Regional Public Administration*, Vol 7, No 2, Halaman 96.

Platform digital yang menjadi sarana dalam mengelola data, baik memproses, menyusun, menyimpan, dan memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yakni informasi yang relevan maupun informasi akurat, yang dapat dimanfaatkan untuk keperluan pribadi maupun dijadikan sebagai hal yang mendasar dalam mengambil sebuah keputusan yang strategis.³ Jika di bandingkan dengan teknologi pada tahun 80an masih tergolong jauh dalam kecanggihan teknologi pada zaman sekarang yang beraneka ragam model.⁴

Pada masa kontemporer, ini menjadi tren yang merujuk pada teknologi informasi dan komunikasi, yaitu digital, satelit, komputer, dan smartphone.⁵ Di era modern seperti sekarang, kebutuhan akan informasi menjadi sesuatu yang cukup vital bagi kehidupan masyarakat. Dengan pesatnya perkembangan teknologi telah membuka akses komunikasi dan informasi tanpa batas waktu dan jarak, serta memungkinkan manusia terhubung secara instan dimana pun mereka berada.⁶

Pesatnya perkembangan di dunia teknologi informasi dan komunikasi tidak hanya membawa dampak yang positif terhadap penggunaannya, akan tetapi juga

³ Cholik, C. A. (2021). "Perkembangan teknologi informasi komunikasi/ICT dalam berbagai bidang". Jurnal: Fakultas Teknik UNISA Kuningan, Vol 2, No 2, Halaman 45-46.

⁴ Wiryany, D., Natasha, S., & Kurniawan, R. (2022). "Perkembangan Teknologi Informasi dan Komunikasi terhadap Perubahan Sistem Komunikasi Indonesia". Jurnal Nomosleca, Vol 8, No 2, Halaman 245.

⁵ Nugroho, C., Sos, S., & Kom, M. I. (2020). "Cyber Society: Teknologi, Media Baru, dan Disrupsi Informasi". Jakarta. Prenada Media. Halaman 14.

⁶ Lukiyana, L. (2020). "Pengaruh Perkembangan Teknologi Aplikasi Smartphone Dan Self Management Terhadap Sikap Dan Perilaku Generasi Milenial Yang Di Moderasi Oleh Kecerdasan Emosional". Media Manajemen Jasa, Vol 8, No 1. Halaman 44.

membawa celah bagi penyalahgunaan yang semakin luas. Fenomena ini menciptakan sebuah tantangan baru berupa kejahatan di ranah digital, yang dikenal dengan istilah *cybercrime*. Berbagai bentuk kejahatan Siber kini marak terjadi menimbulkan kerugian yang cukup signifikan serta dampak negatif yang cukup luas.⁷ Kejahatan melalui teknologi informasi ataupun yang dikenal *cybercrime* ialah representasi dari kejahatan internasional yang memakai hitech sebab karakteristik serta kejahatan yang sangat menonjol merupakan *borderless* atau tidak mengenal batasan negara.⁸

Ragam aksi kejahatan Siber terus berkembang, mulai dari skala yang ringan hingga yang paling berat dan merugikan. Kementerian Komunikasi dan informatika (Kominfo) bahkan menyebutkan kejahatan siber sebagai momok menakutkan bagi Indonesia. Bahkan sepanjang tahun 2023 sudah tercatat lebih dari 29 juta serangan Siber yang berhasil diblokir, mencerminkan urgensi penanganan terhadap ancaman digital yang semakin masif.⁹ Hingga menempatkan Indonesia sebagai negara dengan jumlah serangan siber tertinggi di dunia. Fakta ini terungkap dalam gelaran Indonesia *Cyber Crime Summit* yang diselenggarakan di Institut Teknologi Bandung (ITB).¹⁰

⁷ Habibi, M. R., & Liviani, I. (2020). "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia". *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, Vol 23, No 2, Halaman 413.

⁸ Sambodo, C. G., & Wahyuningsih, S. E. "The Criminal Law Enforcement Against Crime Of Carding In Electronic Transactions. *Law Development Journal*". Vol 3, No 2, Halaman 240-241

⁹ Diskominfo, 2023, "*29 Juta Serangan Siber Diblokir di Indonesia Selama 2023*", <https://kominfo.lhokseumawekota.go.id/berita/read/29-juta-serangan-siber-diblokir-di-indonesia-selama-2023->, diakses 4 Januari 2025, pukul 00:26 WIB.

¹⁰ Antoni, A. (2021). "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online". *Nurani: Jurnal Kajian Syari'ah dan Masyarakat*, Vol 17, No 2, Halaman 273-274.

Cybercrime ialah tindak kejahatan ataupun aktivitas ilegal yang dijalankan lewat jaringan dunia elektronik. Aksi kriminal dalam internet ialah kejahatan yang berhubungan dengan dunia maya yang bisa membahayakan privasi seseorang. Contoh dari kejahatannya semacam pornografi, perjudian online, terorisme, *hacking*, *carding*, *phishing*, serta masih banyak tindak kejahatan yang lain.¹¹

Kejahatan tersebut umumnya dipicu oleh motif kepuasan pribadi, yang mana dalam hal ini dapat diartikan sebagai dorongan atau motif ekonomi dilakukan untuk memperoleh keuntungan finansial, baik secara individu maupun kolektif, dengan merugikan pihak lain secara ekonom melalui media elektronik khususnya platform digital berupa media sosial.¹²

Media sosial merupakan platform digital berbasis daring yang memungkinkan pengguna untuk berpartisipasi secara aktif dalam hal berbagi, berinteraksi serta tidak terlepas dengan bertukar informasi.¹³ Manakala pula media sosial memberikan kebebasan untuk membuat halaman pribadi.¹⁴

Perlu diketahui juga bahwa kejahatan cyber berupa phishing bertujuan untuk memperoleh informasi sensitif, seperti nama pengguna, kata sandi bahkan detail kartu kredit. Serangan Phising umumnya menargetkan pengguna layanan

¹¹ Yulianti, N. P. R., & Pramita, K. D. (2022). "Analysis of Workload, Rest Rights, and the Rights to Enjoy Entertainment in Gender Differences". *Jurnal Komunikasi Hukum (JKH)*, Vol 8, No 1, Halaman 471.

¹² Sari, N. W. (2018). "Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer". *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*. Vol 5, No 2, Halaman 580.

¹³ Arif, E., & Roem, E. R. (2019). "Pemanfaatan media sosial". *Jurnal Ranah Komunikasi (JRK)*, Vol 3 No 1, Halaman 34-44.

¹⁴ Hashim, N., & Razali, A. (2019). "Teknologi dan media sosial dalam komunikasi ibubapa dan anak-anak. *Jurnal Komunikasi: Malaysian Journal of Communication*". Vol 35, No 4, Halaman 337-339.

online banking, pelaku dapat mengetahui pengguna online lainnya jika mereka memasukkan isian data pengguna (ID) dan kata sandi mereka ke formulir login yang palsu, baik dalam aplikasi maupun di internet.¹⁵ Phishing biasanya dilakukan dengan menggunakan platform digital yang terhubung dengan internet, seperti melalui email/SMS, situs web dan media sosial.¹⁶ Berikut beberapa contoh platform digital yang populer saat ini antara lain seperti, Facebook, YouTube, Twitter, Blog, WhatsApp, Telegram dan Instagram dan masih banyak lagi.¹⁷

Saat ini phishing dapat terjadi di berbagai platform digital termasuk media sosial, maupun situs web. Tingginya penggunaan aplikasi WhatsApp oleh masyarakat, celah ini dimanfaatkan oleh pelaku untuk melakukan aksi kejahatan cyber crime dengan memanfaatkan kepercayaan dan kelengahan pengguna media sosial.¹⁸

Modus Pelaku kejahatan melancarkan aksinya dengan mengirimkan berbagai tautan atau link yang sering diakses pengguna WhatsApp, seperti link undangan yg merujuk ke suatu website/domain, file PDF dan aplikasi (APK), yang mengatasnamakan instansi/organisasi, yang dipercayai oleh korban. Dengan menyamar sebagai identitas tertentu, para pelaku phishing berupaya mengecoh korban untuk memberikan informasi pribadi atau sendiri dengan membujuk

¹⁵ Malunsenge, L., Massie, C., & Rorie, R. (2022). "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phishing Di Indonesia". *Lex Crimen*, Vol 11, No 3. Halaman 70-71.

¹⁶ Putra, I. K. O. K., Darmawan, I. M. A., & Juliana, I. P. G. (2023). "Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phishing". *Cyber Security Dan Forensik Digital*, Vol 5 No 2, Halaman 77.

¹⁷ Hashim, N., & Razali, A. *Loc. Cit.*

¹⁸ Putra, I. K. O. K., Darmawan, I. M. A., & Juliana, I. P. G. *Loc. cit.*

korban agar mengklik tautan atau mengunduh sebuah file berbahaya yang telah dikirimkan oleh pelaku sebelumnya, mengingat bahwa WhatsApp merupakan salah satu platform digital yang populer saat ini, tidak dapat dipungkiri kalau WhatsApp menjadi salah satu platform digital yang menjadi target kejahatan cybercrime dalam bentuk phishing.¹⁹ Salah satu contoh kasus phishing yang menonjol di Indonesia adalah kasus penipuan melalui WhatsApp yang terjadi pada tahun 2020. Seorang wanita di Jakarta menerima pesan dari seseorang yang mengaku sebagai perwakilan dari sebuah bank ternama. Pesan tersebut berisi informasi bahwa rekening bank miliknya mengalami masalah keamanan dan diminta untuk mengklik tautan yang disediakan untuk memverifikasi identitasnya dan mengamankan akun.²⁰

Tanpa curiga, wanita tersebut mengklik tautan tersebut dan diarahkan ke situs web yang terlihat persis seperti situs resmi bank. Di situs tersebut, dia diminta untuk memasukkan informasi pribadi dan data login rekening bank. Setelah informasi tersebut dimasukkan. Lalu pelaku melakukan aksinya dengan memanfaatkan data tersebut untuk mengakses dan menguras dana dari rekening bank korban.²¹ Dalam perspektif hukum Islam apabila dihubungkan dengan

¹⁹ Prastya, (2024). "Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Review Metode Studi Literatur. Jurnal Nasional Komputasi dan Teknologi Informasi". JNKTI, Vol 7, No 3. Halaman 193

²⁰ Isadora, et.al. (2024). "Analisis Modus Phishing Whatsapp". Jurnal Akuntansi, Bisnis dan Ekonomi Indonesia. Vol 3. No 2, Halaman 45.

²¹ Rita Puspita Sari, 2024. "*Waspada! Ancaman Phishing Lewat WhatsApp, Bisa Bobol Rekening*". <https://www.cloudcomputing.id/berita/phishing-lewat-whatsapp>. diakses 4 Januari 2025, pukul 06:36 WIB.

tindak pidana cybercrime dalam bentuk phishing yang dapat dikategorikan salah satu tindak kejahatan yang membohongi ataupun menipu korban.

QS. Al Baqarah ayat 10

فِي قُلُوبِهِمْ مَّرَضٌ فَزَادَهُمُ اللَّهُ مَرَضًا وَلَهُمْ عَذَابٌ أَلِيمٌ ۖ بِمَا كَانُوا يَكْذِبُونَ

Artinya : Dalam hati mereka ada penyakit, lalu Allah menambah penyakitnya itu; dan mereka mendapat azab yang pedih, karena mereka berdusta.

Rasulullah SAW bersabda,

"Jauhilah kebohongan, sebab kebohongan menggiring kepada keburukan, dan keburukan akan menggiring kepada neraka'. HR Abu Dawud.

Rasulullah SAW bersabda,

Dari Abu Wail dari Abdullah ia berkata, "Rasulullah Saw bersabda: "Jauhilah kebohongan, sebab kebohongan menggiring kepada keburukan, dan keburukan akan menggiring kepada neraka. Dan sungguh, jika seseorang berbohong dan terbiasa dalam kebohongan hingga di sisi Allah ia akan ditulis sebagai seorang pembohong. Dan hendaklah kalian jujur, sebab jujur menggiring kepada kebaikan, dan kebaikan akan menggiring kepada surga. Dan sungguh, jika seseorang berlaku jujur dan terbiasa dalam kejujuran hingga di sisi Allah ia akan ditulis sebagai orang yang jujur."

Terkait dengan pengaturan pidana terhadap kejahatan siber di Indonesia, hingga saat ini sebagian besar tindak pidana siber di Indonesia belum diatur secara norma hukum yang jelas ataupun secara eksplisit dalam peraturan perundang-undangan.²²

Tindakan phishing dapat dikualifikasikan sebagai perbuatan yang melanggar hukum, berdasarkan pasal 28 ayat (1) Jo pasal 45A ayat (1) Undang

²² Koto, I. (2021). "Cyber crime according to the ITE law. International Journal Reglement & Society". IJRS, Vol 2. No 2. Halaman 109.

undang No 1 tahun 2024 tentang perubahan kedua atas Undang-undang No 11 tahun 2008 Informasi dan transaksi elektronik (UU ITE). Hal ini disebabkan karena phishing mengandung unsur kebohongan yang menyesatkan korban, yang mana pelaku mengarahkan korban ke situs palsu melalui tautan/link tertentu dan memerintahkan korban untuk mengisi form informasi pribadi dalam website tersebut.²³ Cyber crime berupa phishing adalah salah satu kejahatan cybercrime dengan melakukan manipulasi ataupun menciptakan website palsu yang tampilannya menyerupai seperti website aslinya.²⁴

Berdasarkan pada uraian yang sudah disampaikan penulis diatas, Maka cukuplah penulis untuk menyusun skripsi dengan judul, **"Pertanggungjawaban pidana siber phishing dengan menggunakan platform digital whatsApp.**

1. Rumusan Masalah

Berdasarkan uraian yang telah dipaparkan pada latar belakang penelitian, terdapat beberapa pokok permasalahan yang menjadi titik fokus dan batasan dalam ruang lingkup pembahasan pada penelitian ini. Adapun yang menjadi permasalahannya antara lain:

²³ Devi, N. A. R. 2023. Kejahatan phishing dengan modus link undangan pernikahan di sosial media menurut undang undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (Doctoral dissertation, UNIVERSITAS SINTUWU MAROSO).

²⁴ Ferrary, A. A. I., Hartini, S., & Purwaningsih, P. (2023). "kajian hukum terhadap tindak pidana cyber phishing yang digunakan untuk mengambil data pribadi pada situs trading dihubungkan dengan undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi transaksi dan elektronik". Jurnal: Yustisi volume 10, No 2, Halaman 1-12.

- a. Apa saja penyebab terjadinya tindak pidana siber phising dengan menggunakan platform digital WhatsApp?
- b. Bagaimana pengaturan hukum tindak pidana siber phising dengan menggunakan platform WhatsApp?
- c. Bagaimana bentuk perlindungan hukum terhadap korban tindak pidana siber phising dengan menggunakan platform digital WhatsApp?

2. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dikemukakan, maka tujuan daripada penelitian ini rumuskan sebagai berikut:

- a. Mampu memahami penyebab terjadinya tindak Pidana siber phising dengan menggunakan platform digital WhatsApp.
- b. Dapat memahami pengaturan hukum tindak Pidana siber phising dengan menggunakan platform digital WhatsApp.
- c. Mampu memahami bentuk perlindungan hukum terhadap korban tindak pidana siber phising dengan menggunakan platform digital WhatsApp.

3. Manfaat Penelitian

Adapun manfaat yang diharapkan dalam penelitian ini terbagi ke dalam dua aspek utama yakni:

- a. Secara teoritis, penelitian ini diharapkan dapat memberikan pemahaman terkait teori dan konsep dalam hukum positif di Indonesia, khususnya aturan yang mengatur dalam hal pertanggungjawaban pidana siber phising dalam menggunakan platform digital media sosial whatsapp dengan tujuan

mengeksploitasi data pribadi. Selain itu penelitian ini cukup berperan penting dalam mengembangkan daya pikir kritis dan khususnya dalam ruang lingkup di bidang hukum pidana, guna mengungkap sebuah permasalahan secara objektif melalui pendekatan ilmiah. Hal ini menjadi cukup penting dalam upaya menemukan solusi atas berbagai persoalan yang berkaitan dengan hukum pidana

- b. Secara praktisi, Dalam penelitian ini dapat memberikan jawaban atas permasalahan yang diteliti kemudian dapat mengembangkan pola pikir, penalaran dan pengetahuan penulis dalam menyusun suatu penulisan hukum dan juga diharapkan dapat memberikan kontribusi positif bagi para penegak hukum, mahasiswa maupun masyarakat umum, dalam memahami dan mengantisipasi perbuatan phishing sebagai salah satu kejahatan siber

B. Definisi Operasional

Definisi operasional merupakan suatu struktur sistematis yang merumuskan keterkaitan antara definisi-definisi dari sebuah konsep-konsep spesifik yang menjadi fokus penelitian, kerangka ini berfungsi sebagai landasan untuk memperjelas arah analisis yang akan diteliti.²⁵ Maka dengan ini dapat dijelaskan tentang definisi operasional sebagai berikut:

1. Pertanggungjawaban pidana merupakan bentuk pertanggungjawaban hukum yang dikenakan terhadap seseorang atas sebuah tindak pidana yang dilakukannya. Dengan kata lain, yang dipertanggungjawabkan oleh tersangka

²⁵ Ida Hanifah, et.al, 2018, *Pedoman Penulisan Tugas Akhir Mahasiswa*, Medan: CV. Pustaka Prima, Halaman 17.

atau pelaku adalah perbuatan pidana yang telah terjadi. pertanggungjawaban ini muncul apabila seseorang terbukti melakukan perbuatan-perbuatan yang melanggar hukum, disertai dengan sebuah unsur kesalahan dan dapat dinilai mampu bertanggung jawab atas perbuatannya.²⁶

2. WhatsApp merupakan salah satu aplikasi yang berbasis internet dari pesatnya perkembangan teknologi informasi dan komunikasi serta juga menjadi salah satu platform paling populer di era digital saat ini. Aplikasi ini menawarkan kemudahan interaksi antara pengguna secara cepat dan efisien, tanpa memerlukan biaya tinggi, karena penggunaannya tidak semata-mata menggunakan pulsa melainkan menggunakan koneksi data internet. Hal ini menjadikan WhatsApp sebagai media komunikasi yang cukup potensial dan cukup efektif dalam mendukung aktivitas sehari-hari.²⁷ WhatsApp dianggap sebagai aplikasi perpesanan seluler.²⁸
3. Cyber crime, Cyber crime adalah istilah yang merujuk pada suatu bentuk kejahatan yang memanfaatkan perangkat komputer dengan menggunakan jaringan internet sebagai media utamanya. Mekanisme kejahatan seperti ini dapat dilakukan dengan berbagai cara dan metode, mulai dari pencurian data maupun penipuan digital.²⁹ Esensi dari kejahatan siber terpusat pada upaya

²⁶ H. Ishaq, 2020, *Hukum pidana*, Depok: PT RajaGrafindo Persada, Halaman 94.

²⁷ Ryan, D, & Zulfah, Z. (2021). "Peningkatan minat belajar siswa melalui pembelajaran e-learning via Whatsapp Di Kelas X MIPA madrasah aliyah Hasanah Pekanbaru". *Journal on: Education*, Vol. 3. No.2, Halaman 200.

²⁸ Omar, M. N. A. (2021). "The impact of using WhatsApp groups on the Palestinian university students' productive skills improvement". (Doctoral dissertation, Master's thesis, An-Najah National University).

