

**ANALISIS YURIDIS TERHADAP TINDAK PIDANA PHISING
(ANALISIS PUTUSAN NO.60/PID.SUS/2022/PN.BJR)**

SKRIPSI

**Disusun Dalam Rangka Pemenuhan
Tugas Akhir Mahasiswa**

Oleh:

Sahvina Alisya Dewi

2006200069



UMSU

Unggul | Cerdas | Terpercaya

**FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2024**



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

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 **Jum'at**, Tanggal **18 Oktober 2024**, Jam 08.30 WIB sampai dengan selesai, setelah Mendengar, Melihat, Memperhatikan, Menimbang :

MENETAPKAN

NAMA : Sahvina Alisya Dewi
NPM : 2006200069
PRODI/BAGIAN : HUKUM/HUKUM PIDANA
JUDUL SKRIPSI : ANALISIS YURIDIS TERHADAP TINDAK PIDANA PHISING (ANALISIS PUTUSAN NO.60/PID.SUS/2022/PN.BJR)

Dinyatakan : (A) Lulus Yudisium Dengan Predikat **Istimewa**
() Lulus Bersyarat, Memperbaiki/Ujian Ulang
() Tidak Lulus

Setelah lulus dinyatakan berhak dan berwenang mendapatkan gelar **Sarjana Hukum (SH)** 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 : 018047901

Anggota Penguji :

1. Dr. GUNTUR RAMBEY, S.H., M.H.
2. Dr. RACHMAD ABDUH, S.H., M.H.
3. TAUFIK HIDAYAT LUBIS, S.S., S.H., M.H.





1.

2.

3.



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

PENETAPAN
HASIL UJIAN SKRIPSI MAHASISWA FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

Berdasarkan Berita Acara Ujian Skripsi yang dilaksanakan pada hari **Jum'at** tanggal **18 Oktober 2024**. Panitia Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dengan ini menetapkan bahwa :

Nama : Sahvina Alisya Dewi
NPM : 2006200069
Prodi/Bagian : HUKUM/HUKUM PIDANA
Judul Skripsi : ANALISIS YURIDIS TERHADAP TINDAK PIDANA PHISING
(ANALISIS PUTUSAN NO.60/PID.SUS/2022/PN.BJR)

Penguji :

1. Dr. GUNTUR RAMBEY, S.H., M.H	NIDN. 0113087101
2. Dr. RACHMAD ABDUH, S.H., M.H	NIDN. 0004127204
3. TAUFIK HIDAYAT LUBIS, S.S., S.H., M.H	NIDN. 0113118604

Lulus, dengan nilai **A**, Predikat **Istimewa**

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

PANITIA UJIAN

Ketua

Sekretaris


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





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

PENGESAHAN SKRIPSI

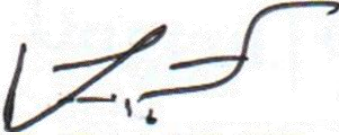
Judul : ANALISIS YURIDIS TERHADAP TINDAK PIDANA PHISING
(ANALISIS PUTUSAN NO.60/PID.SUS/2022/PN.BJR)
Nama : Sahvina Alisya Dewi
NPM : 2006200069
Prodi/Bagian : Hukum/Hukum Pidana

Skripsi tersebut diatas telah diujikan oleh Dosen Penguji Fakultas Hukum Universitas Muhammadiyah Sumatera Utara pada tanggal 18 Oktober 2024.

Dosen Penguji

		
<p>(Dr. GUNTUR RAMBEY, S.H., M.H.) NIDN. 0113087101</p>	<p>(Dr. RACHMAD ABDUH, S.H., M.H.) NIDN : 0004127204</p>	<p>(TAUFIK HIDAYAT LUBIS, S.S., S.H., M.H.) NIDN : 0113118604</p>

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.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

Salah satu surat ini agar disebutkan
Nomor dan tanggalnya

BUKTI PENDAFTARAN UJIAN SKRIPSI

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

Nama : SAHVINA ALISYA DEWI
NPM : 2006200069
Prodi/Bagian : HUKUM/HUKUM PIDANA
Judul skripsi : ANALISIS YURIDIS TERHADAP TINDAK PIDANA
PHISING (ANALISIS PUTUSAN
NO.60/PID.SUS/2022/PN.BJR)
Dosen Pembimbing : TAUFIK HIDAYAT LUBIS, S.S., S.H., M.H.
(NIDN. 0113118604)

Selanjutnya layak untuk diujikan

Medan, 14 Oktober 2024

PANITIA UJIAN

Ketua

Sekretaris

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

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



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](https://www.facebook.com/umsumedan) [umsumedan](https://www.instagram.com/umsumedan) [umsumedan](https://www.twitter.com/umsumedan) [umsumedan](https://www.youtube.com/umsumedan)

Bila menjawab surat ini agar disebutkan
Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA : Sahvina Alisya Dewi
NPM : 2006200069
PRODI/BAGIAN : HUKUM/HUKUM PIDANA
JUDUL SKRIPSI : ANALISIS YURIDIS TERHADAP TINDAK PIDANA PHISING
(ANALISIS PUTUSAN NO.60/PID.SUS/2022/PN.BJR)

Disetujui untuk disampaikan kepada
Panitia ujian skripsi

Medan, 12 Oktober 2024

Dosen Pembimbing

TAUFIK HIDAYAT LUBIS, S.S., S.H., M.H.

NIDN. 0113118604



FAKULTAS HUKUM

Bila dianggap sudah selesai ditandatangani
Maka ditandatangani

KARTU BIMBINGAN SKRIPSI

Nama : SAHVINA ALISYA DEWI
NPM : 2006200069
Prodi/Bagian : Hukum/ Hukum Pidana
Judul Skripsi : Analisis Yuridis Terhadap Tindak Pidana Pengabaian
(Physing) (Analisis Putusan No.60/Pid.Sus/2022/PN.BJR)
Pembimbing : Taufik Hidayat Lubis, S.S., S.H., M.H

No.	TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
	28 November 2023	Diskusi Judul dan Rumusan masalah	
	20 Desember 2023	Bimbingan pertama setelah Acc Judul, Studi Pustaka dan Rumusan masalah	
	10 Januari 2024	Revisi bab 1 dan Revisi bab 2	
	28 Mei 2024	Acc Seminar proposal	
	21 Juli 2024	Bimbingan setelah Seminar proposal	
	28 September 2024	Bimbingan Revisi Bab 3 Pembahasan 1	
	30 September 2024	Revisi Bab 3 Pemb 2 dan Pemb 3	
	11 Oktober 2024	Revisi Bab 3 Pemb 1, 2 & 3 keseluruhan	
	12 Oktober 2024	ACC Skripsi	

Mahasiswa dengan data dan judul skripsi tersebut di atas telah melalui proses bimbingan dan telah dilakukan pemeriksaan terhadap daftar pustaka, oleh karenanya skripsi tersebut disetujui untuk diujikan.

Medan, 11 Oktober 2024

Diketahui,
Dekan Fakultas Hukum

Dosen Pembimbing

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

Taufik Hidayat Lubis, S.S., S.H., M.H
NIDN : 0113118604



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 [f](#) umsumedan [i](#) umsumedan [t](#) umsumedan [y](#) umsumedan

Bila menjawab surat ini agar disebutkan
Nomor dan tanggalnya

PERNYATAAN KEASLIAN SKRIPSI

Saya mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara yang bertandatangan di bawah ini :

NAMA : Sahvina Alisya Dewi
NPM : 2006200069
PRODI/BAGIAN : HUKUM/HUKUM PIDANA
JUDUL SKRIPSI : ANALISIS YURIDIS TERHADAP TINDAK PIDANA PHISING
(ANALISIS PUTUSAN NO.60/PID.SUS/2022/PN.BJR)

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 Oktober 2024
Saya yang menyatakan,



SAHVINA ALISYA DEWI
NPM. 2006200069

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji Syukur peneliti haturkan kepada Allah Subhanahu Wa ta'ala, Alhamdulillah atas Rahmat, Karunia, dan Hidayah-Nya peneliti dapat menyelesaikan skripsi dengan judul: "Analisis Yuridis Terhadap Tindak Pidana *Phishing* Analisis Putusan no.60/Pid.Sus/2022/Pn.Bjr" dengan baik dan maksimal. Secara khusus dengan rasa hormat serta penghargaan yang setinggi-tingginya penulis ucapkan terima kasih kepada kedua orang tua peneliti yang senantiasa memberikan dukungan, semangat dan doa selama melakukan penulisan skripsi ini. Skripsi ini tidak akan berjalan lancar tanpa ridho dari kedua orang tua peneliti. Terima kasih untuk kedua orang tua yang telah memberikan segala kebutuhan dan memberikan tempat ternyaman sehingga peneliti mampu menyelesaikan skripsi ini. Sholawat dan salam kepada Rasulullah Muhammad Shalallahu'Alaihi Wasallama yang telah menjadi suri tauladan terbaik bagi peneliti.

Penyusunan skripsi ini dilakukan dengan maksud untuk memenuhi salah satu syarat dalam menempuh ujian Tingkat Sarjana Strata 1 (S1) pada Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Muhammadiyah Sumatera Utara. Peneliti menyadari dalam penyusunan skripsi ini tidak terlepas dari doa, dukungan, bantuan, bimbingan, dan semangat yang diberikan dari berbagai pihak baik berupa moril maupun materil. Untuk itu, dalam kesempatan ini peneliti mengucapkan banyak terima kasih kepada :

1. 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.
2. 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.**
3. Bpk. **Dr. Faisal Riza S.H.,M.H** selaku Kepala Bagian Hukum Pidana Fakultas Muhammadiyah Sumatera Utara.
4. Terima kasih yang tak terhingga dan penghargaan yang setinggi-tingginya diucapkan kepada Bapak **Taufik Hidayat Lubis S.S.,S.H.,M.H.** selaku Dosen Pembimbing yang dengan penuh perhatian telah memberikan dorongan, bimbingan dan arahan sehingga skripsi ini selesai.
5. Bapak dan Ibu seluruh Dosen Fakultas Hukum, Universitas Muhammadiyah Sumatera Utara. Terutama Bapak/Ibu Dosen Prodi Ilmu Hukum yang telah memberikan ilmu pengetahuan, mendidik dan membimbing peneliti selama perkuliahan. Rasa Hormat dan Bangga peneliti bisa berkesempatan diajarkan dan dibimbing oleh Bapak/Ibu dosen. Semoga Bapak/Ibu Dosen selalu dilimpahkan kesehatan, kemudahan, dan dalam lindungan-Nya.
6. Seluruh staf Tata Usaha Prodi, Fakultas dan Perpustakaan Fakultas Hukum, Universitas Muhammadiyah Sumatera Utara khususnya Bapak Syarif, Ibu Rahma,

yang telah membantu dan memudahkan segala urusan administratif peneliti selama berkuliah di Fakultas Hukum UMSU.

7. Kepada ayahanda tercinta **Alm.Sahman**, banyak hal yang menyakitkan saya lalui tanpa sosok ayah selama 2 tahun belakangan ini. Dihadapi oleh kenyataan yang tidak sesuai dengan harapan saya. Rasa iri dan rindu yang sering kali membuat saya terjatuh dan kemudian bangkit dari kenyataan. Tapi itu semua tidak mengurangi rasa bangga dan terima kasih atas kehidupan yang diberikan Ayah saya kepada peneliti semasa hidup selama 20 tahun dengan anda. Maka, peneliti mempersembahkan tulisan ini untuk Ayah saya.
8. Kepada ibunda **Sri Dewi yani**, Wanita hebat yang melahirkan peneliti dan sosok seorang Ibu yang mempunyai pintu surga di telapak kakinya, terima kasih atas limpahan doa yang tak berkesudahan, selalu berada di sisi peneliti saat terpuruk, dukungan yang selalu diberikan kepada penulis. Sebagai tanda bakti, hormat dan rasa terima kasih yang tak terhingga kupersembahkan karya sederhana ini untuk ibu.
9. Kepada **Hanna Sadeya Safira** dan **Sri Satika Indah Mawarni** selaku kakak kandung peneliti, terima kasih selalu mendukung peneliti, selalu menjadi tempat keluh kesah saat tidak baik- baik saja, terima kasih atas dukungan yang selalu kalian berikan dan kerja keras kalian untuk memenuhi kebutuhan peneliti secara materi. Dan juga seluruh keluarga Almarhum Sahman yang selalu memberikan dukungan besar kepada peneliti.

10. Kepada **Dhe Ajeng Ghufrana** dan **Nibella Sativa** selaku sahabat dari saya duduk dibangku perkuliahan yang telah menjadi tempat berkeluh kesah, saling menyemangati, dan mendukung selama proses perkuliahan penyelesaian skripsi.
11. Kepada teman-teman peneliti Hukum 2020 di bangku perkuliahan yang telah kebersamai peneliti dalam masa perkuliahan dan pengerjaan skripsi ini tiada henti untuk saling menyemangati.
12. Kepada seluruh pihak yang turut membantu memberikan masukan, motivasi, dukungan dan doa baik secara langsung maupun tidak langsung yang tidak dapat peneliti sebutkan satu persatu. Semoga Allah Subhanahu Wata'ala membalas ketulusan hati dan kebaikan yang telah diberikan kepada peneliti.
13. Dan yang terakhir kepada diri peneliti sendiri **Sahvina Alisya Dewi**. Terima kasih sudah berjalan sejauh ini, terima kasih tetap memilih berusaha dan merayakan sendiri hingga detik ini, walau sering mengeluh dan menangis sepanjang malam lalu bangkit lagi saat matahari mulai terbit. Namun peneliti bangga kepada diri sendiri, mari bekerja sama untuk lebih berkembang lagi dari hari ke hari, kehidupan dunia akan segera dimulai, mohon untuk tetap kuat dan semangat menjalani kehidupan di masa depan, sekali lagi terima kasih.

Peneliti berharap skripsi ini dapat membawa dampak positif bagi para pembaca, karena di dalam skripsi ini memuat pembelajaran yang peneliti dapatkan selama penelitian berlangsung. Dalam hal ini, peneliti tidak menutup diri untuk menerima kritik dan saran yang sekiranya bisa menjadi pembelajaran bagi peneliti untuk

berkembang menjadi lebih baik lagi.

Medan, 12 Oktober 2024

Peneliti,

Sahvina Alisya Dewi

2006200069

ABSTRAK

ANALISIS YURIDIS TERHADAP TINDAK PIDANA *PHISING* (Analisis

Putusan No.60/Pid.Sus/2022/Pn.Bjr)

Oleh

Sahvina Alisya Dewi

2006200069

Penelitian ini bertujuan untuk meneliti Tindak Pidana *Phising* dalam Putusan No.60/Pid.Sud/2022/Pn.Bjr. Dalam penelitian ini, akan menganalisis unsur-unsur perbuatan Tindak Pidana *Phising* berdasarkan Pengaturan Hukum Perundang-undang Informasi dan Transaksi Elektronik untuk mempertimbangkan putusan hakim dalam menjatuhkan putusannya. Sehingga dapat menentukan pertanggungjawaban pelaku atas Tindak Pidana *Phising* dalam Putusan Nomor 60/Pid.Sus/2022/Pn.Bjr.

Jenis penelitian skripsi ini adalah menggunakan jenis penelitian normative yaitu pendekatan studi kasus (case apoach). Adapun metode penelitian yang dipakai adalah studi kepustakaan (Library Research) dengan teknik pengumpulan menggunakan data sekunder yang terdiri dari bahan hukum primer, sekunder, dan tersier yaitu Perundangan-undangan, Buku, Jurnal Hukum dan Kamus Hukum Online. Penulis menganalisis putusan dan menemukan analisis tentang Tindak Pidana *Phising* berdasarkan Undang-Undang Informasi, Transaksi dan Elektronik.

Berdasarkan hasil penelitian, Pengaturan Hukum terhadap Tindak Pidana *Phising* berdasarkan Undang-Undang tentang Informasi dan Transaksi Elektronik masih mengalami kekaburan hukum karena pasal dalam Undang-Undang tentang Informasi dan Transaksi Elektronik belum ada yang mencakup semua unsur Tindak Pidana *Phising*. Hal itu disebabkan *Phising* termasuk suatu perbuatan melanggar hukum yang menyebabkan kerugian bagi orang lain. Kergian yang ditimbulkan dari tindak pidana ini merupakan suatu delik materiil, karena dalam perbuatannya telah merugikan berupa informasi pribadi yang diketahui oleh pelaku *phising*.

Kata Kunci : Tindak Pidana, Phising

DAFTAR ISI

KATA PENGANTAR.....	i
ABSTRAK	vii
DAFTAR ISI.....	ix
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah.....	1
1. Rumusan Masalah	6
2. Tujuan Penelitian.....	7
3. Manfaat Penelitian	7
B. Definisi Operasional.....	8
C. Keaslian Penelitian.....	9
D. Metode Penelitian.....	12
1. Jenis Penelitian.....	12
2. Sifat Penelitian	13
3. Pendekatan Penelitian	13
4. Sumber Data Penelitian.....	15
5. Alat Pengumpul Data	16
6. Analisis Data	16
BAB II TINJAUAN PUSTAKA.....	18
A. Tinjauan Umum Tentang Tindak Pidana.....	18
B. Tinjauan Umum tentang <i>Phising</i>	24

BAB III HASIL PENELITIAN DAN PEMBAHASAN	35
A. Pengaturan Hukum mengenai Tindak Pidana <i>Phising</i> Di Indonesia	35
B. Pertimbangan Hukum Oleh Hakim Dalam Putusan No.60/ Pid.Sus/ 2022/ Pn.Bjr	47
C. Pertnggungjaaban Pelaku Tindak Pidana <i>Phising</i> Dalam Putusan No.60/ Pid.sus/ 2022/ Pn.Bjr.....	59
BAB IV KESIMPULAN DAN SARAN	67
A. Kesimpulan	67
B. Saran.....	68
DAFTAR PUSTAKA	71

BAB I

PENDAHULUAN

A. Latar Belakang

Tujuan dari tulisan ini adalah untuk meneliti Tindak Pidana *Phising* dalam Putusan No.60/pid.sus/2022/PN.BJr yang mana peneliti akan menganalisis unsur-unsur perbuatan Tindak Pidana *Phising* berdasarkan Pertimbangan Majelis Hakim dalam Putusan No.60/pid.sus/2022/PN. BJr yang kemudian dikaitkan dengan isi Pasal 51 Ayat (1) Jo Pasal 35 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagaimana telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Tindak pidana *phising* ini diawali dengan perbuatan Terdakwa Maulana Malik Rahman bin Karim Ansori sedang melaminating Sertifikat kerja Ahli (SKA). Kemudian Terdakwa bermu dengan saksi M. Ichwanto bin Winarto yang sedang memfotokopi dokumen perencanaan proyek lain. Bermula saat M. Ichwanto bertanya kepada Maulana Malik Rahman yaitu "Pak sedang Melaminating SKA" dan Maulana Malik Rahman menjawab "ya pak akan dikirim keluar kota. Setelah itu terdakwa berkenalan dengan saksi dan bertukar nomor telepon.

