TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUNIA MAYA BERMODUS PENGELABUAN (*Phising*) DALAM BENTUK MENGIRIMKAN LINK

SKRIPSI
Diajukan Untuk Memenuhi Syarat
Mendapatkan Gelar Sarjana Hukum

Oleh :

Dinda Aulia
1906200378

FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2023

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 1913/SK/BAN-PT/Ak.KP/PT/XI/2022
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@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 1

Panitia Ujian Sarjana Strata-I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Kamis, tanggal 31 Agustus 2023, Jam 08.30 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan, menimbang:

MENETAPKAN

NAMA	**:**	**DINDA AULIA**
NPM	**:**	**1906200378**
PRODI/BAGIAN	**:**	**HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI	**:**	**TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUNIA MAYA BERMODUS PENGELABUAN (PHISING) DALAM BENTUK MENGIRIMKAN LINK**

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**
Dr. FAISAL, S.H., M.Hum.	**Dr. ZAINUDDIN, S.H., M.H.**
NIDN: 0122087502	**NIDN: 0118047901**

ANGGOTA PENGUJI:

1. **NURHILMIYAH, S.H., M.H.** — 1. _____
2. **Dr. TEGUH SYUHADA LUBIS, S.H., M.H.** — 2. _____
3. **Dr. FAISAL, S.H., M.Hum.** — 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. 1913/SK/BAN-PT/Ak.KP/PT/XI/2022
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Fakulas Hukum Universitas Muhammadiyah Sumatera Utara Strata I bagi:

NAMA	**:**	**DINDA AULIA**
NPM	**:**	**1906200378**
PRODI/BAGIAN	**:**	**HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI	**:**	**TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUNIA MAYA BERMODUS PENGELABUAN (PHISING) DALAM BENTUK MENGIRIMKAN LINK**
PENDAFTARAN	**:**	**Tanggal 29 Agustus 2023**

Dengan diterimanya skripsi ini, sesudah lulus dari Ujian Komprehensif, penulis berhak memakai gelar:

SARJANA HUKUM (S.H.)

Diketahui
Dekan Fakultas Hukum

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

Pembimbing

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

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 1913/SK/BAN-PT/Ak.KP/PT/XI/2022
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA	:	**DINDA AULIA**
NPM	:	**1906200378**
PRODI/BAGIAN	:	**HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI	:	**TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUINIA MAYA BERMODUS PENGELABUAN (*Phising*) DALAM BENTUK PENGIRIMAN LINK**

Disetujui Untuk Disampaikan Kepada
Panitia Ujian Skripsi

Medan, 28 Agustus 2023

Pembimbing

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

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

KARTU BIMBINGAN SKRIPSI MAHASISWA

NAMA : DINDA AULIA
NPM : 1906200378
PRODI/BAGIAN : ILMU HUKUM/ HUKUM PIDANA
JUDUL SKRIPSI : TINJAUAN KRIMONOLOGI MENGENAI KEJAHATAN DUNIA MAYA BERMODUS PENGELABUHAN (*PHISING*) DALAM BENTUK MENGIRIMKAN LINK

PEMBIMBING : Dr. FAISAL, S.H., M.Hum.

TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
24-1-22	Konsultasi Judul	
03-1-23	Proposal.	
02-2-23	Seminar Proposal.	
27-6-23	Bimbingan skripsi I	
24-7-23	Lokasi Belitung, RM. Steak Bank	
11-8-23	Cara penulisan Kutipan, Bab II	
16-8-23	Outline Secara dgn Sistematika	
21-8-23	Abstrak, Daftar Pustaka	
24-8-23	Acc di perbanyak untuk di ujikan	

Diketahui
DEKAN FAKULTAS HUKUM

(Dr. FAISAL, S.H., M.Hum.)

DOSEN PEMBIMBING

(Dr. FAISAL, S.H., M.Hum.)