²⁹ Hani Dwiwahyu Oktavia, 2021, *Cybercrime*, pubhtml5.com, Halaman 2

yang merusak atau mengancam kerahasiaan, integritas serta ketersediaan data dan sistem komputer yang menjadi pondasi utama dalam dunia digital.³⁰ setiap perbuatan yang dilakukan oleh pelaku kejahatan siber tergolong sebagai perbuatan ilegal, dengan tujuan utamanya yang umumnya mengarah pada pelanggaran terhadap sistem keamanan komputer serta upaya memperoleh akses terhadap data yang bersifat rahasia tanpa izin.³¹

4. Cyber Phising, Secara definisi, phising merupakan suatu upaya penipuan yang bertujuan untuk memperoleh data sensitif atau pribadi seperti nama pengguna, kata sandi maupun detail kartu kredit dengan mengaku sebagai pihak resmi yang dipercayai oleh korban. Dalam hal ini kerugian korban bukan hanya kehilangan data tetapi terancam mengalami kerugian finansial.³² Kejahatan ini sangat bergantung pada akses internet mengingat mekanisme mereka yang memanfaatkan sebuah kecanggihan teknologi.³³

C. Keaslian Penelitian

Keaslian dalam penelitian berdasarkan pada penelitian-penelitian terdahulu yang mempunyai karakteristik yang relatif sama dalam hal tema kajian namun berbeda dalam hal substansi, pembahasan dan objek penelitian. Berdasarkan hasil dari Studi literatur melalui kepustakaa Universitas Muhammadiyah Sumatera Utara dan Perguruan Tinggi lainnya, belum ditemukan

³⁰ Silalahi, F. D. 2022. *Keamanan Cyber (Cyber Security)*. Semarang: Penerbit Yayasan Prima Agus Teknik, Halaman 251.

³¹ Hani Dwiwahyu Oktavia, *Loc.Cit*.

³² Rahmawati, D., *et.al*. 2024. *Waspada Kejahatan Phishing Attack*, Malang: PT. Literasi Nusantara Abadi Grup, Halaman 3-4.

³³ Farid, W, Lubis, U. S., & Susanti, D. 2023, *Hukum Arbitrase dan Alternatif Penyelesaian Sengketa Bisnis: dilengkapi arbitrase online dan arbitrase syariah*, Jakarta: Sinar Grafika, Halaman 171

adanya penelitian sejenis yang membahas topik ini secara spesifik dengan pokok bahasan yang diteliti berjudul "Pertanggungjawaban Pidana Cyber Phising Dengan Menggunakan Platform Digital WhatsApp.

Dari beberapa judul penelitian yang telah dilakukan sebelumnya, terdapat dua judul yang hampir memiliki kesamaan atau relevansi dalam penelitian ini yakni:

1. Syabilah Yuka Kawandoda NIM 04020170376 Mahasiswi Program Studi Hukum Pidana Fakultas Hukum Universitas Muslim Indonesia Makassar tahun 2022 yang berjudul "Penanggulangan kejahatan cyber crime yang dilakukan oleh hacker dalam tinjauan hukum internasional". Yang menjadi perbedaan adalah pada penelitian sebelumnya meneliti tentang Penanggulangan kejahatan cyber crime yang dilakukan oleh hacker dalam tinjauan hukum internasional sementara pada penelitian ini mengkaji bagaimana pertanggungjawaban pidana cyber phising dengan menggunakan platform digital WhatsApp.
2. Dinda Aulia NPM 1906200378 Mahasiswi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara tahun 2024 yang berjudul "Tinjauan Kriminologi Mengenai Kejahatan Dunia Maya Bermodus Pengelabuan (Phising) Dalam Bentuk Pengiriman Link". yang menjadi perbedaan terletak adalah pada penelitian sebelumnya meneliti tentang tinjauan kriminologi mengenai kejahatan dunia maya bermodus pengelabuan (phising) dalam bentuk pengiriman link", sementara peneliti mengkaji tentang

pertanggungjawaban tindak pidana cyber phising dengan menggunakan platform digital WhatsApp.

Secara konstruktif, substansi dan fokus pembahasan dari kedua penelitian tersebut menunjukkan perbedaan yang cukup jelas dibandingkan dengan penelitian ini, khususnya dalam kajian topik yang diangkat oleh penulis, dalam skripsi ini mengarah kepada pertanggungjawaban tindak pidana siber phising dengan menggunakan platform digital WhatsApp yang dalam pembahasan akan membahas tentang bagaimana bentuk pertanggungjawaban tindak pidana cyber phising dengan menggunakan platform digital WhatsApp

D. Metode Penelitian

Penelitian merupakan serangkaian kegiatan ilmiah yang disusun secara sistematis dengan menggunakan metode ilmiah guna mengkaji dan memecahkan masalah suatu permasalahan, serta guna menemukan kebenaran atau fakta fakta yang tujuan utama adalah untuk menjelaskan secara jelas bagaimana proses penelitian dilakukan agar menghasilkan temuan yang faktual.³⁴

Metode penelitian berfungsi sebagai alat untuk mengetahui dan memahami sesuatu permasalahan yang akan diteliti, baik dalam ilmu sosial, hukum, maupun disiplin ilmu lainnya.³⁵ Untuk memperoleh hasil penelitian yang lebih optimal, maka dari itu penelitian ini menggunakan metode sebagai berikut:

³⁴ Idan Hanifah, *et.al*, *Op.Cit.*, Halaman 19.

³⁵ Zainuddin Ali. 2019. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika. Halaman 21.

1. Jenis Penelitian

Jenis penelitian yang digunakan pada penelitian ini adalah hukum normatif (yuridis normatif), yaitu berfokus pada pengkajian terhadap peraturan yang tertulis dan bahan hukum lainnya, penelitian ini lebih banyak menggunakan data sekunder yang diperoleh melalui studi kepustakaan sebagai sumber utama analisis. Sesuai sebagaimana yang dinyatakan oleh Soerjono Soekanto dan Srimahmudji yang dikutip dalam karya Muhaimin, penelitian hukum Normatif diartikan sebagai penelitian hukum yang dilakukan dengan cara meneliti bahan kepustakaan (bahan sekunder). Oleh karena itu, Penelitian ini disebut sebagai penelitian yuridis normatif atau penelitian hukum kepustakaan.³⁶

2. Sifat Penelitian

Penelitian hukum bertujuan untuk dan menggambarkan kondisi serta karakteristik norma hukum, termasuk juga bagaimana norma tersebut berfungsi di dalam kehidupan masyarakat, berdasarkan tujuan tersebut, maka penelitian ini bersifat deskriptif yaitu bertujuan untuk memberikan gambaran yang sistematis dan faktual mengenai objek atau peristiwa hukum.³⁷

3. Pendekatan Penelitian

Dalam penelitian ini menggunakan pendekatan perundangan undangan (Statute approach) dan pendekatan konseptual (Conceptual approach). Sebagaimana yang dijelaskan oleh Peter Mahmud Marzuki, dimana pendekatan

³⁶ Muhaimin. 2020. *Metode Penelitian Hukum*. Mataram: Mataram University Press, Halaman 19.

³⁷ Idah Hanifah, *et.al*, *Op.Cit.*, Halaman 20.

perundangan undangan dilakukan dengan menelaah secara keseluruhan peraturan perundangan undangan dan regulasi yang relevan dengan isu hukum yang akan di kaji. Sementara itu, pendekatan konseptual merupakan pandangan pandangan teoritis dan doktrin-doktrin yang berkembang dalam ilmu hukum yang akan diteliti.³⁸

4. Sumber Data Penelitian

Sumber data yang dapat digunakan dalam penelitian hukum ini terdiri sebagai berikut:

1. Data yang bersumber dari hukum islam: yaitu Al-Qur'an dan Hadist. Data yang bersumber dari hukum Islam kerap disebut sebagai data kewahyuan, Dalam konteks penelitian ini, data tersebut merupakan dalam bentuk berupa ayat-ayat Alqur'an yang dijadikan sebagai landasan untuk mengkaji, menganalisis dan menjawab atas permasalahan yang diangkat atau diteliti.
2. Data sekunder, merupakan data yang diperoleh melalui studi kepustakaan yang mencakup berbagai sumber resmi dan literatur hukum, seperti dokumen dokumen resmi, publikasi hukum yang meliputi kamus-kamus hukum, buku-buku, jurnal ilmiah, serta yurisprudensi dan peraturan perundangan-undangan yang relevan.³⁹

Data sekunder yang digunakan pada penelitian ini terdiri dari:

³⁸ Muhaimin. 2020, *Op.cit.*, Halaman 57.

³⁹ Idah Hanifah, *et.al, Loc.Cit*,

1. Bahan hukum primer, yaitu bahan hukum yang mengikat.⁴⁰ Yang dalam penelitian ini terdiri dari Perundangan undangan seperti, Undang-undang No 27 tahun 2022 tentang perlindungan data pribadi dan Undang-undang No 1 tahun 2024 tentang perubahan kedua atas undang-undang no 11 tahun 2008 tentang informasi dan transaksi elektronik dll.
2. Bahan hukum sekunder adalah segala bentuk literatur yang memberikan penjelasan ataupun pemahaman terhadap bahan hukum primer, bahan ini mencakup publikasi-publikasi hukum seperti buku-buku teks, hasil penelitian, artikel ilmiah dan karya akademik lainnya yang relevan dengan permasalahan yang akan dikaji pada penelitian ini.
3. Bahan hukum tersier merupakan sumber yang memberikan penjelasan atau pemahaman tambahan terhadap bahan hukum primer dan sekunder, antara lain meliputi seperti kamus hukum, ensiklopedia, internet dan berbagai referensi penunjang lainnya.⁴¹

5. Alat Pengumpul Data

Dalam penelitian ini, data diperoleh dari sumber primer dan sekunder dengan menggunakan instrumen atau alat pengumpul data, yakni;

- a. Offline, yaitu dengan menghimpun data studi kepustakaan (library research) secara langsung dengan mengunjungi toko-toko buku, perpustakaan kampus

⁴⁰ Amiruddin dan H.Zainal Asikin, 2004, *Pengantar Metode Penelitian Hukum*, PT Raja Grafindo Persada, Jakarta, Halaman. 118-119.

⁴¹ *Ibid.*, Halaman 121.

Universitas Muhammadiyah Sumatera Utara atau kampus lain. Untuk menghimpun data sekunder yang cukup relevan, seperti buku buku hukum, dokumen resmi, jurnal ilmiah, peraturan perundangan undangan, serta sumber literatur lainnya yang mendukung penelitian ini.

- b. Online, yaitu studi kepustakaan (library research) yang dilakukan secara daring melalui penelusuran berbagai sumber digital di internet untuk menghimpun data yang relevan untuk mendukung penelitian ini.⁴²

6. Analisis Data

Analisis data dalam penelitian ini menggunakan analisis kualitatif yaitu memaparkan data secara keseluruhan yang dinyatakan secara baik, lengkap, jelas, sistematis, akurat dan efektif.⁴³

⁴² *Ibid.*, Halaman 21.

⁴³ *Ibid.*, Halaman 22.

BAB II

TINJAUAN PUSTAKA

A. Pertanggungjawaban pidana

Dalam kehidupan, suatu tindak kejahatan dapat terjadi akibat adanya gesekan kepentingan yang dialami oleh individu atau kelompok.⁴⁴ Kejahatan dalam kehidupan masyarakat ada berbagai macam jenisnya tergantung pada sasaran kejahatannya.⁴⁵ Istilah Pertanggungjawaban pidana dalam bahasa Belanda *torekenbaarheid*, dan dalam bahasa Inggris disebut *criminal responsibility* atau *criminal liability*, yang merujuk kepada pemberian sanksi kepada pelaku tindak Pidana atas perbuatan melanggar hukum. Dengan kata lain, Pertanggungjawaban pidana berkaitan dengan proses hukuman kepada pelaku yang bertanggung jawab atas perbuatan tersebut.⁴⁶

Dalam undang-undang hukum pidana, termuat dalam pasal 36 yang menyatakan bahwa, "pertanggungjawaban pidana adalah diteruskannya celaan yang objektif yang ada pada tindak pidana dan celaan subjektif kepada seseorang yang memenuhi syarat untuk dapat dijatuhi pidana kerana perbuatannya itu".⁴⁷

Jika membahas pertanggungjawaban pidana maka unsur, "kesalahan" tidak bisa dipisahkan. Dalam hukum pidana dikenal asal paling fundamental, yakni, "Tiada Pidana Tanpa Kesalahan", yang dalam istilah asing disebut, *Keine*

⁴⁴ Aristo M.A. Pangaribuan, *et.al.* 2020. *Pengantar Hukum Acara Pidana Di Indonesia*. Depok: Rajawali Pers. Halaman 1.

⁴⁵ Koto, I. & Faisal. 2022. *Hukum Perlindungan Saksi dan Korban*. Medan: Umsu press. Halaman 57

⁴⁶ Fadlian, A. (2020). "Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis". *Jurnal: Hukum Positum*, Vol 5, No 2, Halaman 14.

⁴⁷ H. Ishaq, *Op.Cit.*, Halaman 94-95.

Strafe ohne schuld, geen straf, zonder schuld atau *nulla poena sine culpa*, Asas ini menegaskan bahwasannya seseorang hanya bisa dipidana jika ia benar benar bersalah. Maka dapat dipahami bahwa kesalahan adalah syarat utama agar seseorang bisa dimintai pertanggungjawaban pidana.⁴⁸

Seorang pelaku hanya dapat dimintai pertanggungjawaban pidana jika ia memiliki kemampuan untuk bertanggung jawab. Dengan kata lain, pertanggungjawaban pidana mensyaratkan adanya kemampuan bertanggung jawab (*toerekeningsvatbaarheid*) dari si pembuat atau pelaku. Walaupun demikian, dalam hukum tidak secara tegas merumuskan syarat ini sehingga penjelasannya harus dicari melalui doktrin atau *memorie Van teolichting*.⁴⁹

Menurut Simons yang menyatakan bahwa, "kemampuan bertanggung jawab adalah suatu kondisi kejiwaan tertentu yang memungkinkan seseorang dapat dikenakan sanksi pidana. Dapat dipahami bahwasanya, pembedaan hanya dapat diterapkan apabila seseorang berada dalam keadaan psikis yang sehat yakni apabila:⁵⁰

1. Ia memiliki kesadaran yang cukup untuk memahami bahwa perbuatannya melanggar norma hukum yang berlaku.
2. Ia memiliki kemampuan untuk mengendalikan kehendaknya berdasarkan pemahaman terhadap norma hukum yang disadarinya.

⁴⁸ Tofik Yanuar Chandra. 2022. "*Hukum Pidana*". Jakarta: PT Sangir Multi Usaha. Halaman 68.

⁴⁹ Suyanto. 2018. *Pengantar Hukum Pidana*. Yogyakarta: Deepublish Publisher. Halaman 77.

⁵⁰ *Ibid.*, Halaman 77.

Untuk menetapkan adanya kesalahan perbuatan dalam hukum pidana, subjek hukum harus memenuhi sejumlah unsur tertentu, antara lain:⁵¹

1. Adanya kemampuan untuk mempertanggungjawabkan perbuatan tersebut, yang artinya pelaku berada dalam kondisi kejiwaan yang normal dan mampu memahami serta mengendalikan tindakannya.
2. Terdapat hubungan batin pelaku dengan perbuatannya, yang diwujudkan dengan kesengajaan (*dolus*) atau kealpaan (*culpa*)
3. Tidak terdapat alasan pemaaf yang dapat menghapuskan kesalahan pelaku atas perbuatannya.

Menurut Sutorius dalam tulisannya berjudul *Het Schuldbeginssel/Opzet en de Varianten Daarvan*, mengatakan: "bahwa orang tidak dapat bicara tentang kesalahan tanpa adanya perbuatan tercela atau kedaan yang tidak patut. Oleh karena itu, Asas "tiada pidana tanpa kesalahan", berarti bahwa tidak boleh ada hukuman jika tidak ada perbuatan tercela yang secara objektif bisa dipersalahkan kepada pelakunya. Kesalahan dapat dilihat sebagai hubungan antara pelaku dan perbuatannya, dimana perbuatan tersebut benar-benar berasal dari diri pelaku."⁵²

Dalam hal ini, Roeslan Saleh Berpendapat:⁵³

"bahwa untuk menentukan adanya kemampuan bertanggungjawab itu ditentukan pertama-tama oleh akal, yaitu dapat atau mampu membedakan antara perbuatan yang diperbolehkan dan yang tidak diperbolehkan. Tetapi mengenai faktor kedua, yaitu faktor kehendak

⁵¹ Taufik Yanuar Chandra, *Op.cit.*, Hal 70-71.

⁵² Lukman Hakim. 2020. *Asas Hukum Pidana: Buku Ajar Bagi Mahasiswa*. Yogyakarta: Deepublish. Halaman 52.

⁵³ *Ibid.*, Halaman 40.

bukanlah merupakan faktor dalam menentukan mampu tidaknya orang bertanggungjawab".

Dikatakan demikian, karena menurut Roeslan Saleh:

"kehendak itu bergantung dan merupakan kelanjutan saja dari akal, yaitu bilamana akalnya sehat dan normal, artinya bilamana seorang itu mampu membedakan antara perbuatan yang diperbolehkan dan yang tidak diperbolehkan, maka oleh hukum diharuskanlah orang itu menentukan kehendaknya sesuai dengan yang diperbolehkan oleh hukum. Karenanya faktor kehendak bukanlah merupakan faktor yang menentukan kemampuan bertanggungjawab, yaitu yang menentukan mampu atau tidaknya bertanggungjawab, melainkan hanya merupakan salah satu faktor yang ikut menentukan kesalahan, yaitu salah satu unsur dari kesalahan".⁵⁴

Pertanggungjawaban pidana dimaksudkan sebagai dasar untuk menentukan layak atau tidaknya seseorang, sebagai tersangka atau terdakwa yang dimintai pertanggungjawaban atas suatu perbuatan yang dikualifikasikan sebagai tindak Pidana.⁵⁵ Menurut aliran monisme tindak pidana terdiri dari dua unsur utama, yaitu unsur objektif (perbuatan) dan unsur subjektif (pelaku). Dimana kedua unsur ini dipandang sebagai satu kesatuan dan tidak dapat dipisahkan.⁵⁶

B. WhatsApp

Aplikasi WhatsApp didirikan pada 24 Februari 2009 oleh Jan Koum dan Brian Acton. Nama WhatsApp merupakan plesetan dari kata "*What's Up?*", yang mencerminkan gaya komunikasi santai dan cepat sebagai aplikasi chatting. WhatsApp terhubung langsung dengan nomor telepon dan bisa digunakan secara

⁵⁴ *Ibid.*, Halaman 41.

⁵⁵ Itri Wahyuni. 2017. *Dasar-dasar hukum pidana di Indonesia*. Tangerang: Nusantara Persada Utama, Halaman 67.