Selanjutnya, setelah Maulana Malik Rahman memberi pesan kepada M. Ichwanto bahwa Maulana Malik Rahman bisa membuat Sertifikat Kompetensi Kerja (SKK) dan Sertifikat Badan Usaha (SBU) dengan menjanjikan proses cepat dan tanpa tes atau

assesmen, yang dimana M. Ichwanto diminta untuk membantu Maulana Malik Rahman mengurus pembuatan SKK milik korban. akan tetapi biaya yang dikirimkan oleh beberapa korban harus melalui persyaratan yang diminta oleh Maulana Malik Rahman melalui M. Ichwahto berupa dokumen KTP, Ijazah, NPWP dan foto.

Tindak pidana *phising* sebenarnya adalah jenis perbuatan yang baru dikenal di Indonesia, hal ini dapat ditinjau dari peraturan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Berbeda dengan negara Amerika Serikat yang sudah mengenal jauh lebih lama tentang tindak pidana *phising*. Hal ini dapat dilihat dalam peraturan Undang-Undang Keamanan Dalam Negeri Tahun 2002, yang mencakup Undang-Undang Manajemen Keamanan Informasi Federal dengan mengubah menjadi Undang-Undang Informasi Keamanan *cyber* antara Amerika Serikat dan perusahaan teknologi dan manufaktur.¹

Phising adalah salah satu kejahatan digital yang menargetkan informasi atau data sensitif korban melalui *e-mail*, unggahan media sosial, atau pesan teks dengan kata lain *phising* merupakan sebuah serangan yang dilakukan untuk menipu atau memancing korban agar mengklik link/tautan serta menginput informasi *financial* seperti *username* dan *password*.² Kejahatan ini sering kerap terjadi dan tidak sedikit yang mengalami kerugian akibat modus kejahatan *cyber* ini. Oleh karena itu, kejahatan *phising* adalah aktivitas yang sangat penting untuk perlu diwaspadai oleh setiap orang dari berbagai golongan agar tidak menjadi korban yang bertujuan mendapatkan data informasi

¹ United State Cyber Security Laws and Regulation

² *Ibid*, halaman 6

pribadi secara sukarela tanpa disadari untuk tujuan kejahatan. Oleh sebab itu, Tindak Pidana *Phising* akan diberantas sesuai dengan pengaturan hukum di Indonesia sehingga tidak ada korban yang terkena dampak dari kejahatan tindak pidana phishing.

Indonesia adalah negara hukum, semua tingkah laku manusia sebagai subjek hukum diatur oleh hukum. Hukum sebagai sarana dalam perubahan masyarakat ke arah yang lebih baik serta hukum berperan meluruskan keadaan yang sebelumnya rusak menjadi lebih baik lagi. Sifat manusia sebagai subjek hukum memang banyak melakukan kesalahan akan tetapi dengan adanya hukum, maka manusia dituntun dengan paksa ke arah yang lebih baik. Sebagai subjek hukum manusia tak lepas dari perbuatan yang baik dan perbuatan yang buruk. Perbuatan yang baik tentunya memberikan kebahagiaan bagi orang lain akan tetapi jika perbuatan manusia buruk akan memberikan kesusahan kepada orang lain, hal ini dapat disebut sebagai kejahatan.³

Sejarah *Phising* telah mengganggu dunia maya selama lebih dari 2 dekade, dimulai pada tahun 1995 dengan *America Online (AOL)* (James, 2006). Istilah *Phising* adalah variasi dari istilah memancing di mana tindakan *phising* menyerupai penangkapan ikan dengan cara berikut: penyerang “memancing” korban menggunakan “umpan” dan “memancing” untuk informasi pribadi atau rahasia korban. Studi komprehensif tentang definisi phishing dilakukan oleh *Lastdrager* (2014) dimana dia mengidentifikasi definisi phishing yang disepakati: Phising adalah tindakan penipuan yang dapat diskalakan di

³ Ferry Irawan Febriansyah. “Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional” *Jurnal Ilmu Hukum*, Vol.7 No. 2, 2023, Halaman 183.

mana peniruan identitas digunakan untuk mendapatkan informasi dari target. penyerang menggunakan berbagai saluran untuk menipu korban secara langsung dengan scam atau mengirimkan muatan melalui cara tidak langsung dengan tujuan untuk mendapatkan informasi pribadi atau rahasia dari korban.⁴

Pelaku *phising* juga sering memakai teknik ini untuk mendapatkan keuntungan bisa berupa uang elektronik maupun memakai user orang lain untuk melakukan tindakan kejahatan lain seperti, penyebaran hoax, ujaran kebencian dan lainnya dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.⁵

Kejahatan *Phising* ini telah diatur dalam undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pasal 35 jo. Pasal 51 ayat (1) dengan ancaman maksimal 12 tahun penjara dengan unsur delik dimana setiap orang yang melakukan manipulasi, menciptakan, merubah atau mentransmisikan, menghilangkan serta melakukan pengrusakan data atau sistem informasi elektronik dengan sengaja melakukan tindakan melawan hukum dengan tujuan dokumen atau informasi elektronik tersebut dianggap seolah-olah seperti data yang otentik atau asli.⁶

Salah satu kasus *phising* yang telah diadili dan memiliki kekuatan hukum yang tetap yang diputus pada hari Selasa, 6 Desember 2022 oleh Pengadilan Negeri Banjar

⁴ Purnamasari, Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-hari, Jurnal Digital Teknologi Informasi, 2023, Vol. 6 No.1, Halaman 29.

⁵ Dikdik M. Arief Mansyur & Elisatris Gultom, CYBER LAW Aspek Hukum Teknologi Informasi, PT Reflika Aditama, Bandung 2009, Hlm 89

⁶ Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik" PAMPAS: Journal Of Criminal Volume 1 Nomor 2, 2020

adalah Putusan dengan No.60/Pid.Sus/2022/PN.Bjr yang mana dalam amar putusannya Hakim hanya menjatuhkan 2 (dua) tahun dan 6 (enam) bulan penjara. Vonis tersebut dapat dikatakan sebagai hukuman yang relatif ringan karena jika diperhatikan lagi secara mendetil kasusnya, tindak pidana yang dilakukan Terdakwa tak hanya delik manipulasi data (*phising*), akan tetapi berdasarkan keterangan Terdakwa di muka persidangan, Terdakwa juga mengaku dan terbukti melakukan beberapa tindak pidana lainnya seperti tindak pidana penipuan yang mana antara delik manipulasi data memiliki unsur delik yang berbeda dengan delik lainnya yang dilakukan Terdakwa. Sehingga, sebenarnya Hakim dapat memberikan pemberatan pidana kepada Terdakwa. Walaupun secara yuridis vonis Hakim sudah sama dengan tuntutan Jaksa, akan tetapi alangkah baiknya jika majelis Hakim juga mempertimbangkan putusannya secara non-yuridis dengan memperhatikan rasa keadilan. Karena majelis Hakim dalam menjatuhkan putusannya bersifat independen artinya Hakim memiliki kekuasaan yang merdeka dan terbebas dari intervensi.

Oleh karena itu, *Phishing* dianggap sebagai ancaman dunia maya yang paling sulit diidentifikasi. Ini diikuti dengan teknik pengumpulan informasi lainnya, seperti mengarahkan ke informasi palsu situs *web*, meminta informasi pribadi melalui formulir *online*, dan bahkan mengirimkan *malware* melalui *e-mail*.

Seperti yang ada pada putusan sebagaimana tindak pidana kejahatan *Phising* yang diatur pada Pasal 51 Ayat 1 Juncto Pasal 35 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Pasal 378 kitab Undang-Undang Hukum Pidana (KUHP) serta pasal-pasal dalam Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP) serta peraturan lain yang berhubungan dengan perkara ini.

Pengaruh kemajuan teknologi informasi (*internet*) dan segala bentuk manfaat di dalamnya membawa dampak negatif tersendiri. Dimana semakin mudahnya para penjahat melakukan aksi tindak pidana kejahatan *phising* ini yang semakin merisaukan orang-orang yang terkena kejahatan tersebut. Oleh sebab itu, teknologi informasi (*internet*) mampu mengubah berbagai pola-pola yang sudah berkembang dalam suatu tindak pidana dengan kata lain modus operandi yang umumnya dilakukan pada kejahatan konvensional melalui teknologi internet dapat diubah menjadi modus operandi yang sifatnya baru, sehingga hal ini mengakibatkan perlu adanya upaya-upaya penanganan yang baru sesuai dengan Peraturan Undang-Undang Hukum dan putusan hakim pada tindak pidana *phishing* sesuai dengan ketentuan hukum yang berlaku. Berdasarkan pada penulisan yang diuraikan penulis, maka cukuplah untuk penulis menyusun penelitian dengan judul “Analisis Yuridis Terhadap Tindak Pidana *Phising* (Putusan No.60/PID.SUS/2022/PN.BJR)”

1. Rumusan Masalah

- a. Bagaimana Pengaturan Hukum Tindak Pidana *Phising* di Indonesia?
- b. Bagaimana Pertimbangan Hukum Oleh Hakim dalam Putusan No.60/Pid.Sus/2022/Pn.Bjr Atas tindak Pidana *Phising*?

- c. Bagaimana Pertanggungjawaban Pelaku Tindak Pidana *Phising* dalam Putusan No.60/Pid.Sus/2022/Pn.bjr?

2. Tujuan Penelitian

Untuk menganalisa suatu permasalahan kejahatan *Phising*, harus adanya penelitian untuk menghendaki apa yang telah dicapai dalam permasalahan-permasalahan di atas, tujuan penelitian ini adalah:

- a. Untuk mengetahui bagaimana proses pengaturan suatu Tindak Pidana *Phising* di Indonesia.
- b. Untuk mengetahui bagaimana pertimbangan Hukum oleh Hakim dalam Tindak Pidana *Phising* tersebut.
- c. Untuk mengetahui pertanggungjawaban pidana terhadap pelaku Tindak Pidana *Phising* tersebut

3. Manfaat Penelitian

Manfaat Penelitian ini yaitu;

- a. Manfaat Teoritis

Dengan adanya penelitian ini yang berjudul “Analisis Yuridis terhadap Tindak Pidana *Phising* Putusan No.60/Pid.Sus/2022/Pn.bjr” diharapkan memberi manfaat untuk mempelajari ilmu hukum, terkhusus hukum pidana, menambah perbendaharaan karya ilmiah yang membahas kejahatan internet, memberikan informasi, serta memberi gagasan dalam upaya pencegahan dan penanggulan kejahatan tersebut sehingga kejahatan internet tidak terulang kembali.

b. Manfaat praktis

Untuk dapat mencegah dan menanggulangi kasus-kasus kejahatan internet yang semakin merebak di kalangan mahasiswa dan bermanfaat menjadi evaluasi bagi penegak hukum dalam memberantas kejahatan ini, juga mengetahui peraturan perundang-undangan yang menjadi batas-batas dalam penggunaan internet untuk dapat dipatuhi dan diperhatikan sehingga mahasiswa ataupun penegak hukum tahu pentingnya kejahatan ini yang ternyata sangat tidak bisa diremehkan

B. Definisi Operasional

Definisi operasional adalah kerangka yang menggambarkan hubungan antara definisi atau konsep khusus yang akan diteliti. Konsep merupakan salah satu unsur konkrit dan teori. Sesuai dengan judul penelitian yang akan diajukan yaitu: “**Analisis Yuridis Terhadap Tindak Pidana *Phising* Putusan No. 60/PID.SUS/2022/PN.BJR**” maka dapat dijabarkan definisi operasional penelitian, yaitu:

1. Menurut kamus Hukum Online Analisis yuridis adalah serangkaian perilaku mengamati, mendeskripsikan, dan/atau menyusun kembali suatu objek dengan menggunakan parameter hukum sebagai standar guna menarik suatu kesimpulan terhadap objek tersebut terhadap hukum.⁷ Dapat disimpulkan bahwa Analisis Yuridis adalah penyelidikan suatu peristiwa (perbuatan) untuk mengetahui keadaan yang sebenarnya dan memperoleh pengertian yang tepat menurut hukum atau

⁷ Kamus Hukum Online Indonesia, “Pengertian Analisis Yuridis”

berdasarkan secara hukum.

2. Tindak pidana adalah perbuatan yang dilarang oleh suatu ketentuan hukum. Larangan yang mana disertai ancaman atau sanksi yang berbentuk pidana tertentu, bagi siapa yang melanggar larangan tersebut.⁸
3. *Phising* merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang dibutuhkan oleh pelaku kejahatan tindak pidana *phising*.⁹
4. Tindak Pidana *Phising* adalah perbuatan yang dilakukan oleh seseorang untuk memancing orang lain untuk memasukkan informasi pribadi rahasia pengguna milik orang lain itu ke dalam website yang telah dideface atau diubah mirip dengan yang asli resminya dengan cara menggunakan e-mail yang mengarahkan ke situs *website* palsu guna mendapatkan informasi pribadi rahasia pengguna orang lain. Karena hal itu, perbuatan-perbuatan kejahatan yang terjadi di dunia maya melalui transaksi elektronik sangat merugikan orang lain yang terkena kejahatan tindak pidana *Phising* ini.¹⁰

C. Keaslian Penelitian

Kejahatan dalam Tindak Pidana *Phising*, bukan suatu hal yang baru dibahas. Oleh

⁸ Asas-asas Hukum Pidana, “Moeljatno, 2008, Asas-Asas Hukum Pidana , PT. Rineka Cipta, Jakarta,,” Tindak Pidana (2008): 2004–2006.

⁹ Mila haryati wibowo, Nur Fatimah, “Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime” Vol.1, Nomor 1, Tahun 2017, hal 5.

¹⁰ Sahuri Lasmadi, “Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya,” Jurnal Ilmu Hukum, 2014, hlm. 3

karenanya, peneliti meyakini telah banyak peneliti-peneliti sebelumnya yang mengangkat tentang Analisis Yuridis terhadap Tindak Pidana *Phising*. Sebagai tajuk dalam berbagai penelitian, berdasarkan bahan kepustakaan dari lingkungan Universitas muhammadiyah Sumatera Utara dan perguruan tinggi lainnya. Peneliti tidak menemukan penelitian yang sama dengan tema dan pokok bahasan yang Penulis teliti terkait: **“Analisis Yuridis Terhadap Tindak Pidana *Phising* Putusan No.60/PID.SUS/2022/PN.BJR”**, adapun beberapa penelitian terdahulu yang bersesuaian dengan penelitian sekarang adalah sebagai berikut:

1. Skripsi NAZARY AGAM MULIA, NIM E0016309, Mahasiswa Fakultas Hukum Universitas Sebelas Maret, Surakarta Tahun 2021, yang berjudul “Analisis Tindak Pidana *Phising* melalui *Internet Banking*” di dalam penelitian ini membahas “Bagaimana pelaku melakukan tindak pidana pencurian data pribadi atau informasi bank milik orang lain menggunakan teknik *phising* sebagai penyertaan pelaku melakukan tindak pidana pencucian data atau informasi bank milik orang lain dengan memfokuskan bagaimana *phising* dijadikan sebagai alat untuk melakukan tindak pidana kejahatan tersebut”. Sehingga dalam penelitian ini, harus lebih ditingkatkan dengan bagaimana cara atau langkah-langkah pelaku dapat melakukan kejahatan tersebut menggunakan teknik *phising* yang dilakukan dalam studi kasus Putusan No.105/Pid.Sus/Pn.Pbr.
2. Skripsi KHANIFA JANNATUL DINIYAH, NIM 21801021087, Mahasiswa Fakultas Hukum Universitas Islam Malang, Malang Tahun 2022, yang berjudul “Perlindungan Hukum Bagi Korban Tindak Pidana *CyberCrime Phising*” didalam

penelitian ini membahas bagaimana kejahatan *phising* ini sangat berbahaya bagi pengguna via *online* untuk tujuan yang dapat merugikan korban. Dimana fokus penelitiannya membahas bagaimana perlindungan hukum bagi korban tindak pidana *cybercrime phising*, dimana hasil penelitiannya masih memerlukan peningkatan bagi para penyidik untuk menyusut kejahatan *cybercrime phising* ini yang sesuai dengan pengaturan yang berlaku di Indonesia yang akan menjatuhkan pelaku dengan sanksi hukuman yang sesuai dengan kejahatan yang dilakukannya.

3. Skripsi FAWZI ASWIN HADIST, NIM 198903132018011001, Mahasiswa Fakultas Hukum, Universitas Islam negeri Kalijaga, Yogyakarta Tahun 2022. Yang berjudul “Sanksi pelaku pidana *Phising*” yang dimana penelitian ini membahas tentang bagaimana sanksi yang didapatkan oleh pelaku tindak pidana *phising* dengan memfokuskan sesuai dengan komparasi Undang-Undang Informasi, Transaksi dan Elektronik dengan menggunakan teori Qiyas sehingga di penelitian ini menggunakan perbandingan bagaimana ketentuan sanksi pelaku tindak pidana *phising* dilakukan menurut Undang-Undang Informasi, Transaksi dan Elektronik dan teori Qiyas.
4. Skripsi BAGUS SETYO NUGROHO, NIM 130710101201, Mahasiswa Fakultas Hukum, Universitas Jember, Jember tahun 2018. Yang berjudul “Tanggung jawab Hukum Pihak Bank terhadap nasabah menjadi korban *phising*” yang dimana penelitian ini membahas tentang bagaimana tindak pidana *phising* menjadi alat atau sebuah teknik untuk pelaku melakukan tindak pidana kejahatan tersebut melalui seorang nasabah (korban). Dengan memfokuskan bagaimana pihak bank

bertanggung jawab untuk menangani yang dialami oleh korban atau nasabah yang terkena Tindak Pidana *Phising* dalam permasalahan yang telah terjadi.