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertandatangan di bawah ini :

Nama	:	**DINDA AULIA**
NPM	:	**1906200378**
Fakultas	:	**HUKUM**
Program Studi	:	**HUKUM**
Bagian	:	**HUKUM PIDANA**
Judul Skripsi	:	**TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUNIA MAYA BERMODUS PENGELABUAN (PHISING) DALAM BENTUK PENGIRIMAN LINK**

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, Agustus 2023
Saya yang menyatakan,

DINDA AULIA
NPM. 1906200378

ABSTRAK

TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUNIA MAYA BERMODUS PENGELABUAN (*Phising*) DALAM BENTUK MENGIRIMKAN LINK

DINDA AULIA
NPM: 1906200378

Teknologi informasi mampu mengubah realitas ekonomi, budaya, politik dan hukum. Seiring berkembangnya teknologi informasi mampu memberikan dampak positif bagi banyak orang namun hal ini juga menyebabkan munculnya kejahatan-kejahatan baru yang disebut dengan kejahatan dunia maya baru melalui jaringan internet. Dimana terdapat beberapa orang yang memanfaatkan celah keamanan pada teknologi informasi pada jaringan internet sebagai sarana untuk melakukan kejahatan yang selanjutnya dikenal dengan *cybercrime*, dimana salah satunya adalah *phising*. Phising biasanya dilakukan melalui media social yang terhubung dengan internet seperti melalui email atau SMS dan website, pengetahuan pengguna yang minim tentang alat teknologi informasi yang digunakan adalah yang mendorong terjadinya *phising*.

Penelitian ini adalah penelitian yuridis normatif, menggunakan data sekunder serta data yang bersumber dari Al-Qur'an dan Hadist. Kemudian alat pengumpulan data yaitu : studi kepustakaan

Berdasarkan hasil penelitian diketahui modus kejahatan pengelabuan (*phising*) dalam bentuk mengirimkan suatu link pengguna akan di bawa ke situs *web* berbahaya yang telah dimodifikasi oleh pelaku , phising juga dapat terjadi di berbagai platform, termasuk media sosial, situs *web* dan juga aplikasi lainnya. Faktor-faktor terjadinya kejahatan yaitu kurangnya pengetahuan dan kesadaran pengguna terhadap ancaman serangan *phising* mengenai pengetahuan pengguna untuk mengidentifikasi *website* palsu yang meenyerupai aslinya sangat minim, sehingga pengguna tidak menyadari bahwa telah menggunakan situs palsu. Upaya pencegahan kejahatan perlu ditempuh dengan pendekatan kebijakan secara terpadu (integral), dimana terdapat keterpaduan antara kebijakan kriminal dengan kebijakan sosial juga pencegahannya dengan cara penal dan non penal.

Kata kunci : *Kriminologi, Dunia Maya, Pengelabuan (Phising)*

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Pertama-tama disampaikan rasa syukur kehadirat Allah SWT yang maha pengasih lagi maha penyayang atas segala rahmat dan karuniaNya sehingga skripsi ini dapat diselesaikan. Skripsi merupakan salah satu persyaratan bagi setiap mahasiswa yang ingin menyelesaikan studinya di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Sehubungan dengan itu, disusun skripsi yang berjudulkan. **TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUNIA MAYA BERMODUS PENGELABUAN (*PHISING*) DALAM MENGIRIMKAN SUATU LINK.**

Dengan selesainya skripsi ini, perkenankanlah diucapkan terimakasih yang sebesar-besarnya kepada: Rektor Universitas Muhammadiyah Sumatera Utara Bapak Prof. Dr. Agussani., M.AP atas kesempatan dan fasilitas yang diberikan kepada kami untuk mengikuti dan menyelesaikan pendidikan program sarjana ini. Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Bapak Dr. Faisal, S.H., M.Hum atas kesempatan menjadi mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Demikian juga halnya kepada Wakil Dekan I Bapak Dr. Zainuddin, S.H., M.H dan Wakil Dekan IIII bu Atikah Rahmi ,S.H.,M.H. Terimakasih yang tak terhingga dan penghargaan yang setinggi-tingginya diucapkan kepada Bapak Dr. Faisal, S.H., M.Hum selaku Pembimbing, yang dengan penuh perhatian telah memberikan dorongan, bimbingan dan arahan sehingga skripsi ini selesai.