⁵⁶ Lukman Hakim, *Op.cit.*, Halaman 43.

gratis hanya bermodalkan kuota internet, dengan ukurannya yang ringan tidak membebani memori ponsel. WhatsApp menjadi pilihan favorit jutaan pengguna di seluruh dunia.⁵⁷

WhatsApp merupakan aplikasi berbasis messenger yang memungkinkan penggunanya mengirim pesan. WhatsApp juga termasuk dalam kategori media sosial karena bisa digunakan untuk berkomunikasi dengan banyak orang.⁵⁸

WhatsApp messenger adalah aplikasi pesan yang bisa digunakan di berbagai perangkat dan memungkinkan kita mengirimkan pesan secara gratis.⁵⁹ Kita dapat mengirimkan file dokumen, file foto, video call, lokasi GPS dan lain-lain.⁶⁰ karena aplikasi Whatsapp Massanger menggunakan akses data internet dalam pengoperasiannya⁶¹

Whatsapp menjadi salah satu media sosial yang paling populer yang digunakan oleh masyarakat Indonesia. Penggunaan whatsapp sebagai media sosial hampir sering digunakan orang dalam kehidupan sehari-hari.⁶²

⁵⁷ Suryani, R. (2017). Fungsi Whatsapp Grup Shalihah Cabang Bandar Lampung Sebagai Pengembangan Media Dakwah Dalam Membentuk Akhlakul Karimah (Doctoral dissertation, UIN Raden Intan Lampung).

⁵⁸ Indriyani, E., & Suliworo, D. (2018). "Dampak pemanfaatan WhatsApp dalam meningkatkan motivasi belajar siswa pada pelajaran fisika". In Seminar Nasional Quantum. Vol. 25, No.2, Halaman 27.

⁵⁹ Suryani, R. (2017). "Fungsi Whatsapp Grup Shalihah Cabang Bandar Lampung Sebagai Pengembangan Media Dakwah Dalam Membentuk Akhlakul Karimah". (Doctoral dissertation, UIN Raden Intan Lampung. Halaman 18.

⁶⁰ Shodiq, I. J. F., & Zainiyati, H. S. (2020). "Pemanfaatan media pembelajaran E-Learning menggunakan Whatsapp sebagai solusi ditengah penyebaran Covid-19 di MI Nurulhuda Jelu". Al-Insyiroh: Jurnal Studi Keislaman, Vol 6. No 2. Halaman 151.

⁶¹ Suryani, R. *Loc. Cit.*

⁶² Koten, F. P. N., Jufriansah, A., & Hikmatiar, H. (2022). "Analisis penggunaan aplikasi Whatsapp sebagai media informasi dalam pembelajaran: Literature review". Jurnal Ilmu Pendidikan: STKIP Kusuma Negara, Vol. 14. No. 1, Halaman 74.

Adapun Manfaat Penggunaan WhatsApp sebagai berikut:

1. Whatsapp merupakan sebuah aplikasi yang dapat diakses dengan gratis. .
2. Whatsapp menyediakan berbagai fitur, di antaranya kemampuan untuk mengirimkan pesan teks, gambar, video, pesan teks, rekaman suara, dokumen serta berbagai lokasi GPS secara real-time.
3. Whatsapp dilengkapi berbagai fitur yang dimilikinya, WhatsApp menjadi sarana yang efektif untuk mendistribusikan informasi dan pengetahuan secara mudah dan masif.⁶³

Berbagai keunggulan yang diberikan WhatsApp menjadikannya sebagai salah satu platform digital paling populer saat ini, beriku beberapa keunggulannya: Aplikasi lintas platform, Pesan teks dan panggilan suara gratis, Enkripsi end-to-end, Fitur grup dan siaran, Berbagai lokasi dan kontak, Status dan fitur media sosial dan Integrasi dengan kontak.⁶⁴ Fitur di WhatsApp adalah layanan pesan yang andal dan sederhana. Pengguna dapat mengirim pesan ke teman dan keluarga mereka secara gratis.⁶⁵ Karena WhatsApp menggunakan paket data internet⁶⁶

⁶³ Indaryani, E. & Suliworo. D. (2018). "Dampak Pemanfaatan Dalam Meningkatkan Motivasi Belajar Siswa Pada Pelajaran Fisika". Prosiding Seminar Nasional Quantum. Vol 25, No. 2, Halaman 25.

⁶⁴ Siregar, N. M. (2023). "Pemanfaatan Aplikasi Whatsapps sebagai Media Pembelajaran Prodi Komunikasi Penyiaran Islam (KPI) Fakultas Dakwah Dan Ilmu Komunikasi". Hikmah, Vol.17, No.1, Halaman 154-156.

⁶⁵ Jasrial, D. (2019). "Utilizing WhatsApp application for teaching English language Why and how. unsri: In International Seminar and Annual Meeting" Vol. 1, No. 1, Halaman 152.

⁶⁶ Fadlian, A, Santoso, B, dan Oktaviana, D, 2023, *Cyber crime dalam perkembangan ilmu*, Depok: RajaGrafindo Persada, Halaman 53

C. Cyber Crime

Dalam arti sempit, *Cybercrime* dikenal sebagai *computer crime*, yaitu pelanggaran hukum yang dilakukan dengan menyerang langsung sistem keamanan komputer atau data yang sedang diproses. Selain itu dalam arti luas *Cybercrime* disebut *computer-related crime*, yaitu pelanggaran yang dilakukan dengan melibatkan sistem komputer atau jaringan.⁶⁷ *Cybercrime* ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia IT khususnya media internet.

Adapun karakteristik cybercrime yaitu:

1. (Against Person) Cybercrime yang menyerang individu.
2. (Against Property) Cybercrime yang menyerang hak cipta / hak milik.
3. (Against Government) Cybercrime yang menyerang pemerintah⁶⁸

Jenis jenis kejahatan *cybercrime* memiliki berbagai klasifikasi, salah satu versi menyebutkan bahwa *cybercrime* terbagi menjadi dua kategori utama, Pertama kejahatan yang bermotif Intelektual yang mana pada umumnya tidak menyebabkan kerugian terhadap korban melainkan dilakukan demi sebuah tantangan dan kepuasan tersendiri. Kedua, kejahatan yang dilandasi oleh motif politik, ekonomi dan kriminal yang bisa berdampak cukup serius, termasuk kerugian besar. secara umum kejahatan *cybercrime* diklasifikasikan menjadi tiga kategori utama, pelanggaran akses terhadap sistem, pencurian data dan

⁶⁷ Ketaren, E. 2016. "Cybercrime, cyber space, dan cyber law". Medan: Jurnal Times, Vol 5, No 2, Halaman 36.

⁶⁸ Ketaren. *Op.Cit.*, Halaman 37.

penyebaran informasi, Philip Renata dalam Suplemen Bistek Warta Ekonomi No. 24 edisi Juli 2000 mengemukakan beberapa bentuk kejahatan siber, antara lain: *"hacking, the Trojan horse, data leakage, data diddling, to frustrate data communication, dan software piracy"*.⁶⁹

Dapat dipahami bahwa pada dasarnya pengertian daripada cybercrime cukup beragam, tetapi pada intinya kejahatan tersebut dilakukan:

1. Dilakukan di dunia maya.
2. Menggunakan jaringan internet baik menggunakan komputer atau perangkat lainnya.
3. Perbuatan tersebut dikategorikan sebagai perbuatan pidana sebagaimana diatur dalam ketentuan undang-undang.⁷⁰

Ada banyak jenis *cybercrime* yang dilakukan. Berikut adalah jenis-jenis kejahatan *cybercrime*.⁷¹

1. *Spamming*. Spam adalah jenis informasi yang tidak diinginkan dan tidak diminta yang dikirimkan secara acak. Umumnya Spam dikirimkan melalui email. Namun, Spam juga dapat disebarluaskan melalui teks, panggilan telepon, atau bahkan jejaring sosial.⁷²

a. *Email spamming*

b. *Instant messaging*

⁶⁹ Nudirman, 2017, *Pengantar Hukum siber Indonesia*, Depok: RajaGrafindo Indonesia, Halaman 64

⁷⁰ *Ibid.*, Halaman 411

⁷¹ Marelino, A. (2022). "Understanding the Types of Cyber Crime and Its Prevention". *Mathematical Statistician and Engineering Applications*, Vol. 71, No.1, Halaman 109

⁷² Jaiswal, M. (2019). "cybercrime categories and prevention". *Manishaben Jaiswal: International Journal of Creative Research Thoughts (IJCRT)*, ISSN, Vol. 7, No.1, Halaman 2329

c. *Messenger spamming*

d. *Forums*

e. *Newsgroups*

f. *Mobile*⁷³

2. *Phishing*. Ini terkait dengan akses ilegal di situs web perbankan untuk meretas akun pengguna, dll. Misalnya, peretas dapat mengirim pesan yang mengatakan untuk mengklik tautan tertentu yang memberikan jaminan kepada korban dan akibatnya pelaku mendapatkan akses mudah ke kata sandi dan rincian login orang tersebut yang dapat digunakan peretas untuk kepentingannya sendiri.
3. *Piracy or Theft*. Jenis kejahatan dunia maya ini terkait dengan pencurian hak cipta milik orang lain. Dalam jenis serangan ini penyerang dapat mengunduh lagu atau film atau musik dan membuat salinan duplikat dan menjualnya dengan harga yang lebih murah.
4. *System Damage*. Jenis serangan cyber ini terkait dengan gangguan terhadap jalannya bisnis. atau organisasi dengan merusak sistem. Dalam jenis serangan cyber ini, peretas akan mengirim virus ke merusak sistem. Jika komputer diakses selama waktu tertentu, maka virus dapat masuk sistem dan dapat merusak kerja sistem dan karenanya mempengaruhi alur kerja bisnis.⁷⁴
5. *Malicious Software*. Ini adalah jenis program perangkat lunak yang digunakan oleh peretas untuk menginfeksi sistem pengguna dan memiliki kemampuan

⁷³ Marelino, *Loc.cit.*

⁷⁴ *Ibid.*, Halaman 109

untuk mengakses sistem dan mendapatkan data penting organisasi. Sasaran utamanya adalah merusak perangkat lunak sistem yang menjadi sasaran peretas.

6. *Fraud calls and messages*. Dalam jenis serangan ini, peretas akan menelepon pengguna dan berpura-pura menjadi orang dari bank dan akan menanyakan beberapa detail untuk mengotorisasi data yang disimpan di bank. Orang tersebut harus terjebak dalam panggilan penipuan semacam itu karena tidak ada bank yang akan meminta detail penting pribadi seperti OTP atau PIN ATM oleh bank.⁷⁵
7. *Dark web market*. istilah baru yang telah diperkenalkan dalam beberapa tahun terakhir yang merujuk pada semua pasar gelap daring yang telah dikembangkan dan beroperasi di lingkungan Dark Web. Pasar daring yang relatif baru ini sangat mirip dengan pasar yang ada di Surface ini melibatkan pemasaran gelap produk ilegal untuk dijual di internet.⁷⁶
8. *Cyber Stalking*. Ini juga salah satu dari banyak jenis kejahatan dunia maya, cyber stalking tidak mengenal batas. Siapa pun bisa menjadi korban penguntitan, baik secara acak atau berdasarkan pada penilaian yang buruk ketika seseorang merilis informasi pribadi di Internet.⁷⁷
9. *Theft of person's identity*. Dalam jenis kejahatan ini, peretas akan meretas identitas orang tersebut dan menggunakan identitasnya untuk menggunakan

⁷⁵ *Ibid.*, Halaman 111

⁷⁶ Kermitsis, et.al, 2021. *Dark web markets. Dark web investigation*, Sheffield: CENTRIC Sheffield Hallam University, Halaman 85

⁷⁷ Pittaro, M. L. (2007). "Cyber stalking An analysis of online harassment and intimidation". *International journal of cyber criminology*, Vol.1, No.2, Halaman 190

pin ATM orang tersebut dan dapat menggunakannya untuk membeli barang-barang yang tersedia secara daring yang akan mengakibatkan kerugian finansial orang tersebut.

10. *Cyber Extortion*. Di sini peretas akan mendapatkan akses ke data penting bisnis atau organisasi dengan meretas sistem. Kemudian peretas akan meminta uang sebagai imbalan atas data yang dicurinya. Hal ini sangat umum terjadi akhir-akhir ini dan banyak perusahaan mengalami kerugian besar dan berada dalam kondisi krisis.⁷⁸

Penegakan hukum terhadap *cybercrime* di Indonesia dipengaruhi oleh beberapa faktor utama, seperti landasan undang-undang, kesiapan mental, serta tidak terlepas juga dari sebuah integritas para penegak hukum dalam menjalankan tugasnya.⁷⁹ *Cyber law* memiliki peran yang sangat krusial dalam mencegah dan menangani tindak pidana di era digital. Hukum ini dapat dikatakan sebagai pondasi utama dalam proses penegakan hukum terhadap berbagai bentuk kejahatan yang memanfaatkan sarana elektronik dan komputer.⁸⁰

Terdapat regulasi yang secara khusus mengatur tentang kejahatan di ranah digital yaitu Adapula Undang-Undang No 1 tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang undang ini memuat ketentuan pidana

⁷⁸ Marelino, *Op.cit.*, Halaman 110

⁷⁹ Marelino, *Loc.,cit.*

⁸⁰ Nurdiman, *Op.cit.*, Halaman 197

yang dirancang menindak berbagai bentuk pelanggaran di dunia siber yang berpotensi mengancam keamanan dan kenyamanan para pengguna internet.⁸¹

D. Cyber Phising

Phishing atau dalam bahasa Indonesia pengelabuan merupakan bentuk penipuan siber yang dilakukan dengan cara menyamar sebagai pihak terpercaya baik mengaku sebagai seorang individu maupun sebagai instansi tertentu. Melalui media komunikasi elektronik khususnya seperti aplikasi WhatsApp atau WhatsApp messenger, dimana pelaku berupaya mencuri informasi pribadi pengguna, seperti kata sandi, data pribadi bahkan tidak terlepas juga guna mendapatkan informasi kartu kredit pengguna.⁸²

Istilah *phishing* dalam bahasa Inggris berasal dari kata *fishing* (memancing), dalam hal ini berarti memancing.⁸³ *Phishing* juga merujuk pada upaya ataupun perbuatan memancing pengguna agar secara tidak sadar memberikan informasi pribadi, seperti nama pengguna dan kata sandi, melalui situs palsu yang dimodifikasi agar terlihat seperti situs resminya. Teknik ini kerap menargetkan pengguna layanan banking online, dimana data yang dimasukkan termasuk informasi kartu kredit dapat dimanfaatkan oleh pelaku untuk membobol

⁸¹ *Ibid.*, Halaman 42.

⁸² Nurdiman, *Op.cit.*, Halaman 218-219

⁸³ Mega, 2023, "*Mengenal Phising, Jenis Kejahatan Cyber yang Berbahaya*", <https://www.megasyariah.co.id/id/artikel/edukasi-tips/lainnya/phising>, diakses pada 4 Januari 2025, pukul 23:33 WIB.

akun dan melakukan transaksi ilegal.⁸⁴ Kejahatan *cracking* atau *cracker* merupakan salah satu jenis kejahatan *phishing*.⁸⁵

Dalam konteks keamanan komputer, *phishing* merupakan penipuan elektronik. Phishing biasanya dilakukan melalui email, situs web palsu, pesan teks, atau media sosial.⁸⁶

Kejahatan Phishing berdasarkan undang-undang No 1 tahun 2024 perubahan kedua atas undang-undang no 11 tahun 2008 tentang informasi dan transaksi elektronik

Pasal 35 juncto Pasal 51 ayat (1) terkait dengan perbuatan pemalsuan dokumen elektronik atau informasi elektronik, yang menyatakan:

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memanipulasi, membuat, mengubah, menghilangkan, memusnahkan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap sebagai data yang autentik."

Selain itu, Pasal 28 ayat (1) jo Pasal 45A ayat (1) juga dapat diterapkan karena phishing termasuk perbuatan menipu dan menyesatkan korbannya.

Pasal 28 ayat (1) menyatakan:

"Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

Kemudian ketentuan ancamannya menurut Pasal 45 ayat (1):

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

⁸⁴ Nurdiman, *Loc.cit*

⁸⁵ Harahap, A. Z., & Marpaung, Z. A. (2024). "Criminal Law Enforcement Against Cyber Phishing Perpetrators". LEGAL BRIEF, Vol 13, No 5, Halaman 1371.

⁸⁶ *Ibid.*, Halaman 1372.

Ketentuan dalam pasal tersebut dapat dikaitkan dengan perkara phishing yang terjadi sesuai dengan putusan Nomor 85/Pid.Sus/2022/PN.Bjb. Unsurnya, “setiap orang” adalah pelaku phishing yang dengan sengaja dan melawan hukum melakukan tindak pidana manipulasi elektronik.⁸⁷

Adapun beberapa jenis phising dalam kejahatan dunia maya, sebagai berikut:

1. *Vhising*

Vishing merupakan bentuk kejahatan siber yang dimana memanfaatkan teknologi suara berbasis IP, Khususnya *voice over* internet protocol (Volp), untuk meniup korban agar memberikan informasi pribadi atau informasi lainnya, demi Keuntungan finansial. Istilah vhising berasal dari kombinasi "voice" dan "phising".⁸⁸

Vishing memanfaatkan kepercayaan seseorang terhadap layanan telepon, karena target biasanya tidak menyadari kemampuan penipu untuk menggunakan teknik seperti pemalsuan ID pemanggil dan sistem otomatis canggih untuk melakukan penipuan semacam ini.⁸⁹ Call centers, Penggunaan pusat panggilan yang luas membuat orang terbiasa dengan panggilan orang

⁸⁷ *Ibid.*, Halaman 1378.