5. Skripsi MONICA SHELSA H, NIM 1802026016, Mahasiswa Fakultas Hukum dan Syariah, Universitas Islam Negeri Walisongo, Semarang tahun 2022. Yang berjudul “Analisis Tindak Pidana Pencurian Data Pribadi Melalui Teknik *Phising* ditinjau dalam perspektif fiqih jinayah”. Dimana penelitian ini, membahas bagaimana *Phising* dijadikan sebagai teknik penyertaan untuk pelaku mengambil data pribadi milik orang lain, dengan memfokuskan bagaimana ketentuan hukum terhadap tindak pidana *phising* ini dan bagaimana pandangan perspektif fiqih jinayah terhadap teknik *phising* untuk pelaku melakukan tindak pidana pencurian dengan permasalahan yang dibahas dalam penelitian ini.

D. Metode Penelitian

1. Jenis Penelitian

Berdasarkan permasalahan penelitian yang telah peneliti ambil tentang analisis yuridis terhadap tindak pidana *phising*, maka metode penelitian yang digunakan adalah jenis metode penelitian yuridis atau normatif. Metode penelitian ini merupakan metode penelitian Hukum Normatif atau metode penelitian Hukum Kepustakaan.¹¹ Metode penelitian ini menggunakan penelitian terhadap bahan pustaka yang ada untuk dapat memecahkan masalah penelitian. Tahapan pertama penelitian Hukum Normatif adalah untuk mendapatkan Hukum Obyektif (Norma Hukum), dengan cara melakukan

¹¹ Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat, Cetakan ke-11. (PT Raja Grafindo Persada, Jakarta; 2009), hlm. 13–14.

penelitian terhadap masalah hukum. Tahapan kedua penelitian Hukum Normatif adalah penelitian yang ditujukan untuk mendapatkan Hukum Subjektif (hak dan kewajiban).¹²

Penelitian Hukum Normatif dikaji dari beberapa aspek seperti aspek teori, filosofis, perbandingan, struktur/komposisi, konsistensi, penjelasan umum, penjelasan pada pasal-pasal yang terkait, formalitas, dan bahasa yang dipergunakan yaitu bahasa hukum, sehingga dapat disimpulkan bahwa penelitian hukum normatif mempunyai cakupan yang luas. Oleh karena itu, jenis penelitian yang telah digunakan oleh peneliti untuk mengetahui bagaimana jenis penelitian dapat disesuaikan dengan permasalahan penelitian.

2. Sifat Penelitian

Sifat penelitian yang digunakan dalam menyelesaikan penelitian ini adalah deskriptif dengan pendekatan-pendekatan yang menggunakan pendekatan yuridis normatif untuk menggambarkan secara sistematis data dan mengenai permasalahan yang akan dibahas. Data yang terkumpul kemudian akan di analisis sehingga dapat ditarik untuk keseluruhan hasil penelitian.

Berkaitan dengan penelitian tentang tindak pidana *phising* yang mana tidak seluruh masyarakat memahami bagaimana tindak pidana *phising* ini terjadi tanpa disadari. Maka penulis memfokuskan dengan sifat penelitian yuridis normatif guna mendapatkan data-data yang akurat.

¹² Hardijan Rusli, "Metode Penelitian Hukum Normatif: Bagaimana?", Law Review Fakultas Hukum, Universitas Pelita Harapan, Volume V No. 3 Tahun 2006, hlm. 50.

3. Pendekatan Penelitian

Penelitian ini dilakukan dengan menggunakan pendekatan penelitian yuridis normatif. Pendekatan ini bertujuan menganalisis permasalahan dengan berdasarkan pendekatan undang-undang, pendekatan kasus, pendekatan historis, pendekatan asas-asas hukum dan pendekatan konseptual. kelima pendekatan tersebut akan digunakan secara bersama-sama. Dalam pendekatan ini peneliti akan mendapatkan informasi dari berbagai aspek mengenai isu hukum yang diteliti dan mencari jawabannya yaitu sebagai berikut:

a. Pendekatan undang-undang (*Statute Approach*)

Pendekatan ini dimaksud bahwa penelitian menggunakan peraturan perundang-undangan sebagai dasar awal melakukan analisis. Peraturan perundang-undangan merupakan fokus dari penelitian.

b. Pendekatan kasus (*Case Approach*)

Pendekatan kasus dalam penelitian hukum normative dimaksudkan untuk mempelajari penerapan norma-norma yang dilakukan dalam praktek hukum. Kasus-kasus yang diputus sebagaimana dalam yurisprudensi terhadap perkara yang terjadi merupakan fokus penelitian.

c. Pendekatan konseptual (*Conseptual Approach*)

Konsep berasal dari *concupere* atau *conceptus*, yang di dalam bahasa inggris disebut *consept*. Maknanya adalah memahami, menerima atau menangkap. Secara definisi, konsep memiliki banyak pengertian. Makna yang relavan adalah unsur- unsur abstrak yang universal yang di abstraksikan dari suatu yang partikular, untuk

menganalisis pendapat-pendapat (paham) dan pendekatan yuridis-normatif.¹³

Dapat disimpulkan bahwa pendekatan penelitian ini peneliti memfokuskan bagaimana peraturan perundang-undangan ditelaah secara vertikal dan horizontal, dengan maksud secara vertikal berarti ditelaah bagaimana hirarkinya peraturan perundang-undangan dengan secara horizontal yang dengan maksud menghubungkan peraturan perundang-undangan dengan berbagai pendekatan lainnya seperti asas-asas hukum, delik-delik hukum yang telah digunakan oleh lembaga peradilan untuk menghasilkan suatu putusan yang konkret dan sesuai.

4. Sumber Data Penelitian

Sumber data yang digunakan dalam penelitian ini:

- a. Data yang bersumber dalam; yaitu Al-Quran (QS. Al Maidah: 2) dan hadist hukum islam (HR. Ibnu Hibban 2:326).
- b. Data Sekunder terdiri dari:
 1. Bahan Hukum Primer, yaitu bahan hukum yang terdiri dari peraturan perundang-undangan, putusan pengadilan dan bahan hukum yang bersifat mengikat.¹⁴ Yang terdiri dari: a) Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang sebagaimana dalam Pasal 51 Ayat (1) Jo. Pasal 35 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan pasal 378 Undang-Undang Hukum Pidana, b) pasal-pasal dalam Undang-Undang Nomor 8

¹³ Lorest Bagus, Kamus Filsafat (Jakarta: Gramedia Pustaka Utama, 1996), hlm. 481-483

¹⁴ Soekanto dan Sri Mamudji, Op.Cit, h. 13 dan Bandingkan dengan Amiruddin dan Zainal Asikin, Op.Cit, hlm.31

Tahun 1981 tentang Hukum Acara Pidana, KUHP, serta peraturan perundang-undangan lain yang berhubungan dengan perkara ini

2. Bahan Hukum Sekunder, merupakan bahan yang memberikan penjelasan mengenai bahan hukum primer, bahan- bahan yang memberikan penjelasan mengenai bahan hukum primer seperti tulisan, jurnal, pandangan ahli-ahi dan buku-buku yang dianggap berkaitan dengan pokok permasalahan yang akan diangkat dalam penelitian ini.
3. Bahan Hukum tersier, adalah bahan-bahan atau tulisan-tulisan yang dapat menambah penjelasan dan memberikan petunjuk terhadap bahan hukum primer dan bahan hukum sekunder seperti kamus hukum, kamus bahasa Indonesia, kamus bahasa inggris, dan Wikipedia baik menggunakan via online maupun via offline

5. Alat Pengumpul Data

Alat pengumpul data dalam penelitian ini adalah prosedur atau cara-cara untuk peneliti mengumpulkan data yang berkaitan dengan penelitian ini. alat pengumpulan data yang akan dapat dipergunakan dengan dua cara, yaitu: pengumpulan data dari studi kepustakaan (library research) secara langsung guna memperoleh data sekunder yang dibutuhkan dalam proses penelitian ini.¹⁵

6. Analisis Data

Analisis data merupakan suatu rangkaian kegiatan yang bergerak secara induktif, yaitu dari data/fakta yang menuju ketingkat memfokuskan, mengabstraksikan dan

¹⁵ Riduwan 2010, "Metode dan Teknik Menyusun Proposal Penelitian", Bandung, Alfabeta.

mengorganisasikan data secara rasional dan sistematis.¹⁶ Sehingga prosedur analisisnya dapat dispesifikkan dengan tahapan-tahapan sebagai berikut:

1. Mendapatkan bahan permasalahan yakni, memfokuskan pada suatu hal yang penting sesuai dengan penelitian yang telah diteliti oleh peneliti, agar peneliti dapat mempermudah melakukan pengumpulan data selanjutnya
2. Hasil Pengumpulan data akan dianalisis secara kualitatif dengan menggunakan pendekatan yuridis normative yakni dengan menggunakan delik-delik, asas-asas, dan pasal-pasal didalam suatu perundang-undangan yang relevan dan berkaitan dengan permasalahan penelitian yang diangkat.
3. Data yang sudah dianalisis disajikan secara deskriptif dibuat kesimpulan untuk menghasilkan data yang sistematis dalam rumusan masalah yang menjadi pembahasan dalam penelitian.

Dapat disimpulkan, bahwa keseluruhan data yang terdiri dari data primer dan data sekunder (bahan hukum primer, sekunder, dan tersier). Akan diolah dan dianalisis secara kualitatif. Penelitian kualitatif merupakan tahap penelitian yang melampaui berbagai tahapan berfikir kritis ilmiah dengan upaya melakukan teriosasi berdasarkan pengamatan peneliti dalam penelitian ini.

¹⁶ Hardani, S.Pd.,M.Si.,dkk, Metode Penelitian Kualitatif dan Kuantitatif, Penerbit: CV. Pustaka Ilmu, Yogyakarta 2020, hlm 36.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tentang Tindak Pidana

Istilah tindak pidana berasal dari istilah yang dikenal dalam hukum pidana Belanda yaitu *strafbaar feit* atau *delict*. Menurut buku C.S.T Kansil dan Christine S.T Kansil dikenal juga beberapa terjemahan yang lain seperti perbuatan pidana, pelanggaran pidana, perbuatan yang boleh di hukum atau perbuatan yang dapat dihukum.¹⁷

Tindak pidana merupakan pengertian dasar dalam hukum pidana (yuridis normatif). Kejahatan atau perbuatan jahat bisa diartikan secara yuridis atau kriminologis. Kejahatan atau perbuatan jahat dalam arti yuridis normatif adalah perbuatan seperti yang terwujud in abstracto dalam peraturan pidana.¹⁸

Sebelum kita membahas lebih jauh lagi mengenai tindak pidana, maka ada baiknya kita harus terlebih dahulu mengetahui pengertian tindak pidana menurut para ahli. Berikut adalah pengertian tindak pidana menurut beberapa para ahli:

- a. Menurut Wirjono Prodjodikoro dalam bukunya Asas-Asas Hukum Pidana Di Indonesia memberikan definisi “tindak pidana” atau dalam bahasa Belanda “*strafbaar feit*”, yang sebenarnya merupakan istilah resmi dalam *Strafwetboek* atau disebut Kitab Undang-Undang Hukum Pidana, yang sekarang berlaku di Indonesia. Ada istilah dalam bahasa asing, yaitu *delict*. Tindak pidana berarti suatu perbuatan

¹⁷ C.S.T Kansil dan Christine S.T Kansil, Pokok-Pokok Hukum Pidana, PT. Pradnya Paramitha, Jakarta, 2007. hlm. 67

¹⁸ Sudikno Mertokusumo, Mengenal Hukum, Liberty, Yogyakarta, 1999, Hlm 10

yang pelakunya dapat dikenai hukum pidana. Dan, pelaku ini dapat dikatakan merupakan dari “subjek” tindak pidana.¹⁹

- b. Sedangkan dalam buku pelajaran Hukum Pidana karya Adami Chazawi, menyatakan bahwa istilah tindak pidana adalah berasal dari istilah yang dikenal dalam hukum pidana Belanda yaitu “*strafbaar feit*” tetapi tidak ada penjelasan tentang apa yang dimaksud dengan *strafbaar feit* itu. Karena itu, para ahli hukum berusaha memberikan arti dan isi dari istilah itu. Sayangnya sampai kini belum ada keragaman pendapat.²⁰
- c. Menurut Pompe, pengertian tindak pidana adalah suatu pelanggaran norma (gangguan terhadap tata tertib hukum) yang dengan sengaja ataupun dengan tidak sengaja telah dilakukan oleh seorang pelaku, dimana penjatuhan hukuman terhadap pelaku tersebut adalah perlu demi terpeliharanya tertib hukum dan terjaminnya kepentingan hukum.²¹
- d. Menurut Van Hamel, pengertian tindak pidana ialah suatu serangan atau suatu ancaman terhadap hak- hak orang lain. Van Hammel merumuskan sebagai berikut “*strafbaar feit* adalah kelakuan orang (*menselijke gedraging*) yang dirumuskan dalam *wet*, yang bersifat melawan hukum, yang patut dipidana (*strafwaardig*) dan dilakukan dengan kesalahan.²²

¹⁹ Wirjono Prodjodikoro, Asas-Asas Hukum Pidana Di Indonesia, Refika Aditama, Bandung, 2008. hlm. 58

²⁰ Adami Chazawi, Pelajaran Hukum Pidana, PT. Raja Grafindo Persada, Jakarta, 2002, hlm. 67

²¹ Erdianto Efendi, Hukum Pidana Indonesia, PT. Refika Aditama, Bandung, 2011. hlm. 26.

²² Moeljatno, Asas – Asas Hukum Pidana, Rineka Cipta, Jakarta, 2009, Hlm 33

- e. van Hattum, mengemukakan bahwa sesuatu tindakan itu tidak dapat dipisahkan dari orang yang telah melakukan tindakan tersebut. Menurutnya, perkataan *strafbaar* itu berarti *voor straf in aanmerking komend* atau *straf verdienend* yang juga mempunyai arti sebagai pantas untuk dihukum, sehingga perkataan *strafbaar feit* seperti yang telah digunakan dalam Undang–Undang Hukum Pidana itu secara eliptis haruslah diartikan sebagai suatu “tindakan, yang karena telah melakukan tindakan semacam itu membuat seseorang menjadi dapat dihukum” atau suatu “*feit terzake van hetwelk een persoon strafbaar is.*”²³

Dari penjelasan beberapa ahli di atas dapat disimpulkan bahwa adanya penafsiran yang sama atau yang berbeda mengenai pengertian “perbuatan pidana” dan “tindak pidana”. juga telah dikembangkan pengertian perbuatan pidana, pengertian tindak pidana belum diungkap secara jelas pemisahannya dengan pertanggungjawaban pidana, maka dapat dianggap bahwa tindak pidana termasuk di dalamnya unsur pertanggungjawaban pidana, sehingga pengertian tindak pidana berbeda dengan pengertian tindak pidana. Apabila pengertian tindak pidana terpisah dari pertanggungjawaban pidana, maka dapat di artikan bahwa istilah tindak pidana dianggap sama dengan perbuatan pidana.

1. Unsur-Unsur Tindak Pidana

Ada beberapa unsur-unsur tindak pidana menurut teoritis, ialah:

- a. Menurut Simons, unsur-unsur tindak pidana sebagai berikut:

²³ *Ibid*, halaman 33

- a) Unsur Pidana, Perbuatan manusia (positif atau negatif, berbuat atau tidak berbuat atau membiarkan). Diancam dengan pidana (*strafbaar gesteld*).
 - b) Unsur Pidana, Melawan hukum (*onrechtmatig*). Dilakukan dengan kesalahan (*met schuld in verbandstaand*).
 - c) Unsur Pidana, Oleh orang yang mampu bertanggungjawab (*toerekening vatoaar person*).
- b. Menurut *Schravendijk*, unsur tindak pidana sebagai berikut:
- a) Kelakuan (orang yang)
 - b) Bertentangan dengan keinsyafan hukum
 - c) Diancam bukan hukuman
 - d) Dilakukan oleh orang (yang dapat)
 - e) Dipersalahkan/kesalahan.²⁴
- c. Menurut *moeljatno*, unsur-unsur tindak pidana sebagai berikut:
- a). Perbuatan itu harus merupakan perbuatan manusia
 - b). Perbuatan itu harus dilarang dan diancam pidana
 - c). Perbuatan itu bertentangan dengan undang-undang
 - d). Harus dilakukan oleh orang yang dapat dipertanggungjawabkan
 - e). Perbuatan itu harus disalahkan oleh si pembuat²⁵

Dari beberapa penjelasan para ahli di atas, dapat disimpulkan bahwa suatu perbuatan akan menjadi suatu tindak pidana apabila perbuatan itu melawan hukum,

²⁴ Adami Chazawi, Op.Cit, h. 81

²⁵ *Ibid*, hlm,102.

merugikan masyarakat, dilarang oleh aturan pidana.

2. Jenis-Jenis Tindak Pidana

Tindak pidana dapat dibedakan menjadi beberapa jenis yaitu:

- a. Menurut kitab Undang–Undang Hukum Pidana (KUHP) dibedakan antara lain Kejahatan yang dimuat dalam Buku II dan Pelanggaran yang dimuat dalam Buku III.

Kejahatan adalah perbuatan-perbuatan yang bertentangan dengan keadilan, terlepas apakah perbuatan itu diancam pidana dalam suatu undang-undang atau tidak. Pelanggaran adalah perbuatan-perbuatan yang oleh masyarakat baru disadari sebagai suatu tindak pidana, karena undang-undang merumuskannya sebagai delik.²⁶

- b. Tindak pidana formil dan tindak pidana materil.

Tindak pidana formil adalah tindak pidana yang dirumuskan bahwa larangan yang dirumuskan itu adalah melakukan perbuatan tertentu. Tindak pidana materil inti. larangannya adalah pada menimbulkan akibat yang dilarang, karena itu siapa yang menimbulkan akibat yang dilarang itulah yang dipertanggungjawabkan dan dipidana.²⁷

- c. Delik *Dolus* dan Delik *Culpa*.

Delik *Commissionis*, delik *ommissionis* dan delik *commissionis per omissionis*

²⁶ Ismu Gunadi dan Jonaedi Efendi, *Op.Cit*, h.44

²⁷ Adami Chazawi, *Op.Cit*, h. 126

commissa. Delik *Dolus* memerlukan adanya kesengajaan, misalnya Pasal 354 KUHP: “dengan sengaja melukai berat orang lain” sedangkan Delik *Culpa*, orang juga sudah dapat dipidana bila kesalahannya itu berbentuk kealpaan, misalnya menurut Pasal 359 KUHP dapat dipidananya orang yang menyebabkan matinya orang lain karena kealpaannya.