Secara khusus dengan rasa hormat serta penghargaan yang setinggi-tingginya penulis ucapkan kepada Ayahanda tercinta Darma Yulis dan Ibunda

tercinta Elviana selaku orang tua penulis yang telah mengasuh dan mendidik penulis dengan curahan kasih sayang. Terima kasih atas doa yang yang tulus tiada henti, motivasi dan cinta yang diberikan. Juga kepada Dani, Dini, Ari selaku Abang, Adik-Adik Kandung Penulis, Terima kasih atas doa yang yang tulus tiada henti, motivasi dan cinta yang diberikan. Serta keluarga penulis lainnya yang tidak dapat diutarakan satu persatu yang sedikit banyaknya telah berperan dalam mendukung penulis untuk menyelesaikan penulisan skripsi ini. Disampaikan juga penghargaan kepada seluruh staf pengajar Fakultas Hukum Universitas Muhammadiyah Sumatera Utara (UMSU).

Tiada hal yang paling indah kecuali persahabatan, untuk itu, dalam kesempatan diucapkan terimakasih kepada sahabat-sahabat penulis yang telah banyak berperan, terutama Kak Devi Marlinda Purba, S.H., yang sudah menjadi teman diskusi selama pengerjaan skripsi penulis. Kepada teman-teman seperjuangan dalam menyelesaikan tugas akhir terkhusus Alfina Yulistari Siagian, Sopiah Wardani, Alya Putri, Stefani Auji Tan, dan Iva Fidiawati serta teman-teman seperjuangan di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara yang tidak dapat penulis sebutkan satu persatu, dan terima kasih kepada teman dekat penulis terkhusunya Fernanda Rafiyanto yang telah menemani saya selama saya mengerjakan skripsi yang selalu mendukung penulis untuk mengerjakan skripsi ini.

Terima kasih atas semua kebaikannya semoga Allah SWT membalas kebaikan kalian semua. Akhirnya, tiada gading yang tak retak, retaknya gading karena. alami, tiada orang yang tak bersalah, kecuali Ilahi Robbi. Mohon maaf atas segala kesalahan selama ini, begitupun di dasari bahwa skripsi ini jauh dari

sempurna Untuk itu, diharapkan ada masukan yang membangun untuk kesempurnaannya. Terimakasih semua, tiada lain yang diucapkan selain kata semoga kiranya mendapat balasan dari Allah SWT dan mudah-mudahan semuanya selalu dalam lindungan Allah SWT, Amin. Sesungguhnya Allah mengetahui akan niat baik hamba-hambanya.

Assalamu'alaikum Warahmatullahi Wabarakatuh

Medan, Agustus 2023

Hormat saya,
Penulis

Dinda Aulia
NPM: 1906200378

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Bekakang

Indonesia adalah negara hukum, semua tingkah laku manusia sebagai subyek hukum diatur oleh hukum. Hukum sebagai sarana dalam perubahan masyarakat kearah yang lebih baik, hukum berperan meluruskan keadaan yang sebelumnya rusak menjadi lebih baik lagi. Sifat manusia sebagai subyek hukum memang banyak melakukan kesalahan akan tetapi dengan adanya hukum maka manusia dituntun dengan paksa kearah yang lebih baik lagi. Sebagai subyek 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. [1]

Teknologi informasi mampu mengubah realitas ekonomi, budaya, politik dan hukum. Seiring berkembangnya teknologi informasi mampu memberikan dampak positif bagi banyak orang namun hal ini juga menyebabkan munculnya kejahatan-kejahatan baru yang disebut dengan kejahatan dunia maya baru melalui jaringan internet. Dimana terdapat beberapa orang yang memanfaatkan celah keamanan pada teknologi informasi pada jaringan internet sebagai sarana untuk melakukan kejahatan yang selanjutnya dikenal dengan *cybercrime*.[2] *Cybercrime*

[1] Ferry Irawan Febriansyah. "Model Kejahataan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional" Jurnal Ilmu Hukum , Vol.7 No. 2 , 2023 , Halaman 183.