⁸⁸ Yeboah-Boateng, E. O., & Amanor, P. M. (2014). "Phishing, SMiShing & Vishing an assessment of threats against mobile devices". *Journal of Emerging: Trends in Computing and Information Sciences*, Vol.5, No.4, Halaman 300

⁸⁹ *Ibid.*, Halaman 300

asing dan menanyakan detail pribadi. Hal ini juga mengurangi kecurigaan terhadap penipu dengan aksen asing.⁹⁰

2. *Smishing*

Media SMS (*short messenger service*) Ini adalah penggunaan layanan pesan singkat untuk menerapkan serangan phishing. Ada dua pendekatan utama yang menggunakan metodologi ini. Metode pertama melibatkan pengiriman SMS yang berpura-pura menjadi otoritas tepercaya (seperti bank, dll.).⁹¹ SMS yang tampaknya berasal dari bank Anda dan memberi tahu Anda bahwa akun Anda telah diretas dan Anda harus segera menelepon atau menanggapi adalah contoh skenario umum.⁹²

Korban kemudian diarahkan ke situs web atau nomor telepon palsu, yang mengharuskan korban untuk masuk atau memberikan beberapa informasi pengenalan. Setelah ini terjadi, penyerang kemudian dapat menggunakan rincian yang telah mereka kumpulkan untuk keuntungan mereka sendiri. Metode Kedua melibatkan pengiriman teks ke korban yang secara langsung berisi malware atau menyediakan tautan ke situs web yang berisi *malware*. Setelah malware terinstal, phisher dapat melanjutkan serangan mereka, yang bisa

⁹⁰ Alabdan, R. (2020). "Phishing attacks survey Types, vectors, and technical approaches". Journal: Future internet, Vol.12, No.10, Halaman 7

⁹¹ Yeboah, *Op.,cit.* Halaman 299

⁹² Butt, U. et.al. (2023). "Cloud-based email phishing attack using machine and deep learning algorithm". Journal: Complex & Intelligent Systems, Vol.9, No.3, Halaman 3049

berupa sekadar mencuri kontak dan pesan target, untuk membuat bot-net atau mengakses kode otentikasi untuk login atau pembelian.⁹³

3. *Web phishing*

Situs web palsu merupakan sumber serangan phishing lainnya. Situs-situs ini tampak sah dan digunakan untuk mengambil data pribadi korban saat korban mencoba masuk. Berbagai metode dapat digunakan oleh penyerang, karena pengguna internet pada umumnya lebih cenderung percaya bahwa serangan phishing terutama dilakukan melalui email dan layanan pesan lainnya, mereka cenderung kurang memperhatikan keamanan saat mengunjungi situs web, sehingga membuat mereka rentan terhadap jenis serangan phishing ini.⁹⁴

4. Wifi

Phishing Wi-Fi biasanya terjadi di hotspot publik, dan karenanya biasanya merupakan bentuk serangan phishing yang tidak ditargetkan. Namun, cara ini juga berpotensi digunakan dalam serangan spear phishing (atau mungkin *whaling*), di mana hotspot publik tertentu dipilih karena target tertentu secara teratur mengunjungi dan menggunakan Wi-Fi.⁹⁵

Penipuan Wi-Fi dapat terjadi dalam beberapa bentuk. Bentuk yang umum adalah memasang malware pada perangkat korban untuk mengumpulkan kredensial atau mengalihkan ke situs palsu, seperti bentuk penipuan lain yang diuraikan di atas. Ada juga metode yang menyadap lalu lintas pada jaringan

⁹³ Yeboah, *Loc.cit.*

⁹⁴ Alabdan, *Loc.cit.*

⁹⁵ *Ibid.*, Halaman 7

ini untuk mencuri informasi pribadi yang dikirimkan oleh orang-orang yang menggunakan hotspot publik.⁹⁶

5. *Email Phising*

Email *phishing* ini tentu saja merupakan jenis phishing yang paling dikenal luas sejak tahun sembilan puluhan. Ini adalah pesan yang dapat dikirim oleh pengembang perangkat lunak dari akun email mereka secara masal kepada pengguna email. Email tersebut memberi tahu pengirim bahwa informasi pribadi mereka telah diretas dan mereka harus menanggapi sesegera mungkin dengan menekan tautan 'ini'. Sering kali seseorang menggunakan alat penerjemahan untuk membaca lima jenis pesan yang berbeda dan kemudian muncul dalam bahasa Inggris beberapa saat kemudian. Beberapa pesan jauh lebih sulit diidentifikasi sebagai penipuan phishing.⁹⁷

6. *Spear Phising*

Spear phising merupakan varian dari email *phising*, namun dengan pendekatan yang lebih terarah. Berbeda dengan phishing biasa yang dimana pelaku menyebarkan email secara massal dan acak, spear phishing menargetkan individu atau organisasi tertentu. Dalam hal ini pelaku telah mengumpulkan informasi dasar pengguna atau korban, seperti, nama, alamat dan jabatan, sehingga pesan yang dikirim tampak lebih personal dan meyakinkan.

7. *Whaling*

⁹⁶ *Ibid.*, Halaman 7

⁹⁷ Butt., *Op.,cit.* Halaman 3050

Whaling merupakan jenis serangan *Phising* yang menargetkan individu penting dalam sebuah organisasi, serangan dianggap cukup beresiko tinggi karena apabila salah satu jenis *phising* ini berhasil dampaknya bisa sangat besar. contoh kasus nyata seperti di Amerika pada tahun 2016 ketika peretas menyamar sebagai CEO Crelan bank dan mengirimkan sebuah email kepada karyawannya, dengan meminta sejumlah uang agar ditransfer ke rekening tertentu. Karena email tersebut tampak resmi dan berasal dari pimpinan tertinggi, karyawan pun menuruti permintaan tersebut tanpa curiga sedikitpun dan Crelan Bank mengalami kerugian yang cukup besar, sebanyak 75 juta dollar.⁹⁸

⁹⁸ Butt., Loc.cit.

BAB III HASIL PENELITIAN DAN PEMBAHASAN

A. Penyebab Terjadinya Tindak Pidana Siber Phising Dengan Menggunakan Platform Digital WhatsApp.

Keterlibatan sebuah teknologi informasi dan komunikasi dalam era globalisasi cukup menempati posisi yang sangat strategis dalam kehidupan. Karena hal ini dapat menciptakan dunia tanpa batas, tanpa sekat, bebas dan sepenuhnya merdeka dalam arus komunitas siber.⁹⁹ Tidak dapat dipungkiri bawah hal tersebut membawa hal yang bermanfaat dan dampak positif,¹⁰⁰ akan tetapi disisi lain juga diimbangi dampak negatif dengan menciptakan sebuah celah bagi kejahatan baru dalam ranah digital (*cybercrime*).¹⁰¹ Sehingga diperlukan adanya sebuah perlindungan yang cukup kuat, terutama terhadap *cybercrime* berupa *phising* yang kerap dimanfaatkan sebagai sarana penipuan maupun pencurian data pribadi.¹⁰²

Phising merupakan kejahatan siber di mana penyerang mencoba guna mendapatkan sebuah informasi sensitif seperti nama pengguna, kata sandi, dan rincian kartu kredit dengan menyamar sebagai entitas terpercaya dalam

⁹⁹ Maskun, 2022, *Kejahatan siber (cybercrime)*, Jakarta: Kencana, Halaman 43

¹⁰⁰ Saputra Gulo, A., Lasmadi, S., & Nabawi, K. (2020). :Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik". PAMPAS: Journal Of Criminal, Vol.1, No.2, Halaman 69

¹⁰¹ Haryadi, 2012, *Kebijakan Integral penanggulangan cyberporn di Indonesia*, Semarang: Lima, Halaman 4

¹⁰² Saputra Gulo, A., Lasmadi, S., & Nabawi, K. *Loc.cit*

komunikasi elektronik. *phising* menggambarkan usaha penyerang untuk "memancing" korban agar memberikan informasi pribadi mereka.¹⁰³

Phising melalui aplikasi pesan instan seperti WhatsApp semakin meningkat karena tingginya penggunaan aplikasi tersebut di kalangan masyarakat.¹⁰⁴

Ini menunjukkan bahwa platform pesan instan, termasuk WhatsApp, telah menjadi sasaran populer bagi serangan phising karena penggunaannya yang luas dan kemudahan aksesibilitasnya.¹⁰⁵ Pesan *phising* pada platform ini biasanya mencakup tautan yang mengarahkan pengguna ke situs palsu yang sama persis dengan situs resmi atau pelaku phishing mengirimkan link berupa undangan pdf maupun aplikasi (APK) sehingga pengguna tanpa sadar memasukkan informasi pribadi mereka.¹⁰⁶ Portal ini dibuat secara khusus agar sesuai dengan tujuan mengekstraksi data yang ingin dikumpulkan oleh penyerang.¹⁰⁷ Implikasi adalah akibat dan konsekuensi yang ditimbulkan dalam suatu aktivitas tertentu, implikasi ataupun akibat dari ketidaktahuan pengguna akan kejahatan *cybercrime* dalam bentuk phising mempermudah pelaku untuk menipu korbannya.¹⁰⁸

¹⁰³ Isadora, *Op.cit.*, Halaman 47

¹⁰⁴ *Ibid.*, Halaman 47

¹⁰⁵ *Ibid.*, Halaman 48

¹⁰⁶ Suharto, B., & Kurniawan, A. B. (2020). "Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising)". Jurnal:JHP, No.17, Halaman 59

¹⁰⁷ Hanafi, 2022, *Dasar Cyber Security dan Forensik*, Yogyakarta: Deepublish, Halaman 7

¹⁰⁸ Rahimah, R., & Koto, I. (2022). "Implications of parenting patterns in the development of early childhood social attitudes". International Journal Reglement & Society (IJRS), Vol 3, No 2, Halaman 130.

Menurut penelitian oleh Kaspersky (2020), “serangan phishing di aplikasi WhatsApp lebih sulit dideteksi karena pesan sering kali datang dari pihak yang dikenal, yang menciptakan rasa kepercayaan”.¹⁰⁹

Umumnya, berita yang dimuat dalam pesan WhatsApp atau media sosial berisi berita yang meyakinkan korban untuk mengklik link dan mengakses 'situs web palsu, dan memasukkan data pribadi korban dan bukan hanya sekedar link yang merujuk ke sebuah website pelaku juga sering mengirimkan sebuah file apapun yang berbahaya bagi pengguna smartphone, sejenis *mal-ware* dapat mencakup *virus*, *worm*, *trojan horse*, dan *spywa-re*. Program jahat ini dapat melakukan berbagai fungsi berbeda seperti mencuri, mengenkripsi, atau menghapus data sensitif, mengubah atau membajak fungsi smartphone inti, dan memantau aktivitas smartphone pengguna tanpa izin mereka.

Serangan *Phising* juga berhasil karena kesalahan manusia atau kurangnya kesadaran. Peringatan keamanan sering kali diabaikan oleh pengguna, sehingga memudahkan upaya *Phising* berhasil, penyerang *Phising* menyesatkan pengguna agar membocorkan informasi pribadi dengan menggunakan teknik rekayasa sosial, seperti mempermainkan emosi, seperti rasa takut dan kekhawatiran korban terhadap hal tersebut.¹¹⁰

¹⁰⁹ Isadora, *Op.cit.* Halaman 50

¹¹⁰ Trianurahmah, A., et.al.. (2024). "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspada Maraknya Kejahatan Phising Dengan Modus Berbasis Link". *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, Vol 1. No 2. Halaman 83

Ketidaktahuan mereka terhadap informasi tentang kejahatan *Phising* terhadap pula tidak dapat ketidaktahuan dalam membedakan nama domain asli dan palsu, dan tidak mengetahui cara menangani upaya *Phising*. Kewaspadaan dan pemahaman yang mendalam sangat diperlukan untuk dapat mencegah ancaman tersebut agar terhindar dari kejahatan *Phising*.¹¹¹

Dalam konteks keamanan siber, termasuk phishing di WhatsApp, Penyebab terjadinya *phising* melalui WhatsApp meliputi 2 faktor, faktor internal dan eksternal memiliki peran penting dalam menentukan kerentanan seseorang atau organisasi terhadap serangan. sebagai berikut:

1. Faktor Internal

Metode phishing dengan mengaku sebagai entitas terpercaya untuk mengelabui korban, biasanya dengan mengirimkan sebuah pesan teks khususnya dalam penelitian ini dengan menggunakan platform digital WhatsApp, guna mencuri informasi sensitif korban.¹¹² Maka dalam hal ini Faktor Kognitif dalam Proses *Phishing*, rekayasa sosial adalah mekanisme yang digunakan pelaku *phising* untuk mencuri data pribadi. Rekayasa sosial merupakan cara pelaku dengan memanipulasi psikologis korban dengan cara mengelabui maupun mempengaruhi karena hasil serangan bergantung pada keputusan pengguna atau korban, serta kepercayaan, Jadi, penting untuk memahami faktor psikologis. Oleh karena itu, untuk menganalisis akar penyebab serangan phishing, kita harus

¹¹¹ *Ibid.*, Halaman 84

¹¹² Dianti, S. D., & Nugroho, A. A. (2023). "Perlindungan Hukum Konsumen Pengguna Aplikasi E-Commerce Terhadap Kasus Penyalahgunaan Akun dalam Konstruksi Hukum ITE". Al Qalam: Jurnal Ilmiah Keagamaan dan Kemasyarakatan, Vol.17, No.2, Halaman 977

mempelajari faktor psikologis untuk mengetahui penyebab utama mengapa pengguna terjebak dalam tindak pidana *cybercrime* berupa phishing, sebagai berikut¹¹³

a. *Suspicion* (Kecurigaan)

Sebuah studi baru-baru ini menunjukkan bahwa kecurigaan merupakan salah satu faktor penentu dalam serangan *phishing*. Studi ini juga menunjukkan bahwa pengguna menentukan kecurigaan berdasarkan cara mereka memproses pesan, secara sistematis atau heuristik. Apabila pengguna meyakini perbuatan tersebut merupakan perbuatan *cybercrime* maka mereka akan memproses pesan tersebut secara sistematis (membuat keputusan secara rasional) namun apabila pengguna meyakini perbuatan tersebut bukan perbuatan *cybercrime* maka mereka akan memprosesnya secara heuristik (membuat keputusan dengan cepat).¹¹⁴

Berdasarkan cara heuristik dan sistematis, apabila korban atau pengguna yang menerima pesan yang biasanya merespon dengan cara “pemrosesan sistematis” yang memandang kecurigaan tinggi terhadap pesan phishing tersebut. sedangkan mereka yang lemah tingkat kecurigaannya terhadap pesan-pesan biasanya mereka merespon dengan cara “pemrosesan heuristik” yang menyebabkan rendahnya kecurigaan terhadap *phishing*.

¹¹³ Abroshan, H., et.al. (2018). "Phishing attacks root causes". In Risks and Security of Internet and Systems: 12th International Conference, CRiSIS 2017, Dinard, France, Revised Selected Papers 12. Springer International Publishing. Halaman 191

¹¹⁴ *Ibid.*, Halaman 191

b. *Trust* (Kepercayaan)

Kepercayaan dalam konteks ini diartikan sebagai “kemauan untuk mengambil risiko”, yang artinya kepercayaan dapat memediasi secara positif. Kepercayaan adalah kemauan bertindak dari seorang tanpa memperhitungkan dan mempertimbangkan risiko yang akan diterima.¹¹⁵

Kepercayaan diartikan sebagai keyakinan terhadap diri sendiri sehingga mampu menangani segala situasi walaupun memiliki resiko yang tidak terlalu terlihat. Kepercayaan merupakan salah satu faktor yang mempengaruhi serangan phishing mau dalam hal mempercayai atau tidak.¹¹⁶ Pelaku menggunakan salah satu beberapa kepercayaan yang dipercayai korban atau pengguna sebagai kondisi untuk mendorong korban untuk mempercayai pelaku.

c. *Prediction* (Prediksi)

Pelaku phisher meningkatkan kemiripan mereka dengan Institusi atau organisasi yang menjadi target untuk mendorong rasa kepercayaan korban. Hal ini terjadi karena orang-orang "memprediksi berdasarkan kemiripan"

Apabila terdapat Pengalaman sebelumnya pengguna atau korban memiliki pengetahuan, informasi, dan/atau pengalaman orang tersebut dengan phishing, akan memengaruhi prediksi pengguna dalam upaya phishing tertentu. Misalnya, jika pendapat pengguna/korban tentang phishing merupakan bukan serangan

¹¹⁵ Jasin, H., et.al. (2021). "Apakah Kepercayaan Memediasi Pengaruh Reputasi Bank dan Religiusitas Terhadap Purchase Intention". Jurnal Ilmiah: Manajemen dan Bisnis, Vol.22. No.1, Halaman 97

¹¹⁶ Andiwijaya, D., & Liauw, F. (2019). "Pusat pengembangan kepercayaan diri". Jurnal Sains: Teknologi, Urban, Perancangan, Arsitektur (Stupa), Vol.1, No.2, Halaman 1697

phishing, maka orang tersebut mungkin memprediksi bahwa itu adalah komunikasi normal.¹¹⁷

d. Minimnya Literasi.

Minimnya Literasi menjadi salah satu faktor utama yang menjadi sebuah peluang terjadinya cybercrime berupa phishing. Dengan ketidaktahuan dan kurangnya terhadap pemahaman akan sebuah kecanggihan teknologi dan media elektronik menciptakan celah dan menjadi pengguna sebagai target utama pelaku.

e. Kurangnya pengendalian emosi

Saat menggunakan sebuah media sosial ataupun platform digital turut menjadi faktor yang membuat sebagian pengguna rentan menjadi korban phishing. Karena biasanya korban/pengguna kesulitan menolak atau tidak bisa merespon sesuatu secara tepat. Dalam banyak kasus, fokus pengguna selalu tenggelam dalam emosi baik dipicu oleh pesan ataupun hal lainnya, seperti rasa urgensi untuk segera merespon tautan berisi hal mendesak, iming-iming hadiah atau iming-iming lainnya hingga akhirnya pengguna mengabaikan resiko dibalik tindakan tersebut.¹¹⁸

Maka dapat dipahami, Bahwa minimnya pengetahuan dan kurangnya pengendalian emosi menjadi faktor internal yang harus dipandang. karena menjadi salah satu penyebab terjadinya cybercrime berupa phishing.¹¹⁹

¹¹⁷ *Ibid.*, Halaman 193-194

¹¹⁸ *Ibid.*, Halaman 978

¹¹⁹ *Ibid.*, Halaman 978

2. Faktor Eksternal

Modus *phising* dilakukan dengan pembuatan situs atau *website* palsu, *Website* dibuat sedemikian rupa mungkin seperti website aslinya untuk memikat daya tarik calon korban.¹²⁰

Berikut beberapa faktor eksternal:

- a. Lemahnya sistem keamanan pada Platform ataupun website/situs Platform sangat mudah ditiru, Ketika gambar dapat platform bisa ditiru dan lemahnya keamanan sangat memudahkan bagi Pelaku kejahatan untuk melakukan aksinya.¹²¹

Lemahnya sebuah tingkat sistem keamanan website/situs tidak terlepas juga dengan mudahnya tampilan website yang mudah ditiru sedemikian rupa menjadi salah satu faktor terjadinya *phising*. Banyak sekali dari para pengguna tidak benar-benar mengetahui ciri-ciri khusus pada tampilan situs resmi suatu lembaga/perusahaan, sehingga para pengguna terkecoh dengan tampilan situs palsu yang sedemikian rupa. Pada dasarnya kebanyakan daripada pengguna hanya sekedar mengetahui ataupun mengenali nama sebuah perusahaan/lembaga secara umum. Karena hal itulah cara termudah bagi pengguna untuk mengakses informasi, tanpa perlu memverifikasi keaslian tampilan situs yang mereka kunjungi.¹²² Ketidaktahuan pengguna terhadap

¹²⁰ Mulyadi, M., et.al. (2024). "Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi". Jurnal: Media Hukum Indonesia (MHI), Vol. 2, No.2, Halaman 78

¹²¹ Khairunnisa, A. (2021). Perlindungan Konsumen Dalam Transaksi E-Commerce Platform Bukalapak (Bachelor's thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta). Halaman 88

¹²² Dianti, *Op.cit.* Halaman 978

situs palsu berpotensi menimbulkan konsekuensi cukup serius. Terburuknya berujung kepada kerugian, baik secara finansial maupun privasi data pribadi.

- b. Tata Kelola perlindungan data pribadi. yang dapat dikatakan belum cukup optimal turut serta menjadi salah satu faktor krusial yang menjadi celah terjadinya serangan Phising.¹²³ Tantangan dalam menjaga data pribadi perlu menjadi perhatian utama, mengingat bahwa kebocoran data bisa terjadi akibat lemahnya kapabilitas pengelola data atau penyelenggara sistem elektronik dalam melindungi sistem mereka dan ini tidak terlepas dari terjadinya serangan hacker.¹²⁴ Oleh karena itu, penting bagi pengguna untuk lebih bijak dalam menggunakan informasi pribadi dalam ranah digital.¹²⁵ Kebocoran data pribadi dapat memiliki dampak negatif.¹²⁶ Sebagai penyedia layanan digital perusahaan harus memiliki sebuah tanggung jawab untuk memastikan bahwa keamanan dan kerahasiaan data pribadi bagi pengguna layanan tersebut. Dalam memberikan perlindungan data pribadi bukan hanya sekedar kewajiban bagi pihak terkait, melainkan menjadi fondasi utama guna membantu rasa kepercayaan dan kredibilitas layanan tersebut.