- d. Delik *commisionis* adalah delik yang terdiri dari melakukan sesuatu (berbuat sesuatu) perbuatan yang dilarang oleh aturan-aturan pidana, misalnya mencuri (Pasal 362), menggelapkan (Pasal 372), menipu (Pasal 378). Delik *ommisionis* adalah delik yang terdiri dari tidak melakukan sesuatu padahal mestinya berbuat, misalnya dalam Pasal 164: mengetahui suatu permufakatan jahat untuk melakukan kejahatan yang disebut dalam pasal itu, pada saat masih ada waktu untuk mencegah kejahatan, tidak segera melaporkan kepada instansi yang berwajib atau orang yang terkena. Delik *commissionis peromissionem commissa*, yaitu delik-delik yang umumnya terdiri dari berbuat sesuatu, tetapi dapat pula dilakukan dengan tidak berbuat, misalnya seorang ibu yang merampas nyawa anaknya dengan jalan tidak memberi makan pada anak itu.²⁸

- e. Delik tunggal dan delik berganda.

Delik tunggal adalah delik yang cukup dilakukan dengan sekali perbuatan sedangkan delik berganda adalah delik yang untuk kualifikasinya baru terjadi apabila dilakukan berulang kali perbuatan.²⁹

²⁸ Ismu Gunadi dan Jonaedi Efendi, Op.Cit, h. 46

²⁹Adami Chazawi, Op.Cit, h. 136

f. Delik menerus dan delik tidak menerus.

Dalam delik menerus adalah tindak pidana yang mempunyai ciri, bahwa keadaan/perbuatan yang terlarang itu berlangsung terus. Dengan demikian tindak pidananya berlangsung terus menerus sedangkan delik tidak menerus adalah tindak pidana yang mempunyai ciri, bahwa keadaan / perbuatan yang terlarang itu tidak berlangsung terus. Jenis tindak pidana ini akan selesai setelah dengan telah dilakukannya perbuatan yang dilarang atau telah timbulnya akibat (Pasal 333 KUHP).

g. Delik aduan.

Delik aduan adalah tindak pidana yang penuntutannya hanya dilakukan apabila ada pengaduan dari pihak yang terkena atau yang dirugikan/korban. Dengan demikian, apabila tidak ada pengaduan, terhadap tindak pidana tersebut tidak boleh dilakukan penuntutan. Delik aduan terbagi menjadi dua:

- 1). Delik aduan yang absolut misalnya Pasal 284 KUHP. Delik ini menurut sifatnya hanya dapat dituntut berdasarkan pengaduan.
- 2). Delik aduan yang relatif misalnya Pasal 367 KUHP, disebut relatif karena dalam delik-delik ini ada hubungan istimewa antara pembuat dan orang yang terkena.

h. Delik biasa dan delik yang dikualifikasikan.

Delik biasa adalah bentuk tindak pidana yang paling sederhana tanpa adanya unsur yang bersifat memberatkan sedangkan delik yang dikualifikasikan adalah tindak pidana dalam bentuk pokok yang ditambah dengan adanya unsur pemberatan, sehingga ancaman pidananya menjadi lebih berat.

B. Tinjauan Umum Tentang Phising

Sejarah *Phising* telah mengganggu dunia maya selama lebih dari 2 dekade, dimulai pada tahun 1995 dengan America Online (AOL) (James, 2006). Istilah *phishing* adalah variasi dari istilah memancing di mana tindakan *phishing* menyerupai penangkapan ikan dengan cara berikut: penyerang “memancing” korban menggunakan “umpan” dan “memancing” untuk informasi pribadi atau rahasia korban. Studi komprehensif tentang definisi *phising* dilakukan oleh Lastdrager (2014) dimana dia mengidentifikasi definisi *phising* yang disepakati: *Phising* adalah tindakan penipuan yang dapat diskalakan di mana peniruan identitas digunakan untuk mendapatkan informasi dari target. Penyerang menggunakan berbagai saluran untuk menipu korban secara langsung dengan *scam* atau mengirimkan muatan melalui cara tidak langsung dengan tujuan untuk mendapatkan informasi pribadi atau rahasia dari korban.³⁰

Sejarah *phishing* pertama kali dilakukan pada tahun 1990 oleh geng warez. Penyerang siapa membentuk komunitas warez merancang sebuah algoritma yang menghasilkan kartu kredit acak nomor untuk digunakan dalam serangan mereka. Untuk membuka *account* AOL dan mengirimkan *spam* ke banyak orang klien, nomor kartu kredit yang dihasilkan secara acak digunakan. *Usenet newsgroup* AOHell memberi *label* serangan itu *phising* pada tanggal 2 Januari 1996.³¹

Setelah *phishing* itu diciptakan dan menjadi istilah dengan menggunakan strategi

³⁰ Purnamasari, Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-Hari, Jurnal Digital Teknologi Informasi, 2023, Vol. 6 No.1, Halaman 29.

³¹ Gunikhan Sonowal “*Phishing and Communication Channels A Guide to identifying and Mitigating Phishing Attack*”, Apress, Tinsuka, Assam, India, 2022, hlm 4

ini, penyerang menargetkan pengguna sah dengan upaya *phishing*. AOL akhirnya menerapkan pendekatan verifikasi yang lebih canggih dengan memverifikasi informasi kartu kredit kepada konsumen sebenarnya. Lebih buruk lagi bagi pelanggan AOL, para penyerang mengeksploitasi AOL *Messenger* dan menyamar sebagai staf AOL untuk mengirim pesan pengguna, mendesak mereka untuk memperbarui akun mereka dan memberikan informasi penagihan. Beberapa penyerang menggunakan *phishing* untuk menargetkan pengguna AOL, yang mengakibatkan bencana situasi bagi organisasi.³²

Pelanggan yang menggunakan AOL *Messenger* diberitahu oleh AOL bahwa perusahaan tersebut tidak pernah meminta kata sandi atau informasi penagihan siapa pun akibat kejadian tersebut. Pada akhirnya, penegakan kebijakan AOL mendorong hak cipta pelanggaran pada *server*, dan AOL segera menonaktifkan akun *phishing* tersebut sebelum korban sempat bereaksi. Penutupan lokasi warez AOL memaksa mayoritas *phisher* untuk meninggalkan operasi. Beberapa insiden *phishing* kecil terjadi di tahun berikutnya, namun kejadian *phishing* yang menarik dimulai pada Tahun 2000.³³ Sistem Pembayaran Online menjadi sasaran serangan *phishing* di awal Tahun 2000an. Keuntungan finansial biasanya menjadi tujuan penyerang ketika mereka menargetkan pelanggan *online* penyedia pembayaran. *E-gold* adalah korban serangan langsung pertama yang diketahui terhadap pembayaran sistem pada bulan Juni 2001. penyerang menargetkan keuangan institusi menambahkan senjata lain ke gudang senjata mereka.

³² Gunikhan Sonowal “*Phishing and Communication Channels A Guide to identifying and Mitigating Phishing Attack*, Apress, Tinsuka, Assam, India, 2022, hlm 4

³³ Gunikhan Sonowal “*Phishing and Communication Channels A Guide to identifying and Mitigating Phishing Attack*, Apress, Tinsuka, Assam, India, 2022, hlm 5

Upaya *phising* di situs pembayaran masih menjadi hal yang lumrah saat ini.³⁴

Serangan *phishing* yang tiba-tiba terhadap lembaga keuangan pertama kali dilaporkan pada bulan Juli 2003. Menurut Great Spam Archive, target utamanya adalah E-loan, E-gold, Wells Fargo, dan Citibank. Hal yang paling menarik dari fenomena *phishing* adalah bahwa fenomena ini memperkenalkan kelas vektor serangan baru yang diabaikan di hampir setiap anggaran keamanan lembaga keuangan: elemen manusia. Semua firewall yang mahal, sertifikat SSL, aturan IPS, dan manajemen patch dapat tidak menghentikan eksploitasi kepercayaan online yang tidak hanya membahayakan informasi rahasia pengguna namun juga berdampak besar pada kepercayaan konsumen mengenai telekomunikasi antara perusahaan dan kliennya.³⁵

Dari awal, para pelaku dan mereka yang memperdagangkan *software* bajakan menggunakan layanan ini untuk berkomunikasi satu sama lain. Cara pertama yang dilakukan tersangka (*phiser*) adalah dengan menggunakan algoritma untuk membuat nomor kartu kredit secara acak.³⁶ Jumlah kredit acak kartu yang digunakan untuk membuat rekening America Online. Akun tersebut digunakan untuk mengirim pesan secara bertubi-tubi (*spam*) ke pengguna lain bertujuan untuk berbagai hal lainnya. Program-program khusus seperti AOHell digunakan untuk menyederhanakan proses. Praktek ini diakhiri oleh America Online pada tahun 1995, ketika perusahaan membuat

³⁴ Gunikhan Sonowal “*Phishing and Communication Channels A Guide to identifying and Mitigating Phishing Attack*, Apress, Tinsuka, Assam, India, 2022, hlm 5

³⁵ Lance James, “*Phishing Exposed*” Syngress Publishing, Inc, United States of America, 2006, hlm 11.

³⁶ Adami Chazawi, Tindak Pidana Informasi dan Transaksi Elektronik, Media Nusa Creative, Malang, 2015, hlm. 117-120

langkah-langkah keamanan untuk mencegah keberhasilan pengguna angka kredit secara acak kartu.

Serangan *phising* telah berkembang selama bertahun-tahun secara global dengan peningkatan sebesar 65% menjadi 1.220.523 pada tahun 2016 dibandingkan dengan tahun sebelumnya. APWG melaporkan peningkatan 5.753% dari serangan *phising* rata-rata per bulan selama periode 12 tahun, dari 2004 hingga 2016. Pada 2015, lebih dari setengah miliar catatan pribadi dicuri, meningkat dibandingkan tahun sebelumnya. Lab *Kaspersky* melaporkan bahwa phishing disektor keuangan mencapai rekor tertinggi sepanjang masa pada tahun 2016. Antara periode Oktober 2013 hingga Februari 2016, FBI menerima laporan penipuan email bisnis dengan total kerugian sebesar \$2,3 miliar. Kerugian ini hanya melalui penipuan email bisnis saja dan tidak termasuk kerugian melalui penipuan phishing lainnya. Karena masalah *phising* ini serius, menarik untuk mengetahui secara detail vektor serangan *phising* saat ini dan Informasi ini akan sangat berharga dalam pengembangan teknik anti *phising* serta untuk menciptakan kesadaran publik.³⁷

Phising yaitu aktivitas seseorang untuk mendapatkan informasi rahasia pengguna dengan cara menggunakan email dan situs web palsu yang tampilannya menyerupai tampilan asli atau resmi web sebenarnya. Informasi yang didapat atau dicari oleh phiser adalah berupa password akun atau nomor kartu kredit korban. Penjebak (phisher) menggunakan email, banner atau pop-up window untuk menjebak user agar

³⁷ Purnamasari, Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-Hari, Jurnal Digital Teknologi Informasi, 2023, Vol. 6 No.1, Halaman 29.

mengarahkan ke situs web palsu (fake webpage), di mana pengguna diminta untuk memberikan informasi pribadinya. isinilah phiser memanfaatkan kecerobohan dan ke tidak telitian pengguna dalam web palsu tersebut untuk mendapatkan informasi.³⁸

Phising adalah perbuatan yang dilakukan oleh seseorang untuk memancing orang lain untuk memasukkan informasi pribadi rahasia pengguna milik orang itu ke dalam sebuah *website* yang telah *dideface* atau diubah mirip dengan yang asli resminya dengan cara menggunakan *e-mail* yang mengarahkan ke situs web palsu guna mendapatkan informasi pribadi rahasia pengguna orang lain, sehingga muncul sebuah pertanyaan, apakah dalam menangani *cybercrime* dalam bentuk *Phising* di Indonesia tidak hanya dikenakan Pasal 35 jo Pasal 51 ayat (1) dan Pasal 28 ayat (1) jo Pasal 45A ayat (1) saja atau dapat berkaitan dengan pasal-pasal yang lain di dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan juga mungkin dapat dikenakan dengan pasal-pasal diluar Undang-Undang Informasi dan Transaksi Elektronik seperti KUHP.

Phising adalah penipuan online yang dilakukan melalui *email*, *link*, *website*, atau telepon palsu yang dibuat semirip mungkin dengan aslinya. Tujuannya yaitu untuk mendapatkan data dan informasi sensitif, seperti rekening bank atau *username* dan *password*. Pada dasarnya, *phising* berasal dari kata *phising* dalam bahasa Inggris, mengadaptasi kata *fishing* yang secara harfiah berarti memancing. Jadi, *phising*

³⁸ MOHD. Yusuf DM, Addermi, dan Jasmine Lim, "Kejahatan Phising dalam dunia Cyber Crime dan Sistem Hukum di Indonesia", Jurnal Pendidikan dan Konseling, Vol 4, No. 5, Tahun 2022

merupakan teknik untuk ‘memancing’ informasi dan data rahasia dari para korban melalui umpan atau data palsu yang dibuat semenarik mungkin dan semirip mungkin dengan aslinya.³⁹

Phising adalah bentuk untuk memperoleh informasi. Contohnya: kata sandi, nomor kartu kredit, dan lain-lain untuk mengelabui calon korban mengunduh file palsu yang terinfeksi atau terdapat virus dengan berkamuflase menjadi orang atau badan usaha terpercaya dalam intelijen komunikasi elektronik formal berupa *e-mail* atau pesan singkat.⁴⁰ Oleh karena itu, perilaku ini bisa saja terjadi di setiap saat. kelompok kerja (APWG) mengatakan dalam laporan bulanannya bahwa 12.845 email baru dan unik serta 2.560 situs palsu yang dipergunakan sebagai alat phishing. Seiring dengan peningkatan tersebut, tingkat serangan juga meningkat. Artinya, situs palsu dihosting di suatu sistem komputer yang tidak memiliki keamanan standar untuk menghindari deteksi.⁴¹

Phising menampakkan diri sebagai pihak berwenang dengan menggunakan website atau *e-mail* palsu yang tampak meyakinkan dan kemudian setelah informasi diperoleh akan digunakan dengan tujuan kejahatan.⁴²

Cara yang ditempuh biasanya adalah dengan membuat sebuah halaman web palsu

³⁹ Faradilla A, apa itu phising, hostinger website digital, 2023

⁴⁰ F. E. Purwiantono, “Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia,” 2017

⁴¹ A. S. Gulo, S. Lasmadi, dan K. Nawawi, “*CyberCrime* dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik,” PAMPAS J. Crim. Law, vol. 1, no. 2, hlm. 68-81, Apr 2021.

⁴² Malahayati dan Darul Fata, “Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit melalui Teknik Phising”, Djtechno: *Journal of Information Technology Research*, Vol 2, No. 1, Juli, Tahun 2021, hlm 24.

yang mirip dengan halaman web yang asli (*Web Clonning*). Pada saat seseorang *login* melalui halaman web palsu tersebut, maka data yang dimasukkan seperti *username* dan *password* akan direkam atau dikirim ke pembuat halaman *web* palsu. Oleh karena itu, teknik phishing ini juga dikenal dengan sebutan teknik *fake login*, dimana seseorang login di halaman yang bukan sebenarnya.⁴³

Phising sendiri terbagi menjadi beberapa jenis dan teknik yang sering digunakan oleh penjahat *cyber*. Adapun diantaranya:

- a. *Spear Phising*, mengirim email secara langsung kepada target dan mengakusebagai pihak resmi yang terpercaya.
- b. *Deceptive Phising*, mengaku sebagai pihak resmi yang meminta verifikasi akun, mengubah kata sandi, melakukan pembayaran, dan hal sejenis lainnya yang bersangkutan dengan pelayanan sebagai pihak yang resmi.⁴⁴
- c. *Web Phising*, upaya memanfaatkan website palsu atau kloning untuk mengelabui target. Web hasil kloning tersebut akan terlihat mirip dengan web resmi dengan menggunakan domain yang mirip.⁴⁵

Sumber-sumber ancaman *phising*

1. Email

⁴³ Efy Zam, *Phising Cara Mudah Menyadap Password & Pencegahannya*, PT. Trans Media, Jakarta Selatan, 2014, hlm. 2.

⁴⁴ Anggun Juniamaalia Sholikhah dan Aryo Fadlian, “Perspektif Undang-Undang tentang Informasi dan Transaksi Elektronik Terhadap Cyber Crime dalam bentuk Phising”, Vol 3, No.1, Tahun 2023, hlm 31-32.

⁴⁵ Malahayati dan Darul Fata, “Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit melalui Teknik Phising”, *Djtechno: Journal of Information Technology Research*, Vol 2, No. 1, Juli, Tahun 2021, hlm 24.