Lemahnya sebuah sistem keamanan pada tampilan situs yang sangat mudah ditiru sedemikian rupa seperti aslinya, serta tata kelola perlindungan data pribadi yang belum berjalan secara optimal merupakan faktor yang cukup serius. Serangan Phising merupakan kejahatan siber yang dapat dikatakan bahwa cukup

¹²³ *Ibid.*, Halaman 979

¹²⁴ Muin, I. (2023). Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia. *Journal Law And Justice*, 1(2). Halaman 83

¹²⁵ Dianti, *Op.cit.* Halaman 979

¹²⁶ Muin, *Op.cit.* Halaman 86

sulit dideteksi apabila sistem keamanan pada lembaga/perusahaan tertentu masih tergolong lemah, oleh karena itu bagi penyelenggara layanan baik sebuah aplikasi maupun website dituntut untuk lebih meningkatkan sistem keamanan yang lebih kuat.¹²⁷

B. Pengaturan Hukum Tindak Pidana Siber Phising Dengan Menggunakan Platform WhatsApp

1. Menurut Undang-undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Kejahatan siber berupa phising melalui platform digital seperti WhatsApp terus menjadi sebuah ancaman yang cukup nyata bagi masyarakat.¹²⁸ Di Indonesia, kemajuan baru-baru ini telah dicapai dalam hal regulasi perlindungan data. RUU (Perlindungan Data Pribadi) disahkan menjadi sebuah undang-undang (UU PDP 2022). Undang undang ini sangat diharapkan dapat dijadikan sebagai "payung hukum" dalam ranah digital. Pengesahan RUU menjadi sebuah undang-undang juga merupakan sebuah pencapaian strategis dalam membangun pondasi dalam tata kelola data pribadi yang lebih kuat. Langkah ini menandai bahwa pemerintah cukup serius dalam menjaga dan melindungi privasi warganya.¹²⁹

Tujuan utama dari UU PDP adalah menyediakan kerangka hukum yang memadai untuk melindungi masyarakat dan pemerintah dari kejahatan digital, termasuk pencurian data pribadi Kementerian Komunikasi dan Informatika

¹²⁷ Dianti, *Op.cit.* Halaman 979

¹²⁸ Sutarli, A. F., & Kurniawan, S. (2023). "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia". *Innovative: Journal Of Social Science Research*, Vol 3. No.2, Halaman 4

¹²⁹ Edy Santoso, 2023, *Hukum siber: permasalahan hukum bisnis di bidang teknologi informasi dan komunikasi*, Jakarta: Kencana, Halaman 51

menyatakan bahwa UU PDP akan menandai langkah penting dalam pengelolaan data pribadi di Indonesia.¹³⁰

Berdasarkan pada pasal 1 angka (1) UU RI nomor 27 tahun 2022 tentang perlindungan pribadi yang dimaksud dengan data pribadi adalah sebagai berikut:

"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".

Bersumber pada pasal 1 angka (2) UU RI nomor 27 tahun 2022 tentang perlindungan data pribadi sebagai berikut:

"perlindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi".

Perlindungan data pribadi adalah bagian dari hak pribadi (*privacy rights*).

Hak pribadi mengandung pengertian sebagai berikut:

1. Hak pribadi merupakan hak fundamental yang dimiliki oleh setiap individu untuk menikmati hidup secara tenang, aman dan bebas dari segala macam bentuk intervensi ataupun gangguan. Ini merupakan sebuah fondasi dari kebebasan pribadi yang menjamin ruang privasi yang tak bisa di ganggu gugat oleh siapapun.
2. Hak pribadi mencakup kebebasan untuk berkomunikasi dengan siapapun tanpa rasa khawatir akan di mata matai atau di sadap, ini merupakan salah satu

¹³⁰ Manorek, B. D. (2025). "Penegakan hukum pidana dalam memberantas kejahatan pencucian data elektronik phising", *Lex Privatum*, Vol 15, No 2. Halaman 3

pilar penting dalam menjamin privasi dan menjaga integritas komunikasi dan melindungi kebebasan berekspresi di era digital.

3. Hak pribadi mencakup kendali penuh atas siapa yang dapat mengakses informasi mengenai kehidupan dan data pribadi seseorang. Ini adalah bentuk perlindungan yang mendasar bahwa setiap individu memiliki otoritas atas privasinya.¹³¹

Pemerintah memiliki peran yang cukup penting dalam memastikan implementasi undang-undang perlindungan data pribadi (UU PDP), serta hak-hak individu, selain itu juga pemerintah juga harus memberikan rasa aman dalam beraktifitas di ranah digital.¹³²

Cybercrime dalam bentuk phishing dapat dikategorikan sebagai perbuatan pengumpulan data pribadi secara melawan sesuai sebagaimana yang dimaksud dalam unsur-unsur Pasal 65 angka (1) dan (3) undang undang No 27 tahun 2022 tentang perlindungan data pribadi sebagai berikut:

Angka (1): "Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi".

Angka (3): "Setiap orang dilarang secara melawan hukum menggunakan Data pribadi yang bukan miliknya".

Pada pasal ini secara tegas melarang seseorang dalam mengakses, mengumpulkan, atau membocorkan sebuah data pribadi milik orang lain tanpa

¹³¹ Nawangsasi, E, 2022, *Perlindungan privacy di era new normal digital lifestyle terkait cyber power*, Bandung: Refika adatama, Halaman 44

¹³² *Ibid.*, Halaman 9

hak ataupun izin, terutama apabila tindakan tersebut dapat merugikan pemilik data, dengan larangan dalam hal kegiatan pengumpulan atau perolehan data pribadi yang bukan miliknya secara sengaja melawan hukum, dengan tujuan guna mendapatkan sebuah keuntungan sendiri atau untuk orang lain, yang bisa merugikan pemilik data, sebagaimana yang dimaksud pada pasal tersebut.

Ancaman pidana bagi pelaku pengumpulan data pribadi secara melawan hukum, di tuang dalam pasal 67 angka (1) dan (3) UURI nomor 27 tahun 2022 tentang perlindungan data pribadi:

Angka (1): Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Angka (3): Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)

Jika seseorang terbukti telah melakukan perbuatan-perbuatan melakukan pengumpulan data pribadi secara melawan hukum, sebagaimana yang telah dijelaskan dalam pasal 65, dalam hal perbuatan yang termasuk dalam pasal 65 maka sesuai para pelaku *phising* bisa diancam sanksi pidana sesuai Pasal 67.¹³³

¹³³ Azmi, M. et.al. (2024). "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam". Sistem Perbankan: Indonesia. Jurnal Multidisiplin Ilmu Akademik, Vol 1. No.6, Halaman 450

Dimana pelaku secara melawan hukum mengakses dan memperoleh data pribadi yang bukan miliknya tanpa hak.¹³⁴

Pasal 65 Ayat (1): Pasal ini menegaskan bahwa setiap orang dilarang mengakses, memperoleh, atau mengumpulkan data pribadi milik orang lain secara tidak sah atau melanggar hukum, terlebih jika hal itu dilakukan dengan tujuan untuk mendapatkan keuntungan pribadi atau untuk menguntungkan orang lain. Larangan ini juga berlaku jika tindakan tersebut berpotensi atau dapat menyebabkan kerugian bagi pemilik data pribadi. Dengan kata lain, siapa pun tidak boleh "mengambil" data milik orang lain tanpa izin, apalagi jika digunakan untuk kepentingan tertentu yang merugikan si pemilik data baik Ayat (1) dan (3) juga menyebutkan, bahwa "setiap orang" juga tidak boleh menggunakan data pribadi orang lain secara melawan hukum, meskipun dia mungkin tidak yang mengumpulkannya. Jadi, penggunaan data pribadi milik orang lain tanpa dasar hukum atau tanpa izin tetap dianggap sebagai pelanggaran, meskipun data tersebut diperoleh dari pihak ketiga.

¹³⁴ Sutarli, *Op.cit.*, Halaman 11

2. Menurut Undang-undang No 1 Tahun 2024 Perubahan Kedua Atas Undang-undang No 11 Tahun 2008 Tentang Transaksi Dan Informasi Elektronik

Phising berasal dari kata *fishing* yang berarti memancing, yang menggambarkan upaya seseorang untuk mendapatkan informasi secara ilegal, perbuatan ini termasuk sebuah tindakan manipulatif yang secara khusus untuk menipu korban agar secara tidak sadar korban memberikan informasi pribadi korban.¹³⁵

Pemerintah Indonesia berupaya mendorong dan melindungi para pengguna media sosial untuk tetap aman dan nyaman dalam berselancar di dunia siber. Pemerintah memiliki kewajiban untuk melindungi masyarakat, dari kejahatan *cybercrime*, negara masih tetap memiliki yuridiksi penuh dalam ranah digital dan tidak ada satu individu yang dapat terlepas dari sanksi atas tindak Pidana yang dilakukan dalam ranah digital.¹³⁶

Didalam Undang-Undang No.1 Tahun 2024 tentang perubahan kedua atas Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Perbuatan *cybercrime* dalam bentuk *phising* secara *eksplisit* belum diatur di UU, akan tetapi Perbuatan *cybercrime* berupa *phising* dapat dijerat dengan beberapa pasal di UU ITE, salah satunya diatur dalam pada Pasal 35 jo Pasal 51 ayat(1), yang dijelaskan sebagai berikut:

¹³⁵ Manorek, *Op.cit.*, Halaman 4

¹³⁶ Danrivanto, 2017, *Revolusi cyber law Indonesia pembaruan dan revisi undang-undang informasi dan transaksi elektronik 2016*, Bandung, Refika aditama, Halaman 140-144

Pasal 35

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memanipulasi, membuat, mengubah, menghilangkan, memusnahkan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap sebagai data yang autentik.”

Pasal 51 ayat (1)

"Setiap orang yang memenuhi pasal 35 maka dipidana dengan pidana penjara paling lama 12(dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)".

Pelaku membuat sebuah *website* palsu yang dapat dikategorikan sedemikian rupa menyerupai *website* aslinya.¹³⁷ Tujuan pengaturan Pasal 35 UU ITE adalah untuk memastikan terpercayanya sebuah informasi atau dokumen elektronik, terutama dalam konteks transaksi elektronik. Keautentikan (authenticity) informasi ini mengindikasikan bahwa dokumen atau data elektronik tersebut dapat dipercaya dan sah secara hukum.

Dalam perbuatan menciptakan sebuah *website* yang menyerupai *website* aslinya termasuk dalam manipulasi informasi elektronik, manipulasi merupakan suatu tindakan atau perbuatan dengan rekayasa yang dilakukan dengan sadar dan sistematis dengan cara menambahkan ataupun menyamarkan informasi baik sebagai maupun seluruhnya. Dalam konteks hukum, manipulasi dianggap sebagai bentuk distorsi informasi yang berpotensi yang menyesatkan dan merugikan orang lain. jika dilihat dari cara pelaku dengan mengirimkan sebuah link melalui

¹³⁷ Banjarnahor, A. C., & Priyana, P. (2022). " Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo". HERMENEUTIKA: Jurnal Ilmu Hukum, Vol 6, No 1, Halaman 34

WhatsApp seperti seolah-olah dari perusahaan/lembaga yang sah, mereka mencoba menipu pengguna untuk mengklik tautan (link) yang tampaknya mengarah ke situs web bisnis yang sah, tetapi sebenarnya membawa pengguna ke situs penipu yang dikendalikan oleh penyerang dan dirancang untuk menyerupai situs resmi dari suatu lembaga ataupun organisasi. Situs meminta pengguna untuk login nama dan kata sandi (*password*) atau informasi akun lainnya.¹³⁸ Pelaku *phishing* melakukan manipulasi informasi elektronik dan/atau dokumen elektronik dengan maksud untuk menciptakan sebuah kesan bahwa data tersebut sah dan otentik, yang secara khusus dituang dalam pasal 35 UU ITE. Unsur-unsur dari pasal tersebut adalah:¹³⁹

1. "Unsur setiap orang",
2. "Unsur dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik, dan"
3. "Unsur dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik."

Berdasarkan hal tersebut, maka dapat dikatakan bahwa "manipulasi informasi elektronik merupakan suatu tindakan dengan cara merekayasa atau merubah suatu informasi elektronik dan/atau dokumen elektronik." Apabila

¹³⁸ Nawangsasi, *Op.cit.*, Halaman 56

¹³⁹ Ablisar, M., et.al. (2022). "Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik: Studi Putusan No. 542/Pid. Sus/2019/PN. Mlg". *Locus: Jurnal Konsep Ilmu Hukum*, Vol 2. No 2, Halaman 55

dikaitkan dengan cara pelaku yang mengirimkan sebuah tautan atau pesan yang tampak resmi untuk menipu korban agar memberikan informasi pribadi atau mengunduh sebuah aplikasi berbahaya dan terdapat juga sebuah penciptaan sebuah informasi elektronik berupa domain pada website, terdapat data data informasi yang menjelaskan ataupun memberikan informasi terhadap suatu *website* tersebut, contohnya informasi seperti data di *website* palsu menggunakan "kikbca.com" (informasi data aslinya klikbca.com). Perbuatannya termasuk memanipulasi informasi elektronik maka dapat dikatakan bahwa Perbuatan ini termasuk dalam bentuk memanipulasi informasi elektronik agar terlihat sah sebagaimana yang disebutkan dalam pasal 35 uu ITE.¹⁴⁰ Apabila seluruh unsur dalam pasal 35 juncto pasal 51 ayat 1, telah terpenuhi maka pelaku dapat dijerat dan diancam dengan pasal tersebut.¹⁴¹

Jika serangan siber berhasil terhadap targetnya maka dapat menimbulkan dampak yang cukup serius, mulai dari kerugian yang di alami oleh individu, gangguan terhadap penyedia layanan digital, hingga terjadi kerusakan serius pada data yang tersimpan di sistem maupun yang sedang dalam proses pengiriman data melalui jaringan. Serangan ini kerap menyusup ataupun membobol ke perangkat korban atau pengguna tanpa sepengetahuannya, sehingga ini menimbulkan resiko terhadap keamanan informasi, seperti kerahasiaan, integritas dan ketersediaan.

¹⁴⁰ *Ibid.*, Halaman 63

¹⁴¹ Putri, I. E. (2023). "Analisis Yuridis Putusan Hakim Dalam Perkara Tindak Pidana Phising Yang Dilakukan Melalui Media Sosial:(Studi Putusan Nomor: 155/Pid. Sus/2018/PN. Cbn)". *Delicti: Jurnal Hukum Pidana Dan Kriminologi*, Vol 1, No 1, Halaman 9

Perbuatan tersebut dapat diklasifikasikan sebagai perbuatan penerobos sistem elektronik sebagaimana yang dimaksud dalam pasal 30 Undang-Undang No 1 Tahun 2024 tentang perubahan kedua atas Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hal ini berlaku bagi siapa saja yang secara melawan hukum melakukan pelanggaran dengan menerobos, menyalip, atau membobol sistem keamanan korban tanpa sepengetahuan korban, sehingga dapat dijerat:¹⁴² Pasal 30 jo. Pasal 46 ayat(3) Undang-Undang No 1 Tahun 2024 tentang perubahan kedua atas Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang disimpulkan sebagai berikut:

Setiap orang yang melakukan secara sengaja, dan tanpa hak dengan melawan hukum dalam mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos.atau menjebol sistem keamanan maka dipidana dengan penjara paling lama 8(delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Cybercrime dalam bentuk *phising* khususnya dalam sebuah *platform* digital WhatsApp dalam sistem elektronik, bahwa pelaku berdalih sebagai perwakilan resmi dari sebuah lembaga, ataupun organisasi tertentu yang dipercayai oleh korban dengan cara bahwasanya terdapat masalah keamanan dalam akun mobile *banking* korban ataupun diiming-imingkan mendapatkan sebuah promo hingga, bonus hadiah dengan diminta untuk segera mungkin untuk melakukan tindakan lanjutan.¹⁴³

Korban terkadang tidak curiga bahwa pesan tersebut berasal dari pelaku secara ilegal. Kerugian korban di sini adalah bahwa mereka tidak berhati-hati

¹⁴² Edy Santoso, *Op.cit.*, Halaman 87

¹⁴³ Banjarnahor, *Op.cit.*, Halaman 35-36.

untuk memeriksa, mana yang datang dari organisasi yang asli atau palsu. Hal yang lebih berbahaya lagi, bahwa *phising* itu memiliki lampiran jahat, seperti dokumen PDF atau aplikasi, seperti file PDF begitu di buka atau aplikasi begitu terinstall dalam perangkat smartphone maka akan membahayakan perangkat pengguna karena telah diinstallnya sebuah perangkat lunak berbahaya, seperti virus (*Malware*).¹⁴⁴

Malware merupakan program komputer yang dirancang untuk mencari kelemahan pada sistem software pada suatu perangkat. Pada dasarnya *Malware* diciptakan dengan tujuan untuk merusak atau membobol sistem pada perangkat. *Malware* mencakup beberapa jenis diantaranya yaitu, *worm*, *Trojan Horse*, *adware*, *browser hijacker*, dan lain-lain.¹⁴⁵

Pelaku dapat menggunakan malware atau jenis serangan lain untuk menguasai perangkat korban, seperti laptop atau smartphone, dan menggunakannya untuk meluncurkan serangannya ke sistem perangkat korban. Hal ini dapat mengakibatkan konsekuensi hukum atau bahkan kerugian bagi korban.¹⁴⁶ Dengan begitu pelaku meretas perangkat tersebut tanpa sepengetahuan korban, akan tetapi pelaku dalam melakukan aksinya harus memiliki keahlian di bidang IT dan jaringan, sehingga mampu menembus sistem keamanan lembaga keuangan. Kuncinya memang ada di sistem keamanannya. perbuatan pelaku termasuk membobol atau menerobos sistem elektronik atau perangkat tanpa

¹⁴⁴ Edy Santoso, *Op.cit.*, Halaman 105

¹⁴⁵ Nurdiman, *Op.cit.*, Halaman 217

¹⁴⁶ Nawangsasi, *Op.cit.*, Halaman 45

sepengetahuan pengguna dan apabila terpenuhinya unsur unsur sebagaimana yang dimaksud pada pasal 30 Jo pasal 46 ayat (3) maka dapat dijerat atau diancam pidana dengan pasal tersebut.¹⁴⁷

Tindak Pidana cybercrime dalam bentuk phising kerap melibatkan tindakan penipuan melalui kebohongan yang disengaja untuk mengelabui korban. Akibatnya, banyak daripada korban mengalami kerugian karena informasi pribadi mereka berhasil diakses oleh pelaku phising, terkait perbuatan tersebut dapat diancam dengan pasal 28 ayat (1) jo Pasal 45A ayat(1) Undang-Undang No.1 Tahun 2024 tentang perubahan kedua atas Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik,¹⁴⁸ karena *phishing* menipu dan menyesatkan korbannya sehingga mengunjungi situs web palsu dan memasukkan data pribadi atas tindakan penipuan.¹⁴⁹

Pasal 28 ayat(1)

"Setiap Orang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik."

Pasal 45A ayat (1)

"Setiap orang yang memenuhi pasal 28 ayat (1) maka dipidana dengan pidana penjara paling lama 6(enam) tahun dan/atau denda paling banyak miliar Rp1.000.000.000,00.¹⁵⁰

¹⁴⁷ *Ibid.*, Halaman 87

¹⁴⁸ *Ibid.*, Halaman 35-36.

¹⁴⁹ Harahap, *Op.cit.*, Halaman 1373

¹⁵⁰ Danrivanto, *Op.cit.*, Halaman 110

¹⁵¹ *Ibid.*, Halaman 11

3. Pengaturan Hukum Menurut Pandangan Islam

Dalam pandangan syariat Islam, perbuatan menipu termasuk dalam golongan perbuatan dosa karena sejatinya merupakan bentuk kebohongan yang merugikan orang lain. Maka dapat dipahami bahwa kebohongan merupakan perbuatan memalsukan kebenaran ataupun mengelabui orang lain. Islam melarang perbuatan tersebut. Allah SWT bahkan memperingatkan hal tersebut dalam Alqur'an tentang orang-orang yang menyebarkan berita bohong, Sebagaimana dalam firman-Nya dalam surah Al-Hujurat' ayat 6 sebagai berikut:

يَا أَيُّهَا الَّذِينَ آمَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَأٍ فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا بِجَهَالَةٍ فَتُصْحَبُوا عَلَىٰ مَا فَعَلْتُمْ نَادِمِينَ

Artinya: "Wahai orang-orang yang beriman! Jika seseorang yang fasik datang kepadamu membawa suatu berita, maka telitilah kebenarannya, agar kamu tidak mencelakakan suatu kaum karena kebodohan (kecerobohan), yang akhirnya kamu menyesali perbuatanmu itu".

Maksud dari ayat di atas adalah bahwa janganlah kita menerima begitu saja berita dari orang lain (fasik) berupa penipuan, sampai kita melakukan tabayyun alias mencari kebenaran dari berita yang kita terima tersebut.¹⁵²

Terdapat Hadits yang melakukan perbuatan berbohong, Rasulullah bersabda:

“Berbohong adalah salah satu tanda orang munafik.” (HR. Bukhari dan Muslim). Tanda orang munafik ada tiga: jika berkata ia dusta, jika berjanji ia mengingkari, jika diberi amanat ia berkhianat".¹⁵³

¹⁵² Sumiati. 2017. Bahaya menyebarkan berita bohong dalam pandangan Islam. diakses dari <https://kalbar.kemenag.go.id/berita/berita.php?nid=4539>. pada tanggal 28 februari 2025 pada pukul 10:47 WIB

¹⁵³ Nurul, 2025. Tidak jujur tanda munafik, diakses dari <https://iainutuban.ac.id/2025/02/13/tidak-jujur-tanda-munafik/#:~:text=Rasulullah%20bersabda%3A%20>

Dalam perkembangan hukum Islam, memang masih belum terdaftar ketentuan khusus yang secara eksplisit mengatur tentang tindak Pidana tentang secara digital seperti phising, Akan tetapi prinsip prinsip syariat Islam telah lama menegaskan bahwa larangan terhadap segala bentuk penipuan dan pemalsuan, bahkan sejak jaman para sahabat.

Salah satu contoh yang cukup relevan dalam hal ini, terjadi pada masa kepemimpinan Khalifah Umar bin Khattab dikatakan bahwa seorang bernama mu'an bin zaidah melakukan penipuan dengan cara memalsukan sebuah stempel resmi milik Baitul Mal (Lembaga keuangan pada saat itu), Namum, ketika penjaga Baitul Mal mengetahui hal tersebut, Mu'an bin zaidah ia segera mengambil kembali stempel palsu tersebut, dan kasusnya tersebut sampai terdengar oleh Umar bin Khattab ia kemudian bertindak tegas, dengan menghukum mu'an bin zaidah dengan dipukul seratus kali, dipenjara, lalu kembali dihukum seratus kali lagi, dimarahi, dipukul lagi hingga seratus kali dan akhirnya di asingkan.

Kisah ini menunjukkan bahwa Islam sejak awal sudah menentang segala bentuk penipuan, termasuk yang dilakukan melalui manipulasi simbol maupun identitas resmi, yang secara khusus dapat dikatakan serupa dengan praktik kejahatan cybercrime berupa phising di era digital saat ini. Walaupun, medianya berbeda, prinsip hukumnya tetap berlaku, penipuan bukan hanya sekedar melanggar hukum manusia, tetapi juga nilai nilai ilahi.

Dari contoh di atas ternyata penipuan dengan modus pemalsuan ini sudah terjadi pada zaman Nabi Muhammad SAW dan sahabat. Seperti hadis Rasulullah di bawah ini yang melarang adanya unsur penipuan dalam dalam hal jual beli:

عن أبي هريرة أن رسول الله ﷺ مر على صبرة طعام فيها فنالت أصابعه بلال فقال هذا يا صاحب الطعام؟ قال أصابته السماء يا رسول الله قال أفال جعلته فوق الطعام كي يراه يراه ما الناس؟ من غش فليس مني

Artinya: "Dari Abu Hurairah ra, berkata: "Pada suatu ketika Rasulullah melewati tumpukan makanan (dipasar)", lalu beliau memasukkan tangannya kedalam tumpukan itu setelah kembali, ternyata jari-jari beliau basah. Lalu beliau bertanya "kenapa begini hai penjual makanan?" "jawabanya" kena hujan ya Rasulullah "sabda beliau", mengapa tidak ditaruh di atas yang basah supaya di lihat orang siapa yang menipu tidak termasuk golonganku" (H.R. Muslim).¹⁵⁴

Dapat dikatakan bahwa tipu muslihat termasuk dalam perbuatan memanipulasi atau memperdayai orang lain dengan akal licik. Tindakan tersebut pada dasarnya mengandung kebathilan atau kebohongan yang merupakan salah satu perbuatan yang di larang, sebagaimana dijelaskan dalam surah Al-baqarah: 42, Allah SWT berfirman:

وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ وَتَكُنُوا لِلْحَقِّ وَالْبَاطِلِ وَأَنْتُمْ تَعْلَمُونَ

Artinya: "Dan janganlah kamu campur adukkan kebenaran dengan kebatilan dan (janganlah) kamu sembunyikan kebenaran, sedangkan kamu mengetahuinya".

¹⁵⁴ Munanda, M., Kamaruzzaman, K., & Sholihin, R. (2020). "Hukuman Tindak Pidana Penipuan Dengan Menggunakan Identitas Palsu Ditinjau Dari Hukum Islam (Analisis Putusan Nomor 164/Pid. B/2016/PN. Bna)". *Dusturiyah: Jurnal Hukum Islam, Perundang-undangan dan Pranata Sosial*, Vol 10, No 1, Halaman 53-54

Sebagaimana juga yang disebutkan dalam Al-Qur'an surah An-Nahl (16):

105, Allah SWT berfirman:

إِنَّمَا يَفْتَرِى الْكُذِبَ الَّذِينَ لَا يُؤْمِنُونَ بِآيَاتِ اللَّهِ وَأُولَئِكَ هُمُ الْكَذِبُونَ

Artinya: "Sesungguhnya yang mengada-adakan kebohongan, hanyalah orang yang tidak beriman kepada ayat-ayat Allah, dan mereka itulah pembohong".

Terdapat sebuah riwayat hadist dari Rasulullah SAW terkait dengan privasi dan pentingnya menjaga sebuah kerahasiaan suatu hal. Contohnya hadits riwayat Anas yang gamblang meng gambarkannya:

عَنْ أَنَسٍ قَالَ أَتَى عَلِيَّ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ وَأَنَا أَلْعَبُ مَعَ الْعِلْمَانِ قَالَ فَسَلَّمْ عَلَيْنَا فَبَعَثَنِي إِلَى حَاجَةٍ فَأَبْطَأْتُ عَلَى أُمِّي فَلَمَّا جِئْتُ قَالَتْ مَا حَبَسَكَ قُلْتُ بَعَثَنِي رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ الْحَاجَةَ قَالَتْ مَا حَاجَتُهُ قُلْتُ إِنَّهَا سِرٌّ قَالَتْ لَا تُحَدِّثَنَّ بِسِرِّ رَسُولِ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ أَحَدًا قَالَ أَنَسُ وَاللَّهِ لَوْ حَدَّثْتُ بِهِ أَحَدًا حَدَّثْتُكَ يَا نَابِثُ

Artinya: "Dari Anas dia berkata, "Saya pernah didatangi oleh Rasulullah SAW ketika saya sedang bermain dengan teman-teman yang lain. Kemudian beliau mengucapkan salam kepada kami dan menyuruh saya untuk suatu keperluan hingga saya terlambat pulang ke rumah. Sesampainya di rumah, Ibu bertanya kepada saya, Mengapa kamu terlambat pulang? Maka saya pun menjawab, "Tadi saya disuruh oleh Rasulullah untuk suatu keperluan. Ibu saya terus bertanya, Keperluan apa?" Saya menjawab, "Itu rahasia. Ibu saya berkata, 'Baiklah, Janganlah kamu ceritakan rahasia Rasulullah SAW kepada siapapun. Anas berkata, "Demi Allah, kalau saya boleh menceritakan rahasia itu kepada seseorang, maka saya akan menceritakannya kepadamu, hai Tsabit!" (HR Muslim no 4533).¹⁵⁵

Dalam hadist tersebut menjelaskan bahwa betapa pentingnya menjaga privasi orang lain, termasuk informasi pribadi milik orang lain.

¹⁵⁵ muiprov, 2022. pentingnya perlindungan pribadi menurut Islam, diakses dari <https://mirror.mui.or.id/tanya-jawab-keislaman/muamalah/42340/pentingnya-perlindungan-pribadi-menurut-perspektif-islam/> pada 5 Maret 2025 pukul 17:46 WIB

Dalam kitab-kitab fiqih Islam, perbuatan pidana dikenal dengan istilah jarimah atau jinayah. Menurut Abu Al-Hasan Al-Mawardi seorang alhi fiqih, "jarimah merupakan sebuah perbuatan yang dilarang oleh syariat atau syarat dan diancam dengan sanksi berupa had atau ta'zir, istilah jarimah merujuk pada sebuah larangan larangan Syara' yang apabila dilanggar akan dikenai hukuman yang telah ditetapkan oleh Allah SWT. Larangan tersebut bisa berupa melakukan perbuatan yang dilarang, atau sebaliknya, dengan meninggalkan perbuatan yang diperintahkan". Maka dalam hal ini dapat dipahami bahwa suatu tindakan baru dapat dianggap sebagai jarimah apabila dilarang Syara'.

Meskipun terdapat sebuah perbedaan istilah dikalangan para fuqaha mengenai istilah jinayah, akan tetapi perbedaan tersebut tidak prinsipil, Oleh karena itu, istilah jinayah dan jarimah pada dasarnya sama.¹⁵⁶ Jinayah atau Jarimah perbuatan-perbuatan yg dilarang oleh *syara'* yang diancam oleh Allah dengan hukuman *had* atau *ta'zir*.¹⁵⁷

Maka yang menjadi objek atau ruang lingkup fiqih Jinayah atau ruang lingkup Hukum Pidana Islam adalah hukum-hukum *syara'* yang menyangkut masalah tindak Pidana dan hukumannya, yaitu:

1. Perbuatan-perbuatan yang secara tegas dilarang oleh syari'at Islam karena bertentangan dengan nilai dan hukum yang telah ditetapkan oleh Allah SWT.
2. Yang dikenai dengan ancaman sanksi berupa hukuman had atau ta'zir sesuai dengan ketentuan syari'at.

¹⁵⁶ Hadiyanto, et.al, 2023, *Tindak Pidana Penipuan Menurut KUHP Dan Syariat Islam*, Jakarta Timur, Damara press, Halaman 37-38

¹⁵⁷ Rasta Kurniawati, 2021, *Hukum Pidana Islam*, Medan, Umsu press, Halaman 1

Hukuman merupakan sanksi yang diberlakukan untuk menegakkan keadilan dalam masyarakat, sebagai konsekuensi atas pelanggaran dalam melanggar aturan Syara'.

Dalam menetapkan aturan pidana, islam menggunakan dua pendekatan utama, yaitu:

1. Menetapkan hukuman berdasarkan nash atau ketentuan, yaitu: Tindak Pidana Zina, Qadzaf (menuduh zina), pencurian, perampokan, minum-minuman keras, Riddah (keluar dari Islam), Pemberontakan, pembunuhan dan Penganiayaan. Dalam hal ini tidak diberikan kesempatan kepada Ulil Amri untuk menetapkan hukuman yang menyimpang dari ketentuan al-Qur'an dan as-Sunnah, dan berlaku sepanjang masa.
2. Menyerahkan penetapannya kepada penguasa ataupun yang dimaksudkan seperti Hakim (Ulil Amri),¹⁵⁸ Dalam pandangan Islam kekuasaan kehakiman termasuk dalam Al- Qadla merupakan kekuasaan sebagai upaya mencari keadilan atau penyelesaian perkara hukum berdasarkan Hukum positif dan Hukum Islam, dalam menentukan hukuman yang sesuai, Bukan hanya dalam perkara Jinayat (pidana) akan tetapi termasuk juga Madainiyat dan alahwal asy syakh syiyah (perdata).¹⁵⁹ Adapun Tindak Pidananya adalah selain 8 tindak pidana yang sudah disebutkan pada poin a diatas. Dalam hal ini Islam memberikan kesempatan yang luas kepada penguasa (ulil amri) kapasitas seorang hakim/penguasa bukan sekadar 'menegakkan aturan', melainkan

¹⁵⁸ *Ibid.*, Halaman 1-2.

¹⁵⁹ Farid, W, dan Suhrawardi, K, 2022, *Hukum Ekonomi Islam*, Jakarta: Sinar Grafika, Halaman 304

'menegakkan hukum' yang lebih efektif agar para pelaku menyesali perbuatannya,¹⁶⁰ dengan menetapkan macam-macam tindak pidana dan hukumannya.¹⁶¹

Ada beberapa penggolongan hukuman/sanksi (Al-uqubah) dalam hukum pidana Islam: pertama; jarimah *hudud*, kedua; jarimah *diyat* atau *qisas*, ketiga; jarimah *ta'zir*.¹⁶² sebagai berikut:

1. Jarimah hudud, Ada tujuh jenis jarimah hudud, yang hukumannya telah ditentukan, yaitu: zina (berhubungan seksual di luar nikah), gadzaf (menuduh orang lain berzina tanpa cukup bukti), khamar (minum-minuman keras), sariga (pencurian), qath'u al-thariq (perampokan), dan al-baghyu (pemberontakan).¹⁶³
2. Jarimah qisas-diyat yang terdiri, Pembunuhan sengaja (al-qathlu al-'amdu). Pembunuhan semi sengaja (al-qathlu syibhu al-'amdi). Pembunuhan karena kesalahan (tidak disengaja, al-qathu khata). Penganiayaan sengaja (al-jarhu al-'amdu). Penganiayaan tidak sengaja (al-jarhu khata).¹⁶⁴
3. Jarimah *ta'zir*, yaitu sebuah jarimah yang tidak di dalam jarimah hudud dan Jarimah qisas-diyat.¹⁶⁵

¹⁶⁰ Farid, W, et.al, 2019, *Memperkuat Peradaban Hukum dan ketatanegaraan Indonesia*, Jakarta: Sekretariat Jenderal komisi yudisial republik Indonesia, Halaman 146

¹⁶¹ Rasta., *Loc.cit*

¹⁶² Novalia, V., et.al. (2024). "Ta'zir Dalam Pidana Islam: Aspek Non Material". Terang: Jurnal Kajian Ilmu Sosial, Politik Dan Hukum, Vol 1, No 2, Halaman 225-234.

¹⁶³ Mardani, 2019, *Hukum pidana Islam*, Jakarta: Prenada Media Grup, Halaman 10

¹⁶⁴ Ibid., Halaman 12

¹⁶⁵ Rasta, *Op.cit.*, Halaman 30-31

Selain dari jarimah huduh dan qisas-diyat, jika dikaitkan dengan cybercrime dalam bentuk phising tersebut termasuk dalam golongan ta'zir. Jarimah ta'zir, merupakan bentuk larangan yang hukumannya tidak ditentukan secara spesifik oleh Syara', karena mencangkup segala macam perbuatan maksiat yang belum memiliki ketentuan hukuman yang jelas dalam Syara", sebab penentuan jenis hukuman jarimah ta'zir diserahkan pada otoritas penguasa, secara etimologis atau bahasa, ta'zir merupakan hukuman yang dapat dikatakan sebagai hukuman yang mendidik atas perbuatan dosa, dan ketentuan hukumannya tidak secara eksplisit diatur dalam syari'at Islam,¹⁶⁶ Melainkan diserahkan kepada Ulil Amri atau hasil ijtihad hakim untuk menetapkan, demi menegakkan keadilan dan menjadi kemaslahatan umat.¹⁶⁷

وعن جابر رضي الله عنه ، عن النبي صلى الله عليه وسلم قال : (ليسَ عَلَى حَائِنٍ وَلَا مُنْتَهَبٍ وَلَا
مُخْتَلَسٍ، قَطْعٌ) رواه أحمد، والأربعة، وصَحَّحَهُ التِّرْمِذِيُّ ، وَأَبْنُ حَبَّانَ

Jabir RA menceritakan, Nabi Muhammad SAW bersabda: "tidak ada hukuman potong tangan atas pengkhianat, pencopet dan perampok di jalan." (HR. Ahmad, Abu Daud, An-Nasa-y, At-Turmudzy dan Ibnu Majah).¹⁶⁸

Berdasarkan hadist di atas dapat disimpulkan bahwa perbuatan pengkhianat dan penipuan dapat dikatakan sama, maka bentuk hukuman yang tepat terhadap kejahatan seperti ini adalah melalui jarimah ta'zir yang penetapan

¹⁶⁶ *Ibid.*, Halaman 54

¹⁶⁷ Munanda, *Op.cit.*, Halaman 55-59

¹⁶⁸ Rahmi, N. (2018). "Hukuman Potong Tangan Perspektif Al-Quran Dan Hadis". Jurnal Ulunnuha, Vol 7, No 2, Halaman 58

hukumannya disesuaikan dengan tingkat kejahatan serta pertimbangan keadilan oleh hakim atau penguasa.¹⁶⁹

Para ulama fiqih mendefinisikan ta'zir sebagai bentuk hukuman yang wajib dijatuhkan atas pelanggaran terhadap hak Allah SWT maupun hak sesama manusia (Bani Adam), yang tidak memiliki batasan hukuman tertentu berdasarkan syariat Islam, dan juga tidak disertai dengan ketentuan kafarah. Hukuman ta'zir ini bersifat fleksibel dan beragam, secara garis besar bentuk bentuk hukuman ta'zir dapat diklasifikasikan kedalam empat kelompok, yaitu:

1. Hukuman ta'zir merupakan hukuman yang berkaitan langsung dengan fisik pelaku, jenis ini mencakup antara lain, seperti hukuman mati dan hukuman jilid.
2. Hukuman ta'zir merupakan yang mencakup aspek kemerdekaan seorang individu, yang bertujuan membatasi gerak pelaku sebagai bentuk rehabilitasi sosial maupun moral, bentuk hukuman ini berupa penjara, pembinaan serta pengasingan.
3. Hukuman ta'zir yang berkaitan dengan harta merupakan bentuk sanksi yang ditunjukkan untuk meninggalkan efek jahat melalui aspek finansial pelaku. jenis hukuman ini mencakup, denda, penyitaan, perampasan aset serta penghancur barang.