Berdasarkan *survey* yang telah dilakukan pada tahun 2014 ada lebih dari 120.000 serangan *phising* yang berpuncak pada miliaran transmisi *email*. 65% dari serangan *phising* mulai dengan mengunjungi link yang diterima dalam sebuah email. Pada Maret 2016, 229.265 laporan emailphishing diterima oleh Kelompok Kerja Anti-*Phishing* dari konsumen. 18,3% penduduk Australia menjadi korban dari *phising* melalui *e-mail*⁴⁶

2. Website

Phising pada website meliputi iklan dan sosial media (Facebook, Twitter, Instagram). Berdasarkan *survey* yang telah dilakukan Facebook memperkirakan 8,7% dari akun yang berjumlah 83.090.000 bukan milik pengguna yang sebenarnya dan perkiraan sekitar 1,5% (14.320.000) adalah akun yang secara tidak sengaja menyebarkan isi berbahaya tanpa diketahui oleh pengguna, seperti pesan spam dan link yang mencurigakan. Sebagian besar serangan *phising* dilakukan melalui web server yang sudah dihack dan 73% situs telah menjadi Korban. Pada Maret 2016 123.555 situs *phising* terdeteksi oleh Kelompok Kerja Anti-*Phishing*. 15,7% penduduk Australia menjadi korban *phising* melalui situs belanja online dan 6,9% melalui sosial media.⁴⁷

3. Malware

Phising yang dilakukan melalui penyebaran malware salah satunya adalah

⁴⁶ Mia Haryati Wibowo, Nur Fatimah, Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia *Cybercrime*, JOEICT (Jurnal of Education and Information Communication Technology) Volume 1, Nomor 1, Tahun 2017: 1 - 5

⁴⁷ *Ibid*, halaman 1-5

malware Koobface yang telah membuat 81% pengguna menjadi korbannya.⁴⁸

Cara kerja *phising* berdasarkan sumber-sumber ancaman *phising* yang diatas yaitu:

1. Email

Serangan ini di mulai dengan mengirimkan email yang terlihat dari sebuah organisasi yang kenal dengan korban. Kemudian email tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti link URL yang terdapat dalam email tersebut. Pada dasarnya, *phising* menggabungkan rekayasa sosial dan faktor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima *e-mail*. Penyerang akan mengirimkan jutaan email ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut. Pastinya serangan-serangan tersebut menggunakan email palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi.⁴⁹

2. Website

Pada situs web mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti *password* dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas. *Phiser* juga menggunakan *tool* untuk mencuri kode sumber laman web yang sah dan menggantinya dengan web palsu. Selain itu, *phiser* menciptakan *embedding link* untuk mendapatkan informasi sensitif milik korban.⁵⁰

⁴⁸ *Ibid*, halaman 1-5

⁴⁹ *Ibid*, halaman 1-5

⁵⁰ *Ibid*, halaman 1-5

3. Malware

Cara penyerangan dengan berpura-pura meminta karyawan untuk mendownload suatu file yang di kirim oleh phiser sebagai penetralisir malware di komputer nantinya⁵¹

Istilah *phising* dalam bahasa inggris berasal dari kata “fishing” (memancing), dalam hal ini “fisihing” berarti memancing informasi dan kata sandi pengguna internet. Aktivitas *phising* tersebut biasanya dilakukan secara sengaja oleh orang dalam, hacker atau penjahat internet yang berhasil menyusupi sebuah website melalui celah keamanan yang ada pada website tersebut, lalu meletakkan halaman phising maupun membuat halaman phising yang baru yang serupa.⁵² Salah satu alasan mengapa menemukan begitu banyak organisasi kurang kompeten dalam hal dasar-dasar keamanan *cyber* adalah banyaknya pemberitaan mengenai pelanggaran data besar dalam satu dekade terakhir yang menyatakan bahwa serangan tersebut adalah "serangan paling canggih yang pernah ada hingga saat ini" atau tindakan "sebuah negara bangsa" merupakan hal yang umum.⁵³

Kuantitas Kejahatan *Phising* dengan Jumlah dan makin hebatnya kecanggihan phising dari waktu ke waktu makin meningkat. Dalam beberapa tahun terakhir ini, puluhan juta orang Amerika telah menjadi korban *e-mail* palsu, *web pages* palsu, dan

⁵¹ *Ibid*, halaman 1-5

⁵² Febry Eka Purwiantono, “Model Klasifikasi Untuk Deteksi Situs Phising Indonesia”, Surabaya, 2017, hlm 11

⁵³ Tim Rains, “*Cybersecurity Threats, Malware Trends, and Strategies (Mitigate exploits, malware, phising, and other socil engineering attacks)*”, Packt Publishing Ltd, Livery Place 35, Birmigham, UK, 2020

pop-up palsu yang bertujuan untuk memperoleh data keuangan pribadi. Hal itu telah menjadikan kejahatan *phising* sebagai salah satu *cybercrime* yang tumbuh dengan cepat.⁵⁴ Saat ini, ada peningkatan kebutuhan untuk mendeteksi situs web phishing karena dampak buruknya terhadap korbannya. Banyak pekerjaan telah dilakukan dalam mendeteksi phishing situs web menggunakan beberapa teknik untuk mencapai tujuan yang sama.⁵⁵ Konsekuensi dari fenomena ini adalah perbaikan terus-menerus pada sistem anti-*phising* dan deteksi, semakin pentingnya keamanan dan perlunya meningkatkan edukasi mengenai bahaya *phising* untuk menjaga keamanan digital.⁵⁶

⁵⁴ Sutan Remy Syahdeini, *Kejahatan & Tindak Pidana Komputer*, PT. Pustaka Utama Grafiti, Jakarta, 2009, hlm. 65-66

⁵⁵ Oluwatobi Ayodeji Akanbi, dkk, “*A Machine Learning Approach to Phishing Detection and Defense*”, Syngress Is an imprint of Elsevier 255, Wymna Street, Waltham, USA, 2015.

⁵⁶ Irma Yurita, M.Kevin Ramadhan dan M. Candra, “Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cyber Crime”, *Jurnal Hukum, Legalita* Vol 5, No. 2, Desember 2023, hlm 146.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Pengaturan Hukum Tindak Pidana Phising di Indonesia

Pengaturan hukum Tindak Pidana *Phising* yang ada di Indonesia sebelum terbentuknya Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, kasus *cybercrime* di Indonesia diadili dengan menerapkan Pasal yang memiliki kesesuaian Unsur dalam KUHP Sehingga Pidanaan kepada para pelaku *Cybercrime* menggunakan KUHP ini. Dalam KUHP, Ketentuan Pidana pada Kasus *Cybercrime* berbentuk *Phising* dapat digunakan berdasarkan Pasal 378 KUHP. Pengaturan Hukum terhadap *Cybercrime* dalam bentuk *Phising* diatur di dalam Pasal 378 KUHP Tentang Penipuan Sebagaimana yang diketahui bahwa *Phising* secara umum merupakan Tindakan Penipuan.

Penggunaan Pasal 378 KUHP dalam Pidanaan Terhadap Kasus *Cybercrime* hanya dilakukan berdasarkan penafsiran dikarenakan terdapat perbedaan jenis Tindak Pidana *Cybercrime* dengan Tindak Pidana konvensional yang ada, Walaupun Metode *Phising* dan Penipuan dalam KUHP ada Kesamaan Unsur Perbuatannya akan tetapi tetap ada perbedaan mulai dari bentuk Tindak Pidana, dalam menentukan *Locus delicti* sampai tempos *Delicti*-nya. Tindak Pidana *Cybercrime* adalah suatu pengelompokan dari jenis Tindak Pidana yang merupakan golongan baru, dikarenakan *Cybercrime* mengikuti Perkembangan Teknologi yang sedang berkembang pesat. Hal tersebut memerlukan adanya suatu aturan khusus yang jelas dalam menangani Tindak Pidana

Cybercrime ini. Karena apabila hanya mengandalkan penafsiran saja akan membuat terbenturnya suatu tatanan hukum sehingga membuat praktik penegakan hukum kurang maksimal.⁵⁷

Dari unsur Pasal 378 KUHP dapat ditarik kesimpulan yang dimaksud dengan barang siapa adalah subjek atau si pelaku yang melakukan tindak pidana penipuan. Adanya niat atau menguntungkan diri sendiri maupun orang lain, yang dimana artinya adalah tujuan yang disadari (*oogmerk*), selanjutnya perbuatan tersebut dilakukan secara melawan hukum, yang berarti pelaku penipuan itu tidak mempunyai hak sama sekali untuk menikmati keuntungan hasil penipuan tersebut.⁵⁸

Phising Saat ini di Indonesia dapat dikenakan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik pada Pasal 35 jo Pasal 51 ayat (1) karena *phising* merupakan kejahatan siber yang membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu. *Cybercrime* dalam bentuk *phising* ini juga dapat dikenakan Pasal berlapis yaitu Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Pasal 28 ayat (1) jo Pasal 45A ayat (1) karena *phising* juga melakukan kebohongan untuk menyesatkan orang lain dimana mengarahkan orang yang dibohongi untuk mengakses sebuah link yang dimana link tersebut ditujukan ke situs palsu dan memberikan suatu perintah untuk

⁵⁷ Faiz Emery Muhammad, Beniharmoni Harefa, Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phising Berbasis Web, Jurnal USM Law Review Vol 6 No 1 Tahun 2023, hlm 231-232

⁵⁸ Andi Hamzah, Delik-Delik Tertentu (*Speciale Delicten*) di dalam KUHP Edisi Kedua, Sinar Grafika, Jakarta, 2015, hlm. 100

memperbarui informasi pribadinya yang rahasia ke dalam situs palsu yang telah dibuat oleh pelaku *Phising*, Sehingga informasi pribadinya yang rahasia tersebut diketahui oleh Pelaku *Phising* dan menyebabkan orang tersebut mengalami kerugian.⁵⁹

Adanya Pengaturan Tersebut tidak Sepenuhnya Mampu Memberikan Kepastian Hukum dalam Penegakan hukum Pada kasus Tindak Pidana *Phising*, Karena masih banyak Penerapan saat Penjatuhan Hukuman kepada Setiap Pelaku Tindak Pidana *Phising* yang begitu beragam. Sehingga hal ini seakan membuat sebuah kekaburan hukum didalamnya karena akan membuat Penegak Hukum Khususnya dari Pihak Kepolisian dan kejaksaan akan menjatuhkan hukuman yang tidak dapat dipastikan pengaturan secara khusus dan pastinya, dan jalan satu-satunya pada setiap penjatuhan Hukum Tindak Pidana *Phising* dapat dilihat dari Unsur-Unsur dari Tindak Pidananya serta unsur turut serta tindak pidana lain yang dilakukan oleh pelaku Tindak Pidana *Phising*.⁶⁰

Tindakan *Phising* Sebagaimana dijelaskan sebelumnya merupakan Tindakan penipuan dengan mekanisme digital. Pada dasarnya, tindakan penipuan dan ancamannya dituangkan dalam Kitab Undang-Undang Hukum Pidana, tepatnya pada Pasal 378 KUHP. Pasal tersebut menjelaskan bahwa pelaku tindakan *Phising* yang memakai Nama Palsu atau martabat palsu dengan tipu muslihat atau kebohongan

⁵⁹ Saputra Gulo, A., Lasmadi, S., & Nabawi, K. (2020), Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, PAMPAS: Journal Of Criminal, 1(2), 68–81.

⁶⁰ Septian Arya Budi Mahesa, Hervina Puspitosari, Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam Penanganan Perkara Tindak Pidana Phising, Jurnal Penelitian dan Pengabdian Masyarakat, Vol. 2 (11) Maret 2023, hlm 2686-2696

sehingga target menyerahkan sesuatu kepadanya, yang dilakukan secara melawan hukum.⁶¹

Sebuah peraturan mengenai Tindak Pidana *Phising* tentunya memerlukan sebuah Kepastian Hukum untuk menjamin penegakan hukum yang dilakukan oleh Negara Para Pelaku Tindak Pidana *Phising*. Pada Dasarnya Asas Kepastian Hukum (*hetrechtszekerheidsbeginsel*), Asas kepastian hukum merupakan konsekuensi sendiri negara berdasarkan atas hukum. Oleh karena itu setiap peraturan yang dibentuk harus jelas. Kepastian Hukum menunjuk kepada pemberlakuan hukum yang jelas, tetap dan konsisten dimana pelaksanaannya tidak dapat dipengaruhi oleh keadaan-keadaan yang sifatnya subjektif.⁶²

Indonesia mengenal Asas "*Lex Specialis Derogat Legi Generali*". Berdasarkan Asas *Lex specialis derogat legi generali*, berarti aturan-aturan hukum yang bersifat khusus dianggap berlaku meskipun bertentangan dengan aturan-aturan hukum yang umum. Dapat disimpulkan bahwa yang berlaku saat ini untuk mengatur tentang bagaimana pengaturan hukum *Cybercrime* dalam bentuk *Phising* tersebut saat ini diatur oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena Undang-Undang ini bersifat khusus. Pada saat ini perbuatan *Phising* tersebut diatur pada Pasal 35 jo Pasal 51 Ayat (1), yang dirumuskan sebagai berikut:

1. Pasal 35: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum

⁶¹ *Ibid.*, halaman 2686-2696

⁶² Julyano, M., & Sulistyawan. A. Y, Pemahaman terhadap asas kepastian hukum melalui konstruksi penalaran positivisme hukum, 2019, *Crepido*, 1(1), 13–22.

melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

2. Pasal 51: “Setiap Orang yang memenuhi unsur sebagaimana dimaksud di dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).” Unsur-unsur yang terdapat di dalam Pasal 35, yaitu:
- a. Setiap Orang;
 - b. Dengan sengaja dan tanpa hak atau melawan hukum;
 - c. Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik;
 - d. dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.⁶³

Perbuatan *phising* ini juga tidak hanya membuat sebuah situs yang seolah-olah mirip dengan situs asli yang resmi, namun juga perbuatan *phising* ini melakukan sebuah tindakan kebohongan untuk menipu atau menyesatkan orang lain sehingga menyebabkan orang tersebut mengalami kerugian karena informasi pribadi rahasia orang itu diketahui oleh pelaku *cybercrime* dalam bentuk *phising* tersebut.⁶⁴

Phising adalah salah satu jenis *Cybercrime* yang tujuannya untuk mencuri data pribadi orang lain dan disalahgunakan tanpa sepengetahuan orang tersebut. *Phising* merupakan salah satu jenis kejahatan digital yang cukup marak di Indonesia. Bahkan, dalam kurun waktu 5 tahun terakhir, tercatat sebanyak 34.622 kasus *Phising Cybercrime* dalam bentuk penipuan kartu kredit, pencurian identitas, dan kerugian finansial. *Phising* ini juga biasanya ditujukan kepada pengguna online

⁶³ Septian Arya Budi Mahesa, Hervina Puspitosari, "Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam Penanganan Perkara Tindak Pidana Phising", Jurnal Penelitian dan pengabdian masyarakat, Volume 2 No. 11, Maret 2023 (2686-2696), hal 2692

⁶⁴ Saputro, *Loc.cit.*

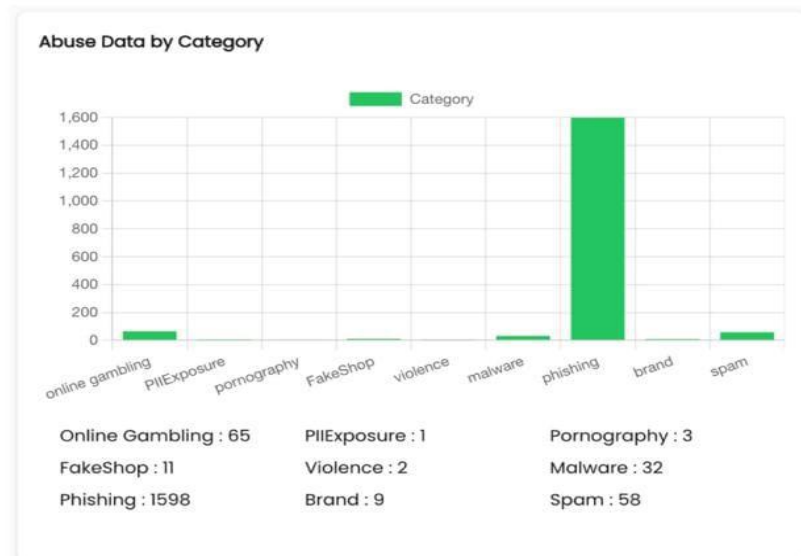
banking, karena menggunakan isian data (ID) pengguna dan kata sandi, dan tidak menutup kemungkinan untuk ditujukan ke pengguna online lainnya. Ketika pengguna memasukkan isian data pengguna miliknya dan kata sandinya ke *form login* yang merupakan *fake form login* maka akan diketahui oleh pelaku *cybercrime* dalam bentuk *phising* tersebut. Aksi *phising* ini semakin marak terjadi. Tercatat secara global, jumlah penipuan bermodus *phising* 42% dari modus selain *phising* yang dinyatakan dalam *website Anti-Phising Working Group (APWG)* dalam laporan bulannya, mencatat ada 12.845 *e-mail* baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana *phising*.⁶⁵

Berdasarkan kategori pada data IDADX Q2 2024 (*Indonesia Anti Phising Data Exchange*) periode April-Juni 2024 diperoleh kategori *phising* mendominasi jumlah laporan yaitu sebanyak 1.598 laporan. Berikut ini statistic data laporan IDADX berdasarkan kategorinya.⁶⁶

Gambar 1:

⁶⁵ Suhardi Rustam, Analisa Clustering Phising dengan K-Means dalam Meningkatkan Keamanan Komputer, *Ilkom Jurnal Ilmiah*, Vol. 10 No. 2, 2018, hlm. 175.

⁶⁶ Laporan Aktivitas Abuse Domain.Id Indonesia Anti-Phishing Data Exchange Periode Q2 2024 April-Juni 2024 https://api.idadx.id/documents/uploads/1724725529_Laporan%20Q2%202024.pdf.pdf



Sumber: <https://api.idadx.id/>

Indonesia menempati posisi teratas sebagai Negara yang menghosting situs abuse domain.id selama Q2 tahun 2024 dan dilanjutkan pada posisi kedua yaitu United State. Pada kuartal pertama ini Negara yang digunakan situs abuse domain lebih bervariasi daripada kuartal sebelumnya. Berikut ini tabel Negara yang masuk dalam aktivitas abuse domain.id (*Indonesia Anti Phising Data Exchange*).⁶⁷

Gambar 2:

⁶⁷ Laporan Aktivitas Abuse Domain.Id Indonesia Anti-Phishing Data Exchange Periode Q2 2024 April-Juni 2024 https://api.idadx.id/documents/uploads/1724725529_Laporan%20Q2%202024.pdf.pdf

Negara	April	Mei	Juni
Indonesia	45,56	60,2	54,06
United States	13,47	11,17	10,64
Russia	0,88	1,36	4,6
India	0,02		
China	1,03		
Germany	0,13	0,29	0,29
Singapore	0,13	0,67	0,84
United Kingdom	0,13	0,18	0,57
Canada	0,02	0,06	
Australia	0,2		0,13
Lithuania	0,15	0,04	
Spain	0,02	0,02	
Iran	0,02		
Norway	0,02	0,02	
Italy	0,02		0,03
Romania		0,1	
Malaysia		0,02	
Philippines			0,03
Brazil			0,03
None	37,22	25,87	28,46

Sumber: <https://api.idadx.id>

Hukum pada prinsipnya merupakan pengaturan terhadap sikap tindak (perilaku) seseorang dan masyarakat yang terhadap pelanggarnya diberikan sanksi oleh negara. Meskipun dunia *cyber* adalah dunia virtual, hukum tetap diperlukan untuk mengatur sikap tindak masyarakat, setidaknya ada dua hal yakni: Pertama, masyarakat yang ada di dunia maya adalah masyarakat yang ada di dunia nyata, masyarakat memiliki nilai dan kepentingan baik secara sendiri-sendiri maupun bersama-sama harus dilindungi. Kedua, walaupun terjadi di Dunia Maya, transaksi yang dilakukan oleh masyarakat memiliki Pengaruh dalam Dunia Nyata, Baik Secara Ekonomis maupun Non Ekonomis.⁶⁸

⁶⁸ Josua Sitompul, *Cyberspace, Cybercrime, Cyberlaw*, Tinjauan Aspek Hukum Pidana, Jakarta: PT Tatanusa, 2012.

Pembentukan hukum hendaknya mengarahkan kepada hakikat hukum (*law truth*). Artinya, pembentukan undang-undang merupakan suatu cara untuk memajukan dan melindungi kepentingan tertentu atau mengutamakan suatu kepentingan di atas yang lain.⁶⁹

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang dikenakan kepada pelaku *phising*, jenisnya adalah tindak pidana penjara dan tindak pidana denda, tidak adanya ancaman sanksi pidana tambahan. Jadi sistem pidana yang dipakai tidak ada inovasi jenis Sanksi Pidana yang khas untuk Tindak Pidana di bidang informasi dan transaksi elektronik.⁷⁰ Pengaturan Hukum Tindak Pidana *Phising* Terhadap Korban Pelaku dijerat Pasal 51 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Ketentuannya dapat dilihat, yaitu: “Setiap Orang yang Memenuhi Unsur Sebagaimana dimaksud di dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).” Unsur-unsur yang terdapat di dalam Pasal 35.

Pemidanaan terhadap Pelaku untuk Menegakkan Hukum bagi Para Korban dianggap sebagai langkah yang tepat sehingga kebanyakan bentuk ketentuan pidana

⁶⁹ Widiatama Widiatama, Hadi Mahmud, and Suparwi Suparwi, “Ideologi Pancasila Sebagai Dasar Membangun Negara Hukum Indonesia,” *Jurnal Usm Law Review* 3, no. 2, 2020, 310–27.

⁷⁰ Muhammad Kamran and Maskun Maskun, “Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika,” *Balobe Law Journal* 1, no. 1, 2021, 41–56.

yang tercantum dalam Undang-Undang Informasi dan Transaksi Elektronik dan juga Kitab Undang-Undang Hukum Pidana, dibuat dengan pemberian sanksi berupa pidana penjara dan pidana denda karena dirasa sudah bisa terselesaikan perkara tersebut dengan memberikan efek jera terhadap pelaku. Sehingga, pidana penjara dan pidana denda bagi pelaku tindak pidana dirasa tidak optimal dalam melindungi dan memenuhi hak para korban untuk mengganti kerugian secara materiil yang tidak sepatutnya korban alami, terlebih khusus bagi korban *Cybercrime* yang perekonomiannya lemah. Hal ini pun dianggap juga sebagai hak warga negara untuk mendapat jaminan, dan perlindungan hukum yang seadil-adilnya.⁷¹

Kerugian materiil bagi korban tindak pidana *Cybercrime* berbentuk *Phising* ini, restitusi adalah metode yang tepat. Seperti dalam Pasal 1 ayat 11 yang menyebutkan bahwa “restitusi berupa ganti kerugian yang diberikan kepada korban atau keluarganya oleh pelaku atau pihak ketiga.”⁷² Hal ini diatur juga dalam Pasal 1 ayat 8 Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, yang menyebutkan, “perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban yang wajib dilaksanakan oleh LPSK atau lembaga lainnya sesuai dengan ketentuan undang-undang ini.”⁷³

⁷¹ Faiz Emery, *Op.cit.*, halaman 233

⁷² *Ibid*, halaman 235

⁷³ *Ibid*, halaman 235

Undang-undang Perlindungan Saksi dan Korban yaitu masih bersifat fakultatif, karena tergantung pada keputusan LPSK untuk pemenuhan hak-hak saksi dan korban tersebut. Kelemahan lainnya yaitu: undang-undang ini tidak menjelaskan lebih lanjut pada tindak pidana apa saja restitusi tersebut dapat diajukan, sehingga penegak hukum tidak serta merta memfasilitasi korban terhadap pengajuan hak atas restitusi tersebut. Pengajuan hak korban atas restitusi menjadi suatu ketidakpastian, yang bermuara pada ketidak-pastian jenis atau kualifikasi tindak pidana sebagai syaratnya. Aturan umum KUHP tidak mengenal jenis “pidana ganti rugi”. Pidana bersyarat yang memuat ganti rugi dalam Pasal 14c KUHP tentang pidana bersyarat pada dasarnya tidak bersifat pidana dan hanya sekedar pengganti untuk menghindari ataupun tidak menjalani pidana.⁷⁴ Ganti rugi dalam KUHP Pasal 14c tentang pidana bersyarat hanya sebagai syarat khusus bagi terpidana agar tidak menjalani pidana pokok, yaitu kalau hakim tidak menjatuhkan putusan pemidanaan terhadap pelaku. Ditetapkannya syarat khusus berupa ganti rugi hanya bisa diberikan hakim berdasarkan putusannya berupa pidana penjara paling lama 1 tahun atau pidana kurungan dan juga syarat khusus ini hanya bersifat fakultatif.⁷⁵

Namun, dapat diketahui bahwa *cybercrime* dalam bentuk *phising* itu sendiri satu kesatuan antara membuat situs yang seolah-olah dengan situs asli resminya dengan melakukan tindakan kebohongan mengirimkan sebuah *e-mail* yang isi nya

⁷⁴ Barda Nawawi Arief, Beberapa Aspek Kebijakan Penegakan Dan Pengembangan Hukum Pidana, Bandung, Citra aditya bakti, 1998.

⁷⁵ *Op.cit*, halaman 235

mengarahkan ke situs palsu tersebut, dimana orang yang mengaksesnya diperintahkan untuk memperbarui informasi pribadi rahasianya, dan kemudian informasi pribadi rahasianya diketahui oleh pelaku *phising* tersebut.⁷⁶

Phising merupakan perbuatan yang melawan hukum, karena telah melakukan suatu tindak pidana yang merugikan orang lain. *Cybercrime* dalam bentuk *phising* ini juga merupakan suatu delik materiil, Karena dapat dikatakan *phising* merupakan suatu tindak pidana ketika *cybercrime* dalam bentuk *phising* ini perbuatannya telah merugikan orang lain yaitu informasi rahasia pribadi orang tersebut atau si korban diketahui oleh pelaku *phising*.⁷⁷

Tetapi, dari semuanya yang telah diuraikan di atas. Pasal 35 jo Pasal 51 ayat (1) tidak memuat unsur kebohongan yang merugikan orang lain dan Pasal 28 ayat (1) jo Pasal 45A ayat (1) tidak memuat unsur manipulasi, penciptaan, dan perubahan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, maksudnya tidak memuat unsur seseorang membuat situs yang seolah-olah mirip situs asli resminya.⁷⁸

Hukum tidak dapat dikenakan apabila hukumnya mengalami kekaburan seperti pasalnya memiliki penafsiran yang bermacam-macam atau konsepnya belum ada dan aturan yang diterapkan untuk pelaku tindak pidana tidak tegas dan jelas, maka

⁷⁶ Saputro Gulo, *Op.cit*, halaman 78

⁷⁷ *Ibid*, halaman 78

⁷⁸ *Ibid*, halaman 78

kebijakan hukum yang dilakukan terhadap konsep *cyber phishing* dan pasal 35 berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah Konsep *Phising* dan Pasal 35 tersebut.⁷⁹

Berdasarkan uraian di atas dapat disimpulkan bahwa pengaturan tindak pidana *Phising* diatur dalam Undang-Undang Nomor 9 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun belum ada Pasal secara khusus untuk membahas mengenai Tindak Pidana *Phising* karena Pasal yang dijatuhkan kepada pelaku tindak pidana *phising* akan dikenakan pasal yang memiliki kesesuaian unsur atau delik kejahatan tindak pidananya.

B. Pertimbangan Hukum Oleh Hakim Dalam Putusan No.60/Pid.Sus/2022/Pn.Bjr Atas Tindak Pidana *Phising*

Pertimbangan Hakim merupakan pandangan atau pendapat majelis Hakim dalam memutus dan mengadili suatu perkara dengan memperhatikan dan mempertimbangkan keadaan yang memberatkan dan meringankan pelaku tindak pidana.⁸⁰ Berdasarkan Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman pada Pasal 14 Ayat (2), yang mana dalam setiap sidang permusyawaratan Majelis Hakim, masing-masing Hakim wajib memberikan pendapat atau pertimbangannya secara tertulis

⁷⁹ *Ibid*, halaman 79.

⁸⁰ Mulyadi, Lilik, Hukum Acara Pidana Normatif, Teoritis, Praktik dan Permasalahannya, Bandung, Alumni, 2012, Hlm. 193.

terhadap perkara yang sedang ia adili.⁸¹ Dalam Pasal 197 Ayat (1) huruf d KUHAP disebutkan bahwa pertimbangan Hakim haruslah ditulis dan disusun secara lugas mengenai keadaan dan fakta serta Alat Bukti yang didapat dari hasil pemeriksaan di muka persidangan yang akan menjadi landasan penentuan kesalahan yang didakwakan pada terdakwa. Secara yuridis, dalam sistem pembuktian yang dianut oleh hukum pidana Indonesia bahwa sistem pembuktian adalah berdasarkan undang-undang secara negatif (*negatief wettelijk bewijs theotrie*). Sistem pembuktian menurut teori ini menyatakan Hakim hanya dapat menjatuhkan putusan pidana kepada terdakwa apabila terdapat 2 (dua) alat bukti yang sah serta berdasarkan pada keyakinan Hakim bahwa suatu tindak pidana benar-benar telah terjadi dan terdakwalah yang terbukti bersalah melakukan tindakan.⁸²

Hakim dalam memberikan hukuman atau pidana kepada terdakwa haruslah memiliki banyak pertimbangan, mulai dari pertimbangan terhadap tuntutan Penuntut Umum, terpenuhi atau tidaknya unsur-unsur delik yang dilanggar dengan pasal yang didakwakan, hingga pertimbangan mengenai keadaan yang meringankan dan memberatkan pidana. Berdasarkan sifatnya, pertimbangan Hakim dibagi menjadi 2 (dua) diantaranya pertimbangan yuridis dan non-yuridis. Pertimbangan Hakim yang dilandaskan pada fakta-fakta hukum (yuridis) yang terungkap dalam pemeriksaan di muka pengadilan dan ditetapkan sebagai hal yang harus ada dalam suatu putusan merupakan definisi dari pertimbangan Hakim yang bersifat yuridis. Aspek-aspek yang

⁸¹ *Ibid.*, halaman 193

⁸² *Ibid.*, halaman 193

menjadi pertimbangan yuridis ialah surat dakwaan, surat tuntutan, keterangan saksi, keterangan terdakwa, barang bukti beserta pasal-pasal yang didakwakan harus ada dalam suatu putusan.⁸³ Sedangkan, pertimbangan yang mempertimbangkan latar belakang terjadinya delik, faktor dampak dari tindakan terdakwa dan kondisi diri terdakwa pada saat dan setelah melakukan tindak pidana, kondisi sosial ekonomi terdakwa, dan keyakinan Hakim bahwa terdakwa telah terbukti bersalah melakukan delik sebagaimana pasal-pasal yang disangkakan kepadanya merupakan pengertian dari pertimbangan non-yuridis.⁸⁴ Begitupun dengan pertimbangan yang bersifat non-yuridis juga merupakan pertimbangan yang mutlak dalam sebuah putusan. Hal ini bersesuaian dengan Pasal 5 Ayat (1) Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman yang menjelaskan bahwa Hakim wajib menggali, mengikuti serta memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat. Dalam perkara sebagaimana putusan pengadilan yang menjadi pembahasan tulisan ini dapat diketahui bahwa berdasarkan dakwaan Penuntut Umum dalam Putusan Nomor: 60/Pid.Sus/2022/Pn.Bjr, Terdakwa oleh Penuntut Umum dengan alternatif yaitu Undang-undang Nomor 11 Tahun 2008 Informasi Transaksi Elektronik Pasal 51 Ayat (1) jo. Pasal 35, kemudian Pasal 378 KUHP tentang delik Pemalsuan Surat. Adapun tuntutan dari Penuntut Umum ialah menyatakan terdakwa terbukti secara sah bersalah melakukan tindak pidana *Phising* dalam membuat surat palsu atau memalsukan surat

⁸³ Syarifah Dewi Indawati, Dasar Pertimbangan Hukum Hakim Menjatuhkan Putusan Lepas dari Segala Tuntutan Hukum Terdakwa dalam Perkara Penipuan, Jurnal Verstek 5, Nomor 2, 2015, 269-270.

⁸⁴ *Ibid.*, halaman 270-271.

yang diancam dengan Pasal 378 KUHP dengan menjatuhkan pidana Terdakwa selama 2 (dua) Tahun 6 (enam) bulan Pidana Penjara. Di samping itu, Penuntut Umum juga menuntut beberapa barang bukti yang dirampas untuk Negara serta membebani Terdakwa dengan membayar biaya perkara sejumlah Rp.2.000,- (dua ribu rupiah).

1. Kasus Posisi

Berawal terdakwa Maulana Malik Rahman bin Karim Ansori telah melakukan tindak pidana penglabuan (*phising*) dan penipuan berupa sertifikat kompetensi kerja (SKK) dan sertifikat badan usaha (SBU) pada hari sabtu, tanggal 5 february 2022 ditempat fotokopi kota banjar. Dalam tindakanya terdakwa maulana malik Rahman bin karim ansori sudah menipu 15 orang korban dan beserta saksi yang bernama M. ichwanto.

Untuk melancarkan perbuatannya, terdakwa maulana malik Rahman bin karim ansori telah mengambil contoh sertifikat kompetensi kerja dan sertfikat badan usaha melalui Lembaga sertifikat profesi astekindo. Lalu setelah mendapatkannya terdakwa hanya akan mengubah data dalam sertifikat dari Lembaga menjadi data korban. Sebelum membuat SKK dan SBU. Korban telah bertemu saksi M. ichwanto selaku rekan kantor terdakwa maulana malik Rahman bin karim ansori saat terdakwa sedang melaminating sertifikat kerja ahli (SKA). Kemudian terdakwa maulana malik Rahman bin karim ansori menawarkan kepada saksi M. ichwanto bahwa terdakwa bisa membuat SKK dan SBU dengan menjanjikan proses cepat dan tanpa tes atau assesmen. Terdakwa maulana malik Rahman bin karim ansori juga meminta tolong bantuan kepada saksi M. ichwanto untuk mengurus skk dan sbu milik korban dan yang ternyata

korban tersebut Sebagian adalah rekan-rekan saksi M. ichwanto.

Selesai membuat SKK tersebut, Terdakwa langsung mengirimkan 15 (lima belas) buah Sertifikat Kompetensi Kerja (SKK) dalam bentuk dokumen elektronik berupa file pdf kepada Saksi M. Ichwanto melalui pesan whatsapp. Setelah menerima 15 (lima belas) buah Sertifikat Kompetensi Kerja (SKK) dalam bentuk dokumen elektronik berupa file pdf dari Terdakwa, Saksi M. Ichwanto melihat banyak tulisan yang salah pada SKK tersebut dan dari bentuknya agak berbeda, sehingga Saksi M. Ichwanto menanyakannya kepada Terdakwa, mengetahui hal tersebut Terdakwa langsung memperbaiki SKK tersebut agar Saksi M. Ichwanto tetap merasa yakin kepada Terdakwa dan bahwa SKK tersebut asli, lalu Terdakwa mengirimkan kembali SKK tersebut kepada Saksi M. Ichwanto.

Kemudian karena saksi M. Ichwanto yang merasa curiga dengan SKK yang diterimanya dari Terdakwa, Saksi M. Ichwanto menanyakannya kepada Saksi Hera Limaya bin (alm.) Tatang Permana dan setelah dilakukan pengecekan menggunakan aplikasi Jakontrust milik Kementerian Pekerjaan Umum dan Perumahan Rakyat diketahui bahwa 15 (lima belas) buah Sertifikat Kompetensi Kerja (SKK) tersebut datanya tidak muncul dan tidak terdaftar. Mengetahui hal tersebut, Saksi M. Ichwanto menyampaikannya kepada rekan-rekannya yang memintanya untuk membantu mengurus pembuatan SKK dan SBU, hingga akhirnya perbuatan Terdakwa dilaporkan kepada Polres Banjar untuk diproses lebih lanjut.

2. Analisis Hukum

Terdakwa Maulana malik rahman bin karima ansori didakwa oleh jaksa penuntut

umum telah melakukan tindak pidana *phising* dan Tindak Pidana Penipuan dengan tuduhan pasal 51 ayat (1) juncto Pasal 35 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Pasal 378 Kitab Undang-undang Hukum Pidana Perbuatan yang dituduhkan kepada terdakwa karena telah melakukan tindakannya. Untuk membuktikan dakwaannya, Jaksa Penuntut Umum menghadirkan alat bukti elektronik berupa;

1. (satu) buah Laptop, merek Asus X454WA-VX004D, warna Hitam; 1 (satu) buah Printer, merek HP Deskjet Ink Advantage 2336, warna Putih; 1 (satu) buah Handphone, merek Vivo, warna Biru, Nomor Imei 1.
2. 1 (satu) buah Flash Drive, merek Sandisk, pemindahan file (export) dari Handphone merek OPPO A5 2020. dan, Jaksa Penuntut Umum Juga menghadirkan alat bukti surat berupa;
 1. 15 (lima belas) dokumen Surat Kompetensi Kerja (SKK) yang tidak terdaftar
 2. alat bukti surat berupa dokumen elektronik/ PDF Sertifikat Kompetensi Kerja (SKK);
 3. 4 (empat) lembar Kwitansi Pembayaran dari Sdr. Ichwanto kepada Sdr. Maulana Malik Rahman.

Tidak hanya itu, JPU juga menghadirkan alat bukti saksi sebanyak 4 saksi. Saksi yang bernama M. Ichwanto bin Winarto menjelaskan apabila terdakwa menawari saya

untuk membantunya menawarkan pembuatan skk palsu kepada korban dan juga rekan m.ichwanto, saksi juga berkata tidak menerima keuntungan sepeserpun saat membantu terdakwa dalam perbuatannya dan dalam keterangan saksi m. ichwanto terdakwa maulana malik rahman bin karim ansori merasa keberatan dikarenakan terdakwa berkata saksi m. ichwanto juga menerima hasil yang diberikan terdakwa maulana malik rahman bin karim ansori. Selanjutnya saksi yang bernama saud bin udin menjelaskan apabila terdakwa maulana malik rahman bin karim ansori menerbitkan skk palsu saat saksi di beritahukan kepada saksi yang bernama m.ichwanto, dan ternyata saksi m.ichwanto meminta saksi saud bin udin menemani m.ichwanto untuk menyerahkan uang kepada terdakwa maulana malik rahman bin karim ansori yang awalnya saksi saud bin udin tidak mengetahui uang siapa yang diberikan saksi m. ichwanto kepada terdakwa maulan malik rahman bin karim ansori dan saksi saud bin udin tidak mengetahui ada tidaknya tanda terima dalam penyerahan uang antara saksi m. ichwanto dan terdakwa maulana malik rahman bin karim ansori.