¹⁶⁹ Dewantara, G. M. (2023). Penegakan Hukum terhadap Pelaku Tindak Pidana Cyber Crime Metode Phising oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta (Doctoral dissertation, Universitas Islam Indonesia)

4. Hukuman-hukuman Ta'zir yang lainnya. Merujuk kepada bentuk bentuk sanksi yang tidak termasuk dalam kategori, hukuman fisik, kemerdekaan serta harta. akan tetapi masih dalam ruang lingkup kewenangan hakim, hukuman ini bersifat fleksibel dan disesuaikan dengan konteks tingkat pelanggaran, Yakni:

- a. Peringatan keras
- b. Diberi nasihat
- c. Celaan
- d. Pengucilan
- e. Pemecatan
- f. Penugumuman kesalahan secara terbuka

Hukuman ta'zir merupakan bentuk hukuman yang bertujuan memberikan efek jera dan pembinaan, terhadap para pelaku kejahatan yang tidak termasuk dalam kategori jarimah hudud, dan qisas-diyat. Dengan demikian bahwa pelanggaran pelanggaran ini tidak memiliki jenis dan kadar hukuman yang secara tegas diatur oleh syariat Islam. Jenis dan berat ringannya hukuman diserahkan sepenuhnya kepada penguasa atau hakim. Hukuman ini dapat dibatalkan apabila penguasa memberikan alasan pemaaf.

Maka jika dilihat jenis-jenis hukuman ta'zir tersebut di atas, maka hukuman hukuman yang diberikan kepada pelaku tindak pidana penipuan online dengan menggunakan platform digital WhatsApp dengan cara mengirimkan sebuah link yang merujuk kepada sebuah *website/domain* ataupun penginstalan apk berbahaya (*Malware*) terkait dengan Hukuman/sanksi (Al-Uqubah), maka

jarimah ta'zir cukup relevan jika dikenakan berdasarkan sebagaimana dikaitkan dengan tindak pidana *cybercrime* dalam bentuk phishing yang dengan cara mengirimkan sebuah link yang merujuk kepada suatu domain/website ataupun aplikasi yang berisi sebuah Malware.¹⁷⁰

Syari'at islam memberikan peringatan keras agar setiap individu menjauhi perbuatan yang dilarang, dengan menerapkan sanksi yang tidak hanya bersifat duniawi, tetapi juga disertai dengan ancaman hukuman akhirat. Sanksi akhirat berfungsi sebagai pengingat spritual, sementara hukuman duniawi menjadi instrumen nyata dalam menegakkan keadilan dan menjaga ketertiban sosial. Keduanya saling melengkapi dalam mencegah dan memberantas kejahatan.¹⁷¹

C. Perlindungan Hukum Dalam Bentuk Preventif Terhadap Korban Tindak Pidana Siber Phising Dengan Menggunakan Platform Digital WhatsApp

Serangan *cybercrime* berupa *phising* menjadi semakin marak dan canggih, menargetkan pengguna dengan metode yang semakin sulit diidentifikasi sebagai penipuan. Menurut Satjipto Raharjo yang dikutip oleh Luthvi Febryka Nola perlindungan hukum adalah “Suatu usaha untuk mengatur berbagai kepentingan dalam masyarakat agar tidak terjadi benturan antar kepentingan dan dapat menikmati segala hak yang diberikan oleh undang-undang”.¹⁷² Dari berbagai literatur yang dianalisis, ditemukan bahwa modus operandi *phising* di WhatsApp

¹⁷⁰ Syarbaini, A. (2023). “Konsep Ta’zir Menurut Perspektif Hukum Pidana Islam”. *Jurnal Tahqiqah: Jurnal Ilmiah Pemikiran Hukum Islam*, Vol 17, No 2, Halaman 45

¹⁷¹ *Ibid.*, Halaman 46

¹⁷² Koto, I., Lubis, T. H., & Sakinah, S. (2022). "Provisions of Legal Protection for Terrorism Victim in Order to Realize Constitution Order". *Volkgeist: Jurnal Ilmu Hukum dan Konstitusi*, 248

seringkali melibatkan pesan teks yang mengandung tautan mencurigakan. Tautan ini biasanya mengarahkan pengguna ke *website* palsu yang dirancang menyerupai situs resmi, maupun sebuah aplikasi berupa Malware, dengan tujuan mencuri informasi pribadi seperti data login, nomor kartu kredit, dan informasi keuangan lainnya.

Bahwa *website* palsu yang digunakan dalam serangan *phising* seringkali memiliki tampilan yang sangat mirip dengan situs asli, termasuk logo, desain, dan bahkan. URI. yang hampir sama. Hal ini membuat banyak pengguna yang kurang waspada mudah terperangkap dan memberikan informasi pribadi mereka tanpa curiga. Selain itu, penyerang sering kali menggunakan teknik sosial engineering untuk menambah kepercayaan pengguna, Dampak dari serangan *phising* ini sangat merugikan bagi korban. Tidak hanya kehilangan data pribadi dan finansial, tetapi juga mengalami kerugian emosional dan psikologis. Korban mungkin merasa cemas dan stres setelah menyadari bahwa mereka telah menjadi korban penipuan.

Dengan memberikan wawasan mendalam mengenai modus operandi *phising* di WhatsApp, dampak yang ditimbulkan, dan langkah-langkah pencegahan yang dapat diambil oleh pengguna. Dengan pemahaman yang lebih baik tentang ancaman ini, diharapkan pengguna WhatsApp dapat lebih waspada dan terlindung dari serangan *phising* yang merugikan. *Literature review* yang dilakukan juga menunjukkan bahwa peningkatan keamanan siber dan kesadaran pengguna merupakan kunci utama dalam melawan serangan *phising* yang semakin canggih dan sulit dideteksi.

Dengan memahami tanda-tanda peringatan dan menerapkan langkah-langkah pencegahan yang efektif, pengguna dapat mengurangi risiko terkena serangan phishing dan menjaga keamanan data pribadi mereka.¹⁷³

Adapun upaya preventif secara (komprehensif) berupa aspek, psikologis dan teknis, terhadap *cybercrime* dalam berupa *phishing* melalui WhatsApp yakni:

1. Tautan yang mencurigakan:

Sebelum mengklik tautan yang dikirim melalui pesan WhatsApp, sangat penting untuk memastikan bahwa. Langkah pertama yang harus dilakukan adalah melakukan pemeriksaan dengan teliti terhadap tautan yang diberikan oleh pelaku. Hal ini dikarenakan kejahatan phishing kerap menggunakan URL palsu atau melakukan modifikasi kecil pada URL resmi, misalnya dengan mengganti huruf, karakter atau domain yang menyerupai situs asli.

2. Pesan menekan atau darurat:

Pesan bernada mendesak atau menekan, merupakan salah satu taktik umum yang digunakan dalam serangan Phishing. Pelaku sengaja menyusun pesan agar seolah-olah bersifat sangat penting dan darurat, dengan tujuan untuk menanamkan rasa panik dan mendesak kepada korban agar segera mengklik tautan atau instruksi tanpa sempat berfikir untuk tenang. Oleh karena itu, setiap pesan yang menimbulkan tekanan berlebihan atau menuntut respon instan terutama jika disertai dengan tautan yang mencurigakan, harus

¹⁷³ *Ibid.*, Halaman 50

diwaspadai dan diverifikasi di kebenarannya sebelum mengambil tindakan lanjutan.

3. Permintaan informasi pribadi:

Permintaan informasi pribadi merupakan salah satu ciri utama dari serangan phishing. Pelaku sering kali mengirimkan sebuah pesan atau tautan yang tampak menakutkan, lalu meminta pengguna untuk memberikan informasi pribadi, data ini kemudian digunakan untuk kejahatan digital yang merugikan korban. pengguna harus selalu memastikan keaslian sumber dan waspada terhadap pesan seperti ini dan patuh dicurigai serta jangan memberikan informasi pribadi dengan begitu mudahnya tanpa adanya verifikasi secara sah.

4. Verifikasi logo dan grafis:

Jika pengirim pesan tersebut menampilkan sebuah logo atau grafis perusahaan pada profilnya, sebelumnya harus benar benar dipastikan terlebih dahulu bahwa akun tersebut benar benar resmi dan terverifikasi, Karena itu merupakan salah satu trik serangan Phising dengan meniru tampilan resmi, termasuk menggunakan logo, nama perusahaan ataupun desain visual lainnya, agar lebih menakutkan korban atau pengguna. Oleh karena itu verifikasi Keaslian akun sangat penting jangan hanya terpaku pada penampilan luar, Langkah awalnya selalu cek melalui sumber resmi yang dapat dipercaya sebelum merespon tautan tersebut.¹⁷⁴

¹⁷⁴ Trianurahmah, *Op.cit.*, Halaman 84-85

5. Menggunakan perangkat lunak keamanan yang kuat: seperti antivirus dapat membantu melindungi data pribadi dari serangan phishing. Antivirus yang diperbarui secara teratur dapat mendeteksi dan memblokir situs web phishing yang berbahaya.
6. Mengaktifkan fitur keamanan tambahan di WhatsApp: seperti verifikasi dua langkah, dapat memberikan lapisan perlindungan ekstra. Verifikasi dua langkah mengharuskan pengguna untuk memasukkan PIN selain kata sandi mereka, membuatnya lebih sulit bagi penyerang untuk mengakses akun.¹⁷⁵

Selain langkah-langkah ini, edukasi berkelanjutan tentang phishing sangat penting. Pengguna harus terus memperbarui pengetahuan mereka tentang teknik-teknik phishing terbaru dan tetap waspada terhadap tren serangan siber yang terus berkembang. Mengikuti berita keamanan siber dan mengikuti saran dari pakar keamanan dapat membantu pengguna tetap selangkah lebih maju dari penjahat siber. Dengan memahami tanda-tanda peringatan dan menerapkan langkah-langkah pencegahan yang efektif, pengguna dapat mengurangi risiko terkena serangan phishing dan menjaga keamanan data pribadi mereka.¹⁷⁶

Islam sebagai agama yang rahmatan lil alamin tidak hanya mengajarkan tentang ibadah spiritual, tetapi juga mengajarkan muamalah. Ini berisi pernyataan etis dan moral dalam kehidupan (*ethical and moral pronouncements in life*). Dalam menggali informasi, pengguna harus menggunakan proses pemikiran yang

¹⁷⁵ Isadora, *Op.cit.*, Halaman 49-50

¹⁷⁶ *Ibid.*, Halaman 50

mendalam dan logis serta etis. Memperhatikan modus operandi yang digunakan oleh para pelaku penipuan dan pencurian identitas yang disebutkan di atas, pengguna harus memahami hal-hal ini dan berhati-hati dengan berita apa pun di media sosial agar tidak menjadi korban materiil maupun immateriil. Mengingat informasi yang dibagikan terkadang mengandung tipuan.

Hoax adalah kata yang digunakan untuk menunjukkan berita palsu atau upaya untuk menipu atau mengakali pembaca agar percayainya. Ini adalah trik di mana seseorang memberi tahu orang tentang kebohongan. Di Indonesia, tahun 2016, hoax menjadi masalah nasional yang sangat mengkhawatirkan masyarakat.

Sebagai respon terhadap maraknya penyebaran informasi yang menyesatkan di era digital, Majelis Ulama Indonesia (MUI), menetapkan sebuah fatwa penting pada tahun 2017. Fatwa tersebut dikenal dengan sebutan Fatwa MUI No 24 tahun 2017 tentang hukum dan oed bermuamalah melalui media sosial. Melalui fatwa ini MUI memberikan landasan hukum dan etika dalam berinteraksi di ranah digital khususnya dalam menanggapi fenomena berita palsu yang menyesatkan

Meskipun fatwa ini tidak mengikat sebagai undang-undang, tetapi akan banyak dipatuhi oleh kebanyakan Muslim. Fatwa ini akan menjadi panduan dalam muamalah. Para ahli hukum Muslim memiliki banyak pendapat dalam kehidupan mereka, tetapi apa yang membuat pendapat mereka sebagai fatwa adalah bahwa itu adalah respons terhadap pertanyaan yang diajukan oleh mustafti (seseorang yang meminta fatwa). Keberadaan fatwa itu penting, mengingat perkembangan

muamalah kali ini sudah begitu pesat. Dengan demikian, masalah masyarakat menjadi sangat kompleks. Kasus saat ini tidak terjadi pada masa Rasulullah, sehingga membutuhkan fatwa.

Dalam hal ini, agama memiliki peran yang sangat signifikan sehingga nilai-nilai Islam dapat dijadikan pedoman bagi masyarakat. Ini diharapkan akan sangat memengaruhi aktivitas penggunaan media sosial. Beberapa identifikasi terkait nilai-nilai Islam yang diharapkan dapat mencegah masyarakat menjadi korban kejahatan dunia maya melalui media sosial khususnya cybercrime berupa phishing.

Sebagai bentuk pencegahan, Islam mengajarkan sebagai berikut:

1. Tabayyun (Klarifikasi)

Merujuk pada fatwa MUI No. Tahun 2017 yang dimaksud Media Sosial adalah media elektronik, yang digunakan untuk berpartisipasi, berbagi, dan membuat konten dalam bentuk blog, jejaring sosial, forum, dunia virtual, dan bentuk lainnya. Namun, sebelum meyakini informasi apa yang diperoleh, pengguna harus tetap waspada dan berhati-hati, dengan melakukan tabayyun. Penting bagi kita untuk menanamkan budaya tabayyun, yaitu memeriksa dan mengklarifikasi berita dan informasi sebelum menerimanya sebagai hal yang benar. Tabayyun sangat penting jika kita ingin berbagi dan meneruskan informasi kepada orang lain.¹⁷⁷

¹⁷⁷ Edy Santoso, *Op.cit.*, Halaman 175-176

Ini merujuk pada QS. al-Hujurat: 6 yang mengatakan "Hai orang-orang yang beriman, jika datang kepadamu orang fasik membawa suatu berita, maka periksalah dengan teliti agar kamu tidak menimpakan suatu musibah kepada suatu kaum tanpa mengetahui keadaannya yang menyebabkan kamu menyesal atas perbuatanmu itu." Ini menjadi penting, agar tidak hanya diri kita sendiri yang menjadi korban kejahatan cyber, tetapi juga pengguna lain yang mendapatkan informasi.

Tabayyun adalah langkah pertama, yang akan mencegah pengguna media sosial untuk menghindari semua bentuk kejahatan dunia maya. Tabayyun selalu membiasakan diri untuk menyelidiki dengan institusi atau orang yang berwenang mengenai masalah yang dihadapi. Pengguna harus benar-benar yakin, jika berita atau informasi berasal dari sumber yang dapat dipercaya. Dalam aktivitas dunia maya, pengguna harus menyelidiki nama domain situs web yang terhubung dalam "tautan (link)".

Sebagian besar kegiatan kejahatan cybercrime berupa phishing merupakan penipuan secara online dengan modus mengirimkan sebuah link maupun sebuah aplikasi yang merujuk ke sebuah domain dan virus, terutama dalam informasi terkait dengan sebuah masalah keamanan pada akun e-banking pengguna. Para pelaku, terampil dalam memprovokasi pemberitahuan kepada korban, sehingga korban secara emosional tidak menyadari bahwa si pengguna adalah seorang target korban. Prinsip tabayyun yang diajarkan oleh agama akan berperan dalam mengingatkan pengguna akan pentingnya melakukan penyelidikan dan klarifikasi sebelumnya, dan memberikan jeda waktu sebelum membuat keputusan.

2. Sabar (*Forbearing*)

Salah satu arti dari sabar atau *forbearing* adalah "*is to keep one-self from doing something*" atau menjaga diri dari melakukan sesuatu. Di sini, perilaku sabar untuk tidak terburu-buru merespons informasi di media sosial menjadi salah satu kunci untuk menghindari upaya penipuan di media sosial. Pelaku akan memanfaatkan situasi ini sebagai model untuk mencari mangsa. Bagi pengguna yang tidak sabar meneliti isi informasi, akan segera menjadi korban penipuan atau pencurian identitas.¹⁷⁸

Sifat tergesa-gesa ini, adalah sifat manusia untuk mendapatkan apa yang mereka inginkan. Seperti yang disebutkan dalam al-Isra: 11 yang berbunyi "Dan manusia (sering kali) berdoa untuk kejahatan sebagaimana (biasanya) dia berdoa untuk kebaikan. Dan memang manusia bersifat tergesa-gesa."

Lebih jauh, Hadis Nabi dari Anas ibn Malik melarang dengan tergesa-gesa, termasuk dengan tergesa-gesa untuk menyebarkan informasi sebelum ada kejelasan, karena perkataannya "Ketenangan adalah dari Allah, dan tergesa-gesa berasal dari setan."

Sifat sabar menjadi penting untuk memikirkan semua informasi yang dibaca pengguna sebelum bertindak. Nilai Islami ini sangat penting untuk memerangi tindak Pidana cybercrime berupa phishing.

3. Menjaga Kerahasiaan (*Keep Secrets*)

Korban kejahatan siber sangat tergantung pada pengguna. Identitas pribadi dan data keuangan adalah hal-hal yang harus dirahasiakan. Dalam hal ini, setiap

¹⁷⁸ *Ibid.*, Halaman 177

undang-undang yang dibuat oleh pemerintah, dan juga sistem keamanan yang dirancang oleh penyedia layanan tanpa partisipasi pengguna itu sendiri akan sulit untuk dicapai. Kegigihan dalam memelihara informasi penting adalah kata kunci untuk menghindari para korban kejahatan di dunia maya. Pengguna telah memainkan peran penting untuk menjaga rahasia pribadi yang penting Dalam hal ini, nilai-nilai agama Islam melarang untuk memberi tahu rahasia pribadi atau informasi lainnya kepada siapa pun. Identitas pribadi dan data adalah hal yang sangat rahasia.¹⁷⁹

¹⁷⁹ *Ibid.*, Halaman 178-179

BAB IV

KESIMPULAN DAN SARAN

A. KESIMPULAN

1. faktor kognitif untuk mengetahui penyebab utama mengapa pengguna terjebak dalam tindak pidana cybercrime berupa phishing, yaitu, pertama Suspicion (Kecurigaan), kedua Trust (Kepercayaan), ketiga Decision-Making (Pengambilan Keputusan), keempat Prediction (Prediksi). Penyebab terjadinya phising melalui WhatsApp tidak terlepas dari 2 faktor, faktor internal dan eksternal, Faktor Internal: pertama Kurangnya literasi pengguna terhadap teknologi pada media elektronik menjadi celah bagi pelaku. kedua kurangnya pengendalian emosi pengguna dalam menggunakan aplikasi online juga menjadi salah satu factor yang menyebabkan sebagian orang menjadi korban phising karena korban biasanya tidak dapat menolak, menanggapi ataupun membedakan tawaran yang ditujukan kepadanya.
2. Pemberitahuan berita bohong dengan merugikan kerugian materil terhadap korban/sebagai tindakan penipuan secara online, pemberitahuan berita bohong terhadap korban dengan tujuan untuk menguntungkan diri sendiri dengan merugikan kerugian materi terhadap korban dengan diaksesnya informasi elektronik berupa data pribadi korban (pasal 28 Jo pasal 45A, serta pasal merujuk ke sebuah website palsu yg menyerupai aslinya dijerat pasal 35 Jo pasal 51, tidak terlepas dari perbuatan penerobos sistem elektronik tanpa sepengetahuan pengguna, dijerat pasal pasal 35 Jo pasal 51 UU ITE. Dalam perbuatan pengumpulan data pribadi secara melawan hukum, maka pelaku phising dapat dijerat dengan pasal 45 ayat 1 dan 3 Jo pasal 47 ayat 1

dan 3 UU Perlindungan Data Pribadi, phishing merupakan Penipuan secara online, dan penipuan termasuk dalam kebohongan, maka berdasarkan pandangan Islam dalam melakukan perbuatan bohong, maka dapat dikategorikan sebagai Jarimah ta'zir yaitu berupa hukuman yang haknya ataupun kewenangannya diberikan oleh penguasa/hakim, berupa hukuman (al-uqubah) Hukuman ta'zir, seperti hukuman mati, penjara seperti denda.