Selanjutnya saksi yang bernama Hera Limaya bin Tatang Permana menjelaskan apabila terdakwa maulana malik rahman bin karim ansori telah membuat skk palsu saat saksi m. ichwanto meminta bantuan kepada saksi hera limaya bin tatang permana saat saksi M. ichwanto meminta untuk mengecek 15 Salinan skk digital di jakontrust milik kementerian PUPR karena memiliki tampilan berbeda dan menemukan kejanggalan saat akan dicetak yang ternyata saat di cek 15 salinan skk digital tidak terdaftar. Selanjutnya saksi yang bernama Dwi Eki Oktora, S.T. bin Yayat Ruhiyat menjelaskan apabila saksi dwi eki oktora adalah salah satu yang meminta bantuan Sdr. M. Ichwanto untuk

pengurusan sertifikat kompetensi kerja saksi dwi eki oktora dan tidak tahu menahu tentang hubungan antara saksi m. ichwanto dengan terdakwa maulana malik rahman bin karim ansori karena saksi dwi eki oktora awalnya diperkenalkan oleh saudara ade satrio untuk menghubungi kepada saksi m. ichwanto untuk membantu membuat Surat Kompetensi Kerja (SKK), setelah kejadian terungkap terdakwa langsung membenarkan dan akan bertanggung jawab.

Bahwa untuk membela kepentingan hukumnya, terdakwa memberikan keterangan di pengadilan bahwa terdakwa maulana malik rahman bin karim ansori benar melakukan pembuatan sertifikat kompetensi kerja palsu, menawarkan saudara m. ichwanto untuk membantunya, mengambil uang sejumlah Rp37.450.000,00 (tiga puluh tujuh juta empat ratus lima puluh ribu rupiah), saksi m. ichwanto pernah menyewa pembuatan sertifikat kompetensi kerja untuk rekannya kepada terdakwa dan memberikan sebagian uangnya kepada saudara m. ichwanto yang tidak mengaku saat bersaksi, mengambil sampel skk di lembaga Sertifikasi Profesi (LSP) Astekindo Mandiri yang berkedudukan di Jakarta, membuat 15 (lima belas) dokumen Sertifikat Kompetensi Kerja pada tanggal 7 Maret 2022 sekira pukul 01.00 s.d. 06.00 WIB, mengedit sertifikat asli menggunakan aplikasi Paint dan Adobe Acrobat DC dalam Laptop merek Asus X454WA-VX004D, kemudian dicetak menggunakan printer merek HP Deskjet Ink Advantage 2336. Selanjutnya mengirimkan salinan digital sertifikat tersebut dalam format PDF melalui WhatsApp pada tanggal 7 Maret 2022. Sedangkan 1 (satu) dokumen Sertifikat Badan Usaha belum sempat dibuat oleh Terdakwa karena Saudara. M. Ichwanto meminta pengembalian uang setelah

mengetahui sertifikat kompetensi kerja tidak terdaftar.

Berdasarkan fakta persidangan yang ada Majelis Hakim mempertimbangkan apabila bersalah atau tidaknya kesalahan terdakwa atas perbuatan yang didakwakan jaksa, dengan memperhatikan fakta-fakta di atas, dan supaya singkatnya, dicatat dalam berita acara sidang. Jika kesalahan terdakwa terbukti, sesuai dengan Pasal, akan mempertimbangkan tingkah laku terdakwa dan cukupnya bukti-bukti lain. karena terdakwa Maulana Malik Rahman bin Karim Ansori didakwa jaksa penuntut umum dengan dakwaan kumulatif lain maka Majelis Hakim akan mempertimbangkan terlebih dahulu dakwaan kumulatif pertama sesuai dengan Pasal 51 ayat 1 yang dibaca dengan Pasal 35 Undang-Undang Republik Indonesia Nomor 11 Undang-Undang Informasi dan Transaksi Elektronik Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Elektronik dan Transaksi Elektronik. yang unsurnya yaitu;

1. Setiap orang.
2. dengan sengaja atau tanpa hak memanipulasi informasi elektronik dan/atau dokumen elektronik dengan sengaja dan tanpa hak atau melanggar hukum, dengan tujuan agar tampak demikian. Itu adalah data nyata.

Selama proses persidangan berlangsung Majelis Hakim memeriksa semua alat bukti (keterangan saksi, keterangan ahli dan keterangan terdakwa, bukti surat/ keterangan petunjuk) beserta barang bukti yang dihadirkan oleh penuntut umum di muka persidangan. Semua itu dijadikan sebagai bahan pertimbangan agar dapat

diketahui terpenuhinya unsur-unsur delik serta hakim juga mempertimbangkan terkait keadaan yang memberatkan dan meringankan pidana bagi Terdakwa.

Dalam pemeriksaan sidang, pada saat Terdakwa memberikan keterangan di persidangan, ia mengaku berterus terang tak hanya melakukan satu tindak pidana saja, yaitu Phising. Akan tetapi juga mengakui bahwa Terdakwa melakukan tindak pidana pencurian secara elektronik di situ web. Hakim dalam putusannya, meyakini, dan mempercayai bahwa Terdakwa telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana manipulasi data secara elektronik yang dijerat dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik, Pasal 51 ayat (1) jo. Pasal 35 dengan pidana penjara selama 2 (dua) tahun 6 (enam) bulan.

Berkenan dengan Putusan Nomor: 60/Pid.Sus/2022/Pn.Bjr, dalam pertimbangan yuridis, majelis Hakim memang sudah menjatuhkan putusan yang sesuai dengan tuntutan Penuntut Umum. Akan tetapi, hal menarik berdasarkan keterangan dan pengakuan terdakwa di muka persidangan membuktikan bahwa sebenarnya terdakwa tidak hanya melakukan satu tindak pidana saja (*phising*), akan tetapi juga terbukti melakukan tindak pidana pencurian secara elektronik. Artinya, terdapat lebih dari satu tindak pidana dengan unsur delik yang berbeda yang dilakukan oleh Terdakwa. hal tersebut dapat menjadi pertimbangan Hakim secara yuridis untuk memberatkan atau menambah pidana bagi Terdakwa karena salah satu syarat pemberatan pidana ialah melakukan perbarengan tindak pidana yang mana masing-masing unsur perbuatan pidana itu berdiri sendiri, maka Hakim dapat menjatuhkan hukuman dengan jumlah maksimum pidana yang terberat ditambah sepertiga sebagaimana tercantum dalam

Pasal 65 ayat (2) KUHP.

Kesimpulan yang diambil oleh Majelis Hakim atas seluruh fakta persidangan adalah menghukum terdakwa Maulana Malik Rahman bin Karim Ansori karena telah melakukan tindak pidana *phising* sebagaimana yang diatur dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 35 Jo. Pasal 51 Ayat 1 dan Pasal 378 Kitab Undang-Undang Hukum Pidana Atas Perubahan Undang-Undang Nomor 1 Tahun 2023 Pasal 492 Kitab Undang-Undang Hukum Pidana Tentang Penipuan serta Pasal-pasal dalam Undang-undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.

Pada prinsipnya menurut undang-undang kekuasaan kehakiman pada Pasal 14 Ayat (2), Hakim dalam menjatuhkan putusannya adalah bersifat independen. Artinya, Hakim dalam menjalankan tugas dan fungsinya, diberikan kekuasaan yang merdeka dan bebas dari intervensi pihak luar baik itu berupa tekanan fisik maupun psikis. Sehingga, Hakim dapat mempertimbangkan hukuman yang akan dijatuhkan kepada Terdakwa termasuk pemberatan pidana dengan memperhatikan aspek-aspek lainnya apalagi menyangkut keterangan dan pengakuan terdakwa di persidangan yang menjadi Pertimbangan Yuridis dalam Sebuah Putusan.⁸⁵ Dalam memutus perkara hakim

⁸⁵ Indah Eka Putri dan Ismansyah, "Analisis Yuridis Putusan Hakim Dalam Perkara Tindak Pidana Phising Yang Dilakukan Melalui Media Sosial", Jurnal Hukum Pidana Dan Kriminologi, DELICTI,

tidaklah harus sama dengan tuntutan Penuntut Umum.⁸⁶ Selanjutnya, apabila ditinjau dari besarnya kerugian beserta lamanya terdakwa melakukan tindak pidana (kurang dari 1 tahun) tersebut, dapat dikatakan hukuman yang dijatuhkan kepada terdakwa relative rendah hanya dengan memberikan 2 (dua) Tahun 6 (enam) bulan penjara, karena ancaman maksimum pidana yang dapat dijatuhkan sebagaimana diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik Pasal 51 ayat (1) yaitu maksimal 12 (dua belas) tahun penjara lamanya. Belum lagi berdasarkan fakta dipersidangan Terdakwa juga melakukan perbarengan tindak pidana yang tak hanya *phising*, tetapi Juga tindak pidana pencurian secara elektronik yaitu mengambil contoh salinan digital dengan cara mengambil dari situs web. Tindak pidana *phising* diatur dalam Pasal 51 ayat (1) jo. Pasal 35 Undang-Undang ITE dengan ancaman maksimal 12 tahun penjara dan /atau denda maksimal 12 milyar rupiah, Artinya, setiap perbuatan pidana yang dilakukan oleh Terdakwa itu berdiri sendiri sehingga ada alasan untuk memberikan pemberatan pidana bagi Terdakwa.

Secara yuridis Hakim dalam menjatuhkan vonis memang sudah sesuai dengan tuntutan Jaksa yaitu dua tahun enam bulan penjara, namun menurut penulis Hakim belum mempertimbangkan perbarengan tindak pidana yang dilakukan oleh Terdakwa. Pada perkara ini Hakim dapat memberikan pemberatan pidana atas perbuatannya tersebut berdasarkan Pasal 65 ayat (2) KUHP. Selain itu, Hakim dalam menjatuhkan suatu putusan juga bersifat independen sehingga tanpa intervensi Hakim boleh

Volume 1 Nomor, 2023, hlm 5.

⁸⁶ *Ibid.*, halaman 5.

menjatuhkan pidana yang lebih tinggi dari tuntutan Penuntut Umum asalkan masih berlandaskan pada peraturan perundang-undangan. Kemudian, dari penerapan sanksi pidana yang relatif ringan tersebut, setelah ditinjau menggunakan teori tujuan pemidanaan yang dikaitkan dengan tujuan pembuat Undang-Undang ITE ternyata belum dapat terpenuhi tujuan pemidanaan dan rasa keadilan sehingga hal ini dapat berdampak pada ketidakefektifitasan pemidanaan di kemudian hari.

C. Pertanggungjawaban Pelaku Tindak Pidana Phishing Dalam Putusan No.60/Pid.Sus/2022/Pn.Bjr

Peraturan hukum di Indonesia mengenal asas *Lex Specialis derogat legi Generalis* dalam bahasa latin yang berarti peraturan hukum yang lebih khusus mengesampingkan peraturan hukum yang lebih umum.⁸⁷ Karena *phising* termasuk kejahatan penipuan dalam *cybercrime*, maka pertanggungjawaban pidana pada pelaku *phising* dalam putusan ini tidak hanya menggunakan peraturan dalam KUHP melainkan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi Dan Transaksi Elektronik karena Undang-Undang tersebut bersifat khusus. Untuk saat ini lembaga Penegak Hukum di Indonesia menggunakan Pasal 35 jo. Pasal 51 ayat (1) dan Pasal 378 KUHP dalam memutuskan dakwaannya terhadap pelaku *phising* tersebut.

Pelaku *Phising* dalam putusan ini tidak hanya membuat sebuah SKK palsu yang terlihat akan seperti SKK asli, tetapi pelaku *Phising* tersebut juga melakukan tindakan

⁸⁷ Shinta Agustina, 2010, Implementasi Asas Lex Specialis Derogat Legi Generali Dalam Sistem Peradilan Pidana, hlm 504.

penipuan untuk menyesatkan orang lain yang bertujuan untuk mendapatkan memperoleh sejumlah uang untuk kepentingan pribadi nya sehingga menyebabkan kerugian kepada beberapa orang yang menjadi korban kejahatan ini. maka perbuatan tersebut dapat dikenakan pasal 35 jo. pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan pasal 378 kuhp. Rumusan pasal 35 jo. pasal 51 ayat (1) sebagai berikut:

1. Pasal 35

“Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”

2. Pasal 51

“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).”

Selanjutnya Rumusan 378 KUHP:

3. Pasal 378

“Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun.”

Berdasarkan rumusan Pasal di atas, tindak pidana *phising* dalam putusan ini telah melakukan suatu tindakan melawan hukum yang melanggar ketentuan Pasal 35 karena telah membuat sertifikat palsu yang seolah-olah mirip dengan sertifikat yang asli, selain itu juga melanggar ketentuan Pasal 378 kuhp dengan melakukan suatu penipuan atau kebohongan untuk menarik korban untuk membuat skk palsu dengan iming-iming

tanpa melakukan tes dan hanya mengirim data korban sehingga menyebabkan kerugian.

Pertanggungjawaban dalam ranah hukum pidana adalah elemen krusial yang tak terpisahkan. Tanpanya, sanksi yang di kenakan terhadap pelaku kejahatan akan kehilangan signifikansinya. Karena itu, memahami dan memperhatikan konsep pertanggungjawaban pidana dalam konteks hukum pidana sangatlah penting.⁸⁸ Roeslan Saleh berpendapat tentang Pertanggungjawaban Pidana adalah suatu perbuatan yang tercela oleh masyarakat dan di pertanggungjawabkan kepada si pembuat pidananya atas perbuatan yang telah dilakukanya. Menurut roeslan Saleh bahwa seseorang mampu bertanggung jawab jika jiwanya sehat apabila:

- a. Mampu untuk mengetahui untuk menyadari bahwa perbuatannya bertentangan dengan hukum.
- b. Dapat menentukan kehendak sesuai dengan kesadaran tersebut.

Tindakan seseorang harus bertanggungjawab berdasarkan konsep atau pemikiran dasar terhadap bukti keberadaan unsur-unsur tindak pidana. Apabila unsur-unsur tindak pidana terbukti, kesalahan mereka juga terbukti, yang kemudian mengakibatkan mereka dijatuhi hukuman, sehingga tanggung jawab pidana diterapkan pada unsur-unsur tindak pidana.⁸⁹

Meskipun pembuatnya memenuhi unsur delik dalam undang-undang dan tidak

⁸⁸Kajian Yuridis Terhadap Pertanggungjawaban Tindak Pidana Informasi Dan Transaksi Elektronik (ITE, Vidya Wertha 6, No.1 (2023):50-59.

⁸⁹ H.M. Rasyid Ariman dan Fahmi Raghil. Hukum Pidana, Malang, Setara Press, 2015, hlm 205.

dibenarkan, namun hal tersebut belum memenuhi syarat untuk menjatuhkan pidana. Untuk pidanaan masih perlu adanya syarat, bahwa orang yang melakukan perbuatan itu mempunyai kesalahan atau bersalah. Dengan perkataan lain, orang tersebut harus dapat di pertanggungjawabkan atas perbuatannya atau jika dilihat dari sudut perbuatannya baru dapat dipertanggungjawabkan kepada orang tersebut. Disinilah berlaku apa yang disebut asas “tiada pidana tanpa kesalahan” (*keine strafe ohne schuld*).⁹⁰

Pertanggungjawaban pidana terhadap tindak pidana *phising* dalam putusan ini dapat dikenakan pasal berlapis yaitu Pasal 35 jo. Pasal 51 ayat (1) dan pasal 378 kuhp serta tidak boleh melebihi maksimum pidana yang terberat ditambah sepertiga. sistem ini dikenal sebagai kumulasi diperlunak, Istilah ini mengenai hal tersebut yaitu perbarengan Peraturan atau “*Concursus Realis*” yang terjadi ketika seseorang melakukan lebih dari satu tindakan, dan masing-masing tindakan tersebut berdiri sendiri sebagai suatu tindak pidana dan tindak pidana yang dilakukan tidak harus berkaitan satu sama lain. Maka yang dipakai adalah ketentuan pidana pokok yang terberat.⁹¹

Apabila “*Concursus Realis*” diterapkan pada tindak pidana *phising* dalam putusan, maka penerapannya dalam Pasal 35 jo. Pasal 51 ayat (1) dikenakan dengan pidana penjara paling lama 12 (dua belas tahun) dan denda paling banyak Rp.

⁹⁰ Septa Candra. “Pembaharuan Hukum Pidana; Konsep Pertanggungjawaban Pidana Dalam Hukum Pidana Nasional Yang Akan Datang”, Jurnal Cita Hukum I, No. 1, 2013, hlm. 39-56.

⁹¹ Teguh Prasetyo, 2013, Hukum Pidana, PT. Raja Grafindo Persada, Jakarta, hlm 182.

12.000.000.000,00 (dua belas miliar rupiah), maka penetapan pada Pasal 35 jo. Pasal 51 ayat (1) dapat ditentukan sebagai pidana yang paling berat, yaitu hukuman maksimal 12 tahun penjara dan denda paling banyak sebesar Rp.12.000.000.000,00, kemudian pidana yang berat tersebut ditambah sepertiga untuk setiap pidananya. Pada pidana penjara, $12 \text{ tahun} + (1/3 \times 12) = 16 \text{ tahun}$ penjara, lalu pada pidana denda $\text{Rp.12.000.000.000,00} + (1/3 \times 12.000.000.000) = \text{Rp.16.000.000.000,00}$ (enam belas miliar rupiah).

Dengan demikian, ancaman pidana dalam Pasal 35 jo. Pasal 51 ayat (1) dan Pasal 378 KUHP jika dijumlahkan yaitu $12 \text{ tahun} + 4 \text{ tahun} = 16 \text{ tahun}$, penjatuhan pidana tersebut diperkenankan karena tidak melebihi batas maksimum pidana penjara terberat setelah ditambah sepertiganya yaitu 16 tahun penjara, maka maksimum pidana penjara yang akan dijatuhkan adalah 16 tahun. Selain itu, jika pidana denda tersebut diperkenankan karena tidak melebihi batas pidana denda terberat setelah ditambah sepertiganya yaitu Rp. 16.000.000.000,00.

Sesuai dengan uraian di atas, dapat disimpulkan bahwa pelaku *phising* dalam putusan ini telah dijatuhkan pidana sesuai dengan Pasal 35 ayat (1) jo. Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan pasal 378 kuhp dengan ancaman pidana paling lama 16 (enam belas) tahun penjara dan denda paling banyak sebesar Rp. 16.000.000.000,00 (enam belas miliar rupiah).

Jenis pidana yang diberikan terhadap pelaku *phising* dalam putusan ini adalah pidana pokok yang meliputi pidana penjara dan pidana denda menurut *stelsel straf*

maksimum yang digunakan dalam KUHP. Hakim dapat memutuskan hukuman yang akan dijatuhkan (berapa tahun penjara dan besarnya denda) berdasarkan aturan dalam UU ITE. Ketentuan dalam pidana tersebut, hakim dapat menggabungkan sistem alternatif atau sistem kumulatif, yang berarti hakim memiliki pilihan apakah tindak pidana tersebut dijatuhkan pidana penjara atau denda ataupun keduanya. Pidana penjara terhadap pelaku *phising* dalam putusan ini yaitu dengan memberlakukan pembatasan kebebasan bergerak seperti pelaku tindak pidana yang lain, selanjutnya pelaku di tahan di dalam lembaga pemasyarakatan dengan kewajiban menaati segala aturan yang berlaku di dalamnya.⁹²

Dalam perumusan terhadap ancaman tindak pidana yang bersifat imperatif, merupakan warisan dari pemikiran aliran klasik dalam menentukan pidana dengan *definite science* (sistem perumusan ancaman pidana yang bersifat pasti). Pidana penjara merupakan bentuk pidana yang paling sering digunakan oleh hakim untuk mengadili suatu perkara di Indonesia, bahkan hampir semua jenis tindak pidana yang ada terdapat ancaman pidana penjara. Akan tetapi, Muladi berpendapat bahwa akibat dari pidana penjara tersebut dapat menimbulkan prisonisasi, dehumanisasi bahkan dapat menyebabkan stigma buruk bagi mantan narapidana dalam kehidupan masyarakat.⁹³

Dalam peraturan perundang-undangan, tidak dijelaskan secara tegas mengenai subjek hukum yang wajib memenuhi pidana denda terhadap suatu tindak pidana, hal tersebut dapat disimpulkan bahwa pembayaran denda bisa dilakukan oleh orang lain

⁹² P.A.F. Lamintang, 1984, "Hukum Penitensier Indonesia", Armico, Bandung, hlm 69.

⁹³ Widodo, 2009, "Sistem Pidana dalam Cyber Crime", Aswaja, Yogyakarta, hlm 49.

maupun pihak ketiga dari pelaku. Ketika denda yang seharusnya dijatuhkan kepada pelaku agar menimbulkan efek jera tidak sepenuhnya dilakukan oleh pelaku tersebut, maka tujuan pemidanaan denda terhadap pelaku *Phising* dalam putusan ini menjadi kurang maksimal.

Aturan hukum mengenai *Cybercrime* khususnya tindak pidana phising dalam Putusan menurut peraturan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik masih mengalami kekaburan hukum terhadap pengaturannya, hal itu disebabkan *phising* termasuk suatu perbuatan melanggar hukum yang menyebabkan kerugian bagi orang lain. Kerugian yang ditimbulkan dari tindak pidana ini merupakan suatu delik materiil, karena dalam perbuatannya telah merugikan orang lain berupa informasi pribadi yang diketahui oleh pelaku *phising*.

Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Pasal 35 jo. Pasal 51 ayat (1) tidak memuat unsur kebohongan yang merugikan orang lain. Selain melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/ atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik. oleh karena itu pelaku juga dikenakan pasal dalam pasal kitab Undang-undang hukum pidana.

Suatu aturan hukum tidak dapat diterapkan kepada pelaku tindak pidana apabila hukumnya mengalami masih mengalami kekaburan, misalnya dalam Pasal tersebut tidak memiliki konsep pidananya dan penafsiran yang bermacam-macam. Oleh karena

itu, kebijakan hukum harus dilakukan terhadap Undang-Undang Informasi Transaksi dan Elektronik tersebut dengan merumuskan konsep secara khusus mengenai *Phising* dalam putusan ini serta merubah Pasal 35 Undang-Undang Informasi Transaksi dan Elektronik, karena isi Pasal 35 Undang-Undang Informasi Transaksi dan Elektronik untuk saat ini paling mendekati dengan konsep *phising* dalam putusan ini tetapi masih terdapat beberapa unsur yang tidak di rumuskan dalam Pasal tersebut, sehingga Pasal 35 Undang-Undang Informasi Transaksi dan Elektronik masih mengalami kekaburan hukum.⁹⁴

⁹⁴ Ardi Saputra Gulo, 2020, "Cyber Crime dalam bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik", PAMPAS: Journal of Criminal, hlm 78.

BAB IV

KESIMPULAN DAN SARAN

A. KESIMPULAN

Berdasarkan pembahasan diatas, Penulis dapat menarik beberapa kesimpulan sebagai berikut;

1. Aturan yang digunakan untuk menjatuhkan hukuman Terdakwa Tindak Pidana Phising Diatur dalam Undang-Undang yang Mengatur Tentang Tindak Pidana *Phising* Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. belum ada Pasal yang membahas secara khusus. Akan tetapi untuk memperkuat Hasil voni belum ada pasal yang membahas secara khusus tentang tindak pidana phising. Pasal yang dijatuhkan kepada pelaku tindak pidana phising akan menggunakan kesesuaian unsur atau delik yang terdakwa lakukan sehingga dapat menjatuhkan pasal tindak pidana phising untuk tindakan kejahatan pelaku. menggunakan pidana penjara dan denda yang bisa dibidang relatif ringan.
2. Secara yuridis Hakim dalam menjatuhkan vonis terhadap Terdakwa memang sudah sesuai dengan tuntutan Jaksa yaitu dua tahun enam bulan penjara, Namun menurut penulis Hakim belum mempertimbangkan perbarengan tindak pidana yang dilakukan oleh Terdakwa karena dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik Pasal 51 ayat (1) jo. Pasal 35 dengan ancaman maksimal 12 tahun penjara dan /atau denda maksimal 12 milyar rupiah. dalam putusan No.60/Pid.Sus/2022/Pn.Bjr apabila ditinjau dari besarnya kerugian

beserta lamanya terdakwa maulana malik rahman bin karim anshori melakukan tindak pidana (kurang dari 1 tahun) tersebut, dapat dikatakan hukuman yang dijatuhkan kepada terdakwa relative rendah hanya dengan memberikan 2 (dua) Tahun 6 (enam) bulan penjara,

3. Pertanggungjawaban tindak pidana Pada Pelaku *phising* dalam putusan no.60/pid.sus/2022/Pn.bjr oleh terdakwa maulana malik rahman bin karim anshori terbilang ringan yaitu dua tahun enam bulan penjara. yang seharusnya jika dihitung sepertiga dengan penerapan "*Concurcus Realis*" maka seharusnya terdakwa mendapatkan 12 tahun pidana penjara dengan 16 milyar pidana denda. Jika Hukuman diperberat Maka Pelaku akan jera pada perbuatannya dan tidak akan Melakukan Tindak Pidana *Phising* tersebut.

B. SARAN

Berdasarkan dari pengkajian hasil penelitian maka penulis bermaksud memberikan Saran yang mudah-mudahan dapat bermanfaat

1. Penulis menyarankan bahwa harus ada kepastian hukum indonesia dalam menjatuhkan sanksi pidana kepada terdakwa dengan menerapkan jenis pertanggungjawaban pidana kepada terdakwa. Karena sejatinya Tindak Pidana phising adalah kejahatan yang dianggap serius dan kejahatan terorganisasi yang dapat mengakibatkan dampak yang luar biasa terhadap perekonomian negara dan masyarakat karena tindak pidana phising juga merupakan perbuatan yang melawan hukum. Salah satu bentuk kepastian hukum tersebut adalah dengan memastikan undang-undang tindak pidana phising beserta pasalnya yang menentukan

penjatuhan hukumannya sehingga dapat mewujudkan keinginan dan cita-cita masyarakat yakni untuk memberantas tindak pidana phising sampai ke akar-akarnya.

2. Menurut Penulis Meskipun hakim memiliki penilaian tersendiri dalam menentukan jumlah hukuman pidana penjara dan pidana denda akan tetapi jaksa dan hakim juga harus mengikuti ketentuan tindak pidana phising untuk menentukan tuntutan sebagaimana yang telah diatur dalam peraturan perundang-undangan sehingga dalam penuntutan sampai putusan oleh jaksa penuntut umum dan hakim benar-benar adil sesuai konteks keadilan yang sesungguhnya dan sesuai fakta pengadilan dan menjunjung tinggi tujuannya yaitu nilai efektifitas yang sesuai dengan keadilan walaupun jika terdakwa mengakui perbuatannya.
3. penulis menyarankan diperlukannya Pemerintah untuk merumuskan Undang-Undang Informasi dan Transaksi Elektronik beserta Pasal yang menyebutkan Adanya Pasal Untuk menjatuhkan Tindak Pidana Phising dan menentukan hukumannya agar tidak adanya kekeliruan Hukum untuk penulis selanjutnya untuk Meneliti tentang Tindak Pidana Phising di Indonesia sehingga Undang-Undang Tindak Pidana Phising dapat diketahui Oleh Masyarakat ataupun Korban Yang Terkena Tindak Pidana Phising.

DAFTAR PUSTAKA

Buku

- Dikdik M. Arief Mansyur & Elisatris Gultom, 2009, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung , PT Reflika Aditama.
- Gunikhan Sonowal, 2022, *“Phishing and Communication Channels A Guide to identifying and Mitigating Phishing Attack*, Assam, India, Apress, Tinsuka.
- Moeljatno, 2008, *“Asas-Asas Hukum Pidana* , PT. Rineka Cipta, Jakarta.
- C.S.T Kansil dan Christine S.T Kansil, 2007, *Pokok-Pokok Hukum Pidana*, Jakarta, PT. Pradnya Paramitha.
- Wirjono Prodjodikoro, 2008, *Asas-Asas Hukum Pidana Di Indonesia*, Bandung, Refika Aditama.
- Adami Chazawi, 2002, *Pelajaran Hukum Pidana*, Jakarta , PT. Raja Grafindo Persada.
- Erdianto Efendi, 2011, *Hukum Pidana Indonesia*, Bandung, PT. Refika Aditama.
- Lance James, 2006 *“Phishing Exposed” Syngress Publishing, Inc, United States of America*
- Adami Chazawi, 2006, *Tindak Pidana Informasi dan Transaksi Elektronik*, Malang, Media Nusa Creative.
- F. E. Purwiantono, 2017, *“Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia*.
- Efvy Zam, 2014, *Phising Cara Mudah Menyadap Password & Pencegahannya*, Jakarta Selatan, PT. Trans Media.
- Febry Eka Purwiantono, 2017, *“Model Klasifikasi Untuk Deteksi Situs Phising Indonesia”*, Surabaya.
- Tim Rains, 2020 *“Cybersecurity Threats, Malware Trends, and Strategies (Mitigate exploits,malware, phising, and other socil engineering attacks)”*, Birmigham, UK, Packt Publishing Ltd, Livery Place 35.
- Sutan Remy Syahdeini, 2009, *Kejahatan & Tindak Pidana Komputer*, Jakarta, PT. Pustaka Utama Grafiti.

- Oluwatobi Ayodeji Akanbi, dkk, 2015, “*A Machine Learning Approach to Phishing Detection and Defense*”, USA, Syngress Is an imprint of Elsevier 255, Wymna Street, Waltham.
- Soerjono Soekanto dan Sri Mamudji, 2009, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Jakarta, PT Raja Grafindo Persada.
- Riduwan 2010, *Metode dan Teknik Menyusun Proposal Penelitian*, Bandung, Alfabeta
- Hardani, S.Pd.,M.Si.,dkk, 2020, *Metode Penelitian Kualitatif dan Kuantitatif*, Yogyakarta, Penerbit: CV.Pustaka Ilmu.
- Julyano, M., & Sulistyawan, A. Y, 2019, *Pemahaman terhadap asas kepastian hukum melalui konstruksi penalaran positivisme hukum*. Crepido.
- Josua Sitompul, 2012, *Cyberspace, Cybercrime, Cyberlaw, Tinjauan Aspek Hukum Pidana*, Jakarta, PT Tatanusa.
- Barda Nawawi Arief, 1998, *Beberapa Aspek Kebijakan Penegakan Dan Pengembangan Hukum Pidana*, Bandung, Citra aditya bakti.
- Mulyadi, Lilik. 2012, *Hukum Acara Pidana: Normatif, Teoritis, Praktik dan Permasalahannya*. Bandung, Alumni.
- Muhammad Syukri Albani Nasution, 2017, *Hukum dalam Pendekatan Filsafat*, Jakarta, Kencana.
- Shinta Agustina, 2010, “*Implementasi Asas Lex Specialis Derogat Legi Generali Dalam Sistem Peradilan Pidana*”.
- Teguh Prasetyo, 2013, *Hukum Pidana*, Jakarta, PT. Raja Grafindo Persada.
- P.A.F. Lamintang, 1984, “*Hukum Penitensier Indonesia*”, Bandung, Armico.
- Widodo, 2009, “*Sistem Pidana dalam Cyber Crime*”, Yogyakarta, Aswaja.
- Andi Hamzah, 2015, *Delik-Delik Tertentu (Speciale Delicten) Di dalam KUHP Edisi Kedua*, Jakarta, Sinar Grafika.
- H.M. Rasyid Ariman dan Fahmi Raghieb, 2015, *Hukum Pidana*, Malang, Setara Press.

Jurnal Ilmiah

United State Cyber Security Laws and Regulation

Ferry Irawan Febriansyah. "Model Kejahataan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional" *Jurnal Ilmu Hukum* , Vol.7 No. 2, 2023.

Mila haryati wibowo, Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime" Vol.1, Nomor 1, Tahun 2017

Sahuri Lasmadi, "Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya," *Jurnal Ilmu Hukum*, 2014.

Purnamasari, Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-Hari, *Jurnal Digital Teknologi Informasi*, 2023, Vol. 6 No.1.

MOHD. Yusuf DM, Addermi, dan Jasmine Lim, "Kejahatan Phising dalam dunia Cyber Crime dan Sistem Hukum di Indonesia", *Jurnal Pendidikan dan Konseling*, Vol 4, No. 5, Tahun 2022.

A. S. Gulo, S. Lasmadi, dan K. Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," *PAMPAS J. Criminal Law*, vol. 1, no. 2, April 2021.

Malahayati dan Darul Fata, "Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit melalui Teknik Phising", *Djtechno: Journal of Information Technology Research*, Vol 2, No. 1, Juli, Tahun 2021.

Anggun Juniamalia Sholikhah dan Aryo Fadlian, "Perspektif Undang-Undang tentang Informasi dan Transaksi Elektronik Terhadap Cyber Crime dalam bentuk Phising", Vol 3, No.1, Tahun 2023.

Malahayati dan Darul Fata, "Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit melalui Teknik Phising", *Djtechno: Journal of Information Technology Research*, Vol 2, No. 1, Juli, Tahun 2021.

Irma Yurita, M. Kevin Ramadhan dan M. Candra, "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cyber Crime", *Jurnal Hukum, Legalita* Vol 5, No. 2, Desember 2023.

Hardijan Rusli, "Metode Penelitian Hukum Normatif: Bagaimana?", *Law Review*

- Fakultas Hukum Universitas Pelita Harapan, Volume V No. 3 Tahun 2006,.
- Septian Arya Budi Mahesa, Hervina Puspitosari, "Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam Penanganan Perkara Tindak Pidana Phising", Jurnal Penelitian dan pengabdian masyarakat, Volume 2 No. 11, Maret 2023.
- Suhardi Rustam, "Analisa Clustering Phising dengan K-Means dalam Meningkatkan Keamanan Komputer, "Ilkom Jurnal Ilmiah, Vol. 10 No. 2, 2018.
- Widiatama Widiatama, Hadi Mahmud, and Suparwi Suparwi, "Ideologi Pancasila Sebagai Dasar Membangun Negara Hukum Indonesia," Jurnal Usm Law Review 3, no. 2, 2020..
- Syarifah Dewi Indawati. "Dasar Pertimbangan Hukum Hakim Menjatuhkan Putusan Lepas dari Segala Tuntutan Hukum Terdakwa dalam Perkara Penipuan, Jurnal Verstek 5, Nomor 2, 2015,
- "Kajian Yuridis Terhadap Pertanggungjawaban Tindak Pidana Informasi Dan Transaksi Elektronik (ITE)" Vidya Wertta 6, No.1, 2023.
- Muhammad Kamran and Maskun Maskun, "Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika," Balobe Law Journal 1, no. 1, 2021,
- Septian Arya Budi Mahesa, Hervina Puspitosari, "Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam Penanganan Perkara Tindak Pidana Phising",Jurnal Penelitian dan Pengabdian Masyarakat, Vol. 2 (11) Maret 2023.
- Faiz Emery Muhammad, Beniharmoni Harefa "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phising Berbasis Web", Jurnal USM Law Review Vol 6 No 1 Tahun 2023.
- Septa Candra. "Pembaharuan Hukum Pidana; Konsep Pertanggungjawaban Pidana Dalam Hukum Pidana Nasional Yang Akan Datang" Jurnal Cita Hukum I No. 1, 2013.
- Mia Haryati Wibowo, Nur Fatimah, Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia *Cybercrime*, JOEICT (Jurnal of Education and

Information Communication Technology) Volume 1, Nomor 1, 2017

Peraturan Perundang-undangan

Pasal 51 Ayat (1) Jo Pasal 35 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagaimana diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasal 378 kitab Undang-Undang Hukum Pidana (KUHP) serta pasal-pasal dalam Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP)

Pasal 378 Kitab Undang-Undang Hukum Pidana Atas Perubahan Undang-Undang Nomor 1 Tahun 2023 Pasal 492 Kitab Undang-Undang Hukum Pidana Tentang Penipuan.

Undang-undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.

Pasal 28 ayat (1) jo Pasal 45A ayat (1) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagaimana diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Internet

Faradilla A, “apa itu phishing”, hostinger website digital, 2023

Kamus Hukum Online, “Pengertian Analisis Yuridis

Laporan Aktivitas Abuse Domain.Id Indonesia Anti-*Phishing* Data Exchange Periode Q2 2024 April-Juni 2024
https://api.idadx.id/documents/uploads/1724725529_Laporan%20Q2%202024.pdf.pdf