3. Upaya Preventif secara integral (komprehensif) berupa aspek, psikologis, teknis dan sosia. Pertama terhadap Tautan yang mencurigakan, dengan memastikan link URL resmi dari pihak terkait, kedua Pesan menekan atau darurat: pesan yang menekan ataupun menyakinkan pengguna secara terus menerus patut dicurigai. ketiga Permintaan informasi pribadi, berupa permintaan pribadi sepatunya menjadi indikasi kecurigaan pengguna. keempat Verifikasi logo dan grafis: Jika pengirim pesan terdapat mencantumkan logo atau grafis perusahaan pada profilnya pastikan dulu. Phisher sering juga menggunakan taktik ini untuk mencoba meniru elemen desain. Adapun upaya preventif dalam hal teknis, Menggunakan perangkat lunak keamanan yang kuat seperti antivirus, Mengaktifkan fitur keamanan tambahan di WhatsApp, seperti verifikasi dua langkah.

B. SARAN

1. Terhadap pemerintah sebagai pihak pembentuk kebijakan, diharapkan untuk kedepannya harus memperhatikan masyarakat, dalam menggunakan teknologi terkhususnya Smartphone dengan menghimbau bahwa semakin banyaknya kejahatan dengan menggunakan elektronik khususnya melalui aplikasi

WhatsApp, agar lebih berhati-hati dalam menggunakan media tersebut, khususnya kejahatan dengan mengirimkan sebuah pesan singkat yang bertujuan untuk memberikan informasi pribadi pengguna.

2. Diharapkan juga terhadap pemerintah dalam hal Perundangan-undangan, bahwa undang-undang yang secara khusus mengatur kegiatan elektronik/jaringan internet/ ataupun aktivitas online, masih terdapat kekaburan dalam menjerat pelaku kejahatan *cybercrime*, khususnya *cybercrime* dalam bentuk phishing, bahwa undang-undang ITE tidak secara *eksplisit* mengatur tentang kejahatan tersebut secara jelas dan tegas.

DAFTAR PUSTAKA

A. Buku

- Amiruddin dan H.Zainal Asikin. 2004. *Pengantar Metode Penelitian Hukum*, Mataram PT Raja Grafindo
- Aristo M.A. Pangaribuan, dkk. 2020. *Pengantar Hukum Acara Pidana Di Indonesia*. Depok: Rajawali Pers. Hal 1.
- Danrivanto, 2017, *Revolusi cyber law Indonesia pembaruan dan revisi undang-undang informasi dan transaksi elektronik 2016*, Bandung, Refika aditama.
- Edy Santoso, 2023, *Hukum siber: permasalahan hukum bisnis di bidang teknologi informasi dan komunikasi*, Jakarta: Kencana.
- Fadlian, A, Santoso, B, dan Oktaviana, D, 2023, *Cyber crime dalam perkembangan ilmu*, Depok: RajaGrafindo Persada.
- Farid, W, Lubis, U. S., & Susanti, D. 2023, *Hukum Arbitrase dan Alternatif Penyelesaian Sengketa Bisnis: dilengkapi arbitrase online dan arbitrase syariah*, Jakarta: Sinar Grafika.
- Farid, W, dan Suhrawardi, K, 2022, *Hukum Ekonomi Islam*, Jakarta: Sinar Grafika.
- Farid, W, et.al, 2019, *Memperkuat Peradaban Hukum dan ketatanegaraan Indonesia*, Jakarta: Sekretariat Jenderal komisi yudisial republik Indonesia.
- Hadiyanto, et.al, 2023, *Tindak Pidana Penipuan Menurut KUHP Dan Syariat Islam*, Jakarta Timur, Damara press.
- Hani Dwiwahyu Oktavia, 2021. *Cybercrime*. Jakarta. pubhtml5.
- H. Ishaq. 2020. *Hukum pidana*. Depok. PT RajaGrafindo Persada.
- Hanafi, 2022, *Dasar Cyber Security dan Forensik*, Yogyakarta: Deepublish.
- Haryadi, 2012, *Kebijakan Integral penanggulangan cyberporn di Indonesia*, Semarang: V Lima.
- Ida Hanifah. et.al. 2018. *Pedoman Penulisan Tugas Akhir Mahasiswa*. Medan: CV. Pustaka Prima.
- Koto, I. & Faisal. 2022. *Hukum Perlindungan Saksi dan Korban*. Medan: Umsu press.

- Kermitsis, et.al, 2021. *Dark web markets. Dark web investigation*, Sheffield: CENTRIC Sheffield Hallam University, Halaman 85
- Muhaimin. 2020. *Metode Penelitian Hukum*. Mataram: Mataram University Press.
- Maskun, 2022, *Kejahatan siber (cybercrime)*, Jakarta: Kencana.
- Mardani, 2019, *Hukum pidana Islam*, Jakarta: Prenada Media Grup.
- Nugroho, C., Sos, S., & Kom, M. I. 2020. *Cyber Society: Teknologi Media Baru dan Disrupsi Informasi*. Jakarta. Prenada Media.
- Nudirman, 2017, *Pengantar Hukum siber Indonesia*, Depok: RajaGrafindo Indonesia.
- Nawangsasi, E, 2022, *Perlindungan privacy di era new normal digital lifestyle terkait cyber power*, Bandung: Refika adatama.
- Rahmawati D. 2024. *Waspada Kejahatan Phishing Attack*. Malang. PT. Literasi Nusantara Abadi Grup.
- Rasta Kurniawati, 2021, *Hukum Pidana Islam*, Medan, Umsu press, Halaman
- Silalahi, F. D. 2022. *Keamanan Cyber (Cyber Security)*. Semarang Penerbit Yayasan Prima Agus Teknik.
- Suyanto. 2018. *Pengantar Hukum Pidana*. Yogyakarta: Deepublish Publisher.
- Tofik Yanuar Chandra. 2022. *"Hukum Pidana"*. Jakarta: PT Sangir Multi Usaha.
- Zainuddin Ali. 2019. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

B. Jurnal

- Arif, E., & Roem, E. R. "Pemanfaatan media sosial". Jurnal Ranah Komunikasi JRK. Vol 3 No 1. 2019.
- Andiwijaya, D., & Liauw, F. "Pusat pengembangan kepercayaan diri". Jurnal Sains: Teknologi, Urban, Perancangan, Arsitektur (Stupa), Vol.1, No.2, 2019

- Azmi, M. N. A., et.al. "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan: Indonesia". Jurnal Multidisiplin Ilmu Akademik, Vol 3, No 2 2024
- Ablisar, M., et.al. "Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik": Studi Putusan No. 542/Pid. Sus/2019/PN. Mlg. Locus: Jurnal Konsep Ilmu Hukum, Vol 2, No 2, 2022
- Abroshan, H., et.al. "Phishing attacks root causes". In Risks and Security of Internet and Systems: 12th International Conference, CRiSIS 2017, Dinard, France, Revised Selected Papers 12. Springer International Publishing. 2018
- Antoni, A. "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online". Nurani: Jurnal Kajian Syari'ah dan Masyarakat. Vol 17. No 2. 2021.
- Butt, U. et.al. "Cloud-based email phishing attack using machine and deep learning algorithm". Journal: Complex & Intelligent Systems, Vol.9, No.3, 2023
- Banjarnahor, A. C., & Priyana, P. "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo". HERMENEUTIKA: Jurnal Ilmu Hukum, Vol 6, No 1, 2022
- Cholik, C. A. "Perkembangan teknologi informasi komunikasi/ICT dalam berbagai bidang". Jurnal Fakultas Teknik UNISA Kuningan. Vol 2. No 2. 2021.
- Dianti, S. D., & Nugroho, A. A. "Perlindungan Hukum Konsumen Pengguna Aplikasi E-Commerce Terhadap Kasus Penyalahgunaan Akun dalam Konstruksi Hukum ITE". Al Qalam: Jurnal Ilmiah Keagamaan dan Kemasyarakatan, Vol.17, No.2, 2023
- Fikri, A. W. N., Fauzi, A., Rachman, A. A., Khaerunisa, A., Sari, D. P., Vernanda, P., ... & Fadyanti, T. P. "Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking". Jurnal Ilmu Multidisplin, Vol 2. No 1, 2023
- Fadlian, A. "Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis". Jurnal Hukum Positum. Vol 5. No 2. 2020.
- Ferrary, A. A. I., Hartini, S., & Purwaningsih, P. "kajian hukum terhadap tindak pidana cyber phising yang digunakan untuk mengambil data pribadi pada situs trading dihubungkan dengan undang-undang nomor 19 tahun 2016

tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi transaksi dan elektronik". Yustisi. vol 10. No 2. 2023.

Harahap, A. Z., & Marpaung, Z. A. "Criminal Law Enforcement Against Cyber Phishing Perpetrators". LEGAL BRIEF. Vol 13. No 5. 2024.

Hashim, N., & Razali, A. "Teknologi dan media sosial dalam komunikasi ibubapa dan anak-anak". Jurnal Komunikasi: Malaysian Journal of Communication. Vol 35. No 4. 2019.

Habibi, M. R., & Liviani, I. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia". Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam. Vol 23. No 2. 2020

Indaryani, E. & Suliworo. D. (2018). "Dampak Pemanfaatan Dalam Meningkatkan Motivasi Belajar Siswa Pada Pelajaran Fisika". Prosiding Seminar Nasional Quantum. Vol 25. No. 2. 2018.

Isadora, et.al. "Analisis Modus Phishing Whatsapp". Jurnal Akuntansi, Bisnis dan Ekonomi Indonesia. Vol 3. No 2. 2024.

Jasrial, D. "Utilizing WhatsApp application for teaching English language Why and how. unsri: In International Seminar and Annual Meeting" Vol. 1, No. 1. 2019.

Jaiswal, M. "cybercrime categories and prevention". Manishaben Jaiswal: International Journal of Creative Research Thoughts (IJCRT), ISSN, Vol. 7, No.1, 2019

Jasin, H., et.al. "Apakah Kepercayaan Memediasi Pengaruh Reputasi Bank dan Religiusitas Terhadap Purchase Intention". Jurnal Ilmiah: Manajemen dan Bisnis, Vol.22. No.1, 2021

Koto, I. "Cyber crime according to the ITE law. International Journal Reglement & Society". IJRS, Vol 2. No 2. 2021.

Koto, I., Lubis, T. H., & Sakinah, S. "Provisions of Legal Protection for Terrorism Victim in Order to Realize Constitution Order". Volksgeist: Jurnal Ilmu Hukum dan Konstitusi, 2022.

Koto, I, & Rahimah, R. "Implications of parenting patterns in the development of early childhood social attitudes". International Journal Reglement & Society (IJRS), Vol 3, No 2, 2022.

Ketaren, E. Cybercrime, cyber space, dan cyber law". Medan. Jurnal Times. Vol 5. No 2. 2016.

- Lukiyana, L. "Pengaruh Perkembangan Teknologi Aplikasi Smartphone Dan Self Management Terhadap Sikap Dan Perilaku Generasi Milenial Yang Di Moderasi Oleh Kecerdasan Emosional". Media Manajemen Jasa. Vol 8. No 1. 2020.
- Marelino, A. "Understanding the Types of Cyber Crime and Its Prevention". Mathematical Statistician and Engineering Applications, Vol. 71, No.1, 2022
- Munanda, M., Kamaruzzaman, K., & Sholihin, R. (2020). Hukuman Tindak Pidana Penipuan Dengan Menggunakan Identitas Palsu Ditinjau Dari Hukum Islam (Analisis Putusan Nomor 164/Pid. B/2016/PN. Bna). Dusturiyah: Jurnal Hukum Islam, Perundang-undangan dan Pranata Sosial, Vol 10, No 1, 2020
- Malunsenge, L., Massie, C., & Rorie, R. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia". Lex Crimen. Vol 11. No 3. 2022.
- Mulyadi, M., et.al. "Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi". Jurnal: Media Hukum Indonesia (MHI), Vol. 2, No.2, 2024
- Muin, I. Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia. Journal Law And Justice, Vol 1, No 2. 2023
- Novalia, V., et.al. "Ta'zir Dalam Pidana Islam: Aspek Non Material. Terang: Jurnal Kajian Ilmu Sosial", Politik Dan Hukum, Vol 1, No 2, 2024
- Manorek, B. D. (2025). Penegakan hukum pidana dalam memberantas kejahatan pencurian data elektronik (phising)", Lex: privatum, Vol 15, No 2, 2025
- Omar, M. N. A. The impact of using WhatsApp groups on the Palestinian university students' productive skills improvement (Doctoral dissertation, Master's thesis, An-Najah National University. 2021.
- Prastya, M. W. A., "Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Review Metode Studi Literatur". Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), Vol 7, No 3, 2024
- Putra, I. K. O. K., Darmawan, I. M. A., & Juliana, I. P. G. "Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phising". Cyber Security Dan Forensik Digital. Vol 5 No 2. 2023.

- Priatna, et.al. "Pengaruh Efektivitas Platform Digital Terhadap Kinerja Pegawai Dinas Arsip Dan Perpustakaan Kabupaten Sumedang". *JRPA-Journal of Regional Public Administration*. Vol 7. No 2. 2022.
- Pittaro, M. L. "Cyber stalking An analysis of online harassment and intimidation". *International journal of cyber criminology*, Vol.1, No.2, 2007
- Putri, I. E. "Analisis Yuridis Putusan Hakim Dalam Perkara Tindak Pidana Phising Yang Dilakukan Melalui Media Sosial:(Studi Putusan Nomor: 155/Pid. Sus/2018/PN. Cbn)". *Delicti: Jurnal Hukum Pidana Dan Kriminologi*, Vol 1, No 1, 2023
- Rahmi, N. "Hukuman Potong Tangan Perspektif Al-Quran Dan Hadis". *Jurnal Ulunnuha*, Vol 7, No 2, 2018
- Saputra Gulo, A., Lasmadi, S., & Nabawi, K. :Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik". *pampas: Journal Of Criminal*, Vol.1, No.2, 2020
- Syarbaini,A. "Konsep Ta'zir Menurut Perspektif Hukum Pidana Islam". *Jurnal Tahqiqah: Jurnal Ilmiah Pemikiran Hukum Islam*, Vol 17, No 2, 2023
- Saputra, D., & Marpaung, Z. A. "Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh Paid Verified Account Di Media Sosial Menurut Undang-Undang Perlindungan Data Pribadi". *UNES Law Review*, Vol 5, No 4, 2023
- Shodiq, I. J. F., & Zainiyati, H. S. "Pemanfaatan media pembelajaran E-Learning menggunakan Whastsapp sebagai solusi ditengah penyebaran Covid-19 di MI Nurulhuda Jelu". *Al-Insyiroh: Jurnal Studi Keislaman*, Vol 6. No 2. 2020.
- Sari, N. W. "Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer". *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*. Vol 5. No 2. 2018.
- Sambodo, C. G., & Wahyuningsih, S. E. "The Criminal Law Enforcement Against Crime Of Carding In Electronic Transactions". *Law Development Journal*. Vol 3. No 2. 2021.
- Sutarli, A. F., & Kurniawan, S. "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia". *Innovative: Journal Of Social Science Research*, Vol 3, No 2, 2023

- Siregar, N. M.. "Pemanfaatan Aplikasi Whatsapps sebagai Media Pembelajaran Prodi Komunikasi Penyiaran Islam (KPI) Fakultas Dakwah Dan Ilmu Komunikasi". Hikmah, Vol.17, No.1, 2023
- Suharto, B., & Kurniawan, A. B.. "Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising)". Jurnal:JHP, No.17, 2020
- Trianurahmah, A. "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspada Maraknya Kejahatan Phising Dengan Modus Berbasis Link". Orbit: Jurnal Ilmu Multidisiplin Nusantara, Vol 1, No 2, 2024
- Wiriany, D., Natasha, S., & Kurniawan, R. "Perkembangan Teknologi Informasi dan Komunikasi terhadap Perubahan Sistem Komunikasi Indonesia". Jurnal Nomosleca. Vol 8. No 2. 2022.
- Yulianti, N. P. R., & Pramita, K. D. "Analysis of Workload, Rest Rights, and the Rights to Enjoy Entertainment in Gender Differences". Jurnal Komunikasi Hukum JKH. Vol 8. No 1. 2022.
- Yeboah-Boateng, E. O., & Amanor, P. M. "Phishing, SMiShing & Vishing an assessment of threats against mobile devices". Journal of Emerging: Trends in Computing and Information Sciences, Vol.5, No.4, 2014

C. Skripsi

- Devi, N. A. R. 2023. Kejahatan phising dengan modus link undangan pernikahan di sosial media menurut undang undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (Doctoral dissertation, UNIVERSITAS SINTUWU MAROSO).
- Dewantara, G. M. (2023). Penegakan Hukum terhadap Pelaku Tindak Pidana Cyber Crime Metode Phising oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta (Doctoral dissertation, Universitas Islam Indonesia)
- Prasetyo, R. A. 2023. "Analisis hukum terhadap praktik phising dalam game online". (Doctoral dissertation, Wijaya Kusuma Surabaya University.
- Khairunnisa, A. 2021. Perlindungan Konsumen Dalam Transaksi E-Commerce Platform Bukalapak (Bachelor's thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta). Halaman 88

Ramadhan, A. D. R. 2023. Analisis yuridis tindak pidana eksploitasi ekonomi dan seksual terhadap anak melalui aplikasi michat. Universitas Hasanuddin. Doctoral dissertation. Semarang.

Suryani, R. 2017. "Fungsi Whatsapp Grup Shalihah Cabang Bandar Lampung Sebagai Pengembangan Media Dakwah Dalam Membentuk Akhlakul Karimah". (Doctoral dissertation, UIN Raden Intan Lampung.

D. Perundang Undangan

Undang- Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang- Undang Nomor 1 Tahun 2024 Perubahan atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

E. Internet

Mega. "Mengenal Phising, Jenis Kejahatan Cyber yang Berbahaya", <https://www.megasyariah.co.id/id/artikel/edukasi-tips/lainnya/phising>.

muiprov, 2022. pentingnya perlindungan pribadi menurut Islam, diakses dari <https://mirror.mui.or.id/tanya-jawab-keislaman/muamalah/42340/pentingnya-perlindungan-pribadi-menurut-perspektif-islam/>

<https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/bacaartikel/14851/Waspada-Kehajatan-ishing-Mengintai-Anda.html>.

Sumiati. 2017. Bahaya menyebarkan berita bohong dalam pandangan Islam. diakses dari <https://kalbar.kemenag.go.id/berita/berita.php?nid=4539>.

Nurul, 2025. "Tidak jujur tanda munafik", diakses dari <https://iainutuban.ac.id/2025/02/13/tidak-jujur-tanda-munafik/#:~:text=Rasulullah%20bersabda%3A%20%E2%80%9CBerbohong%20adalah%20salah,jika%20diberi%20amanat%20ia%20berkhianat>.

Rita Puspita Sari. "Waspada Ancaman Phishing Lewat WhatsApp, Bisa Bobol Rekening". <https://www.cloudcomputing.id/berita/phishing-lewat-whatsapp>.

Diskominfo. "29 Juta Serangan Siber Diblokir di Indonesia Selama 2023". <https://kominfo.lhokseumawekota.go.id/berita/read/>.

Ratna Patria, "Platform Digital adalah: Pahami Jenis-Jenis Platform Digital"
<https://www.dominesia.com/berita/platform-digital-adal>