[2] Kadek Odie Kharisma Putra. "*Tindakan Kejahatan Pada Dunia Dalam BentukP hising*" Jurnal *cybersccurity* dan Forensik Digital, Vol. 5 No 2, 2022, halaman 77

adalah nama lain dari kejahatan di dunia maya. *Cybercrime* umumnya di definisikan sebagai aktivitas ilegal yang melibatkan komputer perangkat digital lainnya atau jaringan komputer. Contoh kejahatan dunia maya termasuk ancaman keamanan dunia maya seperti rekayasa sosial, eksploitasi kerentanan perangkat lunak dan serangan jaringan.[3] *Cybercrime* merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan jaringan komputer atau internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi untuk memperoleh keuntungan dengan merugikan pihak lain. *Cybercrime* adalah kegiatan kriminal di dunia maya yang menggunakan jaringan komputer sebagai alatnya dan internet sebagai medianya dalam arti yang lebih luas, kejahatan dunia maya adalah aktivitas ilegal yang terjadi di jaringan komputer atau internet untuk menghasilkan keuntungan dengan mengorbankan orang lain. Selanjutnya, *cybercrime* yang di definisikan secara sempit adalah aktivitas ilegal yang ditujukan untuk menyerang sistem keamanan komputer dan data yang diproses oleh sistem komputer.[4]

Perkembangan teknologi dan informasi di Indonesia semakin tahun semakin cepat. Hampir Sebagian besar penduduk Indonesia saat ini telah melek teknologi dan menggunakan jaringan internet sebagai sarana untuk berkomunikasi, hanya sedikit masyarakat Indonesia yang belum bisa menggunakan jaringan internet. Berbagai kejahatan telah terjadi di dunia maya ini, kasus-kasus tersebut tentu saja merugikan dan berdampak negatif, kejahatan dunia maya semacam ini

[3] Ferry Irawan Febriansyah , *Op.cit*., Halaman 185.

[4] Mohd. Yusuf DM. "Kejahatan *Phising* dalam Dunia *Cyber crime* dan *system* hukum di Indonesia*"* Jurnal pendidikan dan konseling , Vol. 4 No 5 , 2022 halaman 8019.

tidak hanya mencakup Indonesia tetapi juga mencakup seluruh dunia. Jaringan internet tidak hanya memberikan dampak positif yang diantaranya sebagai sarana komunikasi orang yang sedang tidak berada ditempat dengan kita namun juga tentunya memberikan dampak negatif bagi penggunanya. Dampak negatifnya diantaranya masyarakat dapat kecanduan bermain internet dan sosial media hingga melupakan kewajibannya dapat berpotensi menyebarkan ujaran kebencian ataupun *hoax* kepada pengguna jaringan internet lainnya hingga dapat berpotensi adanya kejahatan dunia maya seperti *phising*.[5]

Berbicara mengenai kejahatan, merupakan bagian dari sifat buruk manusia yang memberikan kesusahan bagi orang lain. Kejahatan menimbulkan kerugian baik moril maupun materiil kepada orang lain yang disebabkan karena keinginan manusia yang besar untuk membuat dirinya bahagia dengan menyakiti orang. Seiring dengan perkembangan teknologi, kejahatan manusia tidak hanya dilakukan di dunia nyata saja, melainkan dilakukan di dunia maya atau biasa disebut dengan *Cybercrime*. Namun tidak dapat dipungkiri bahwa disisi lain perkembangan teknologi yang begitu pesat dapat memebrikan dampak yang begitu besar pula, yang dimana dapat menyebabkan munculnya berbagai macam kejahatan yang biasa disebut dengan *cybercrime*. Munculnya Internet sebagai media komunikasi baru dikaitkan dengan klaim yang saling bertentangan tentang munculnya pola-pola baru interaksi sosial.[6]

[5] Ferry Irawan Febriansyah , *Op.cit*., Halaman 187.
[6] *Ibid.,* Halaman 184.

Phising adalah jenis penipuan dunia maya yang bertujuan mencuri akun korban. Tentu saja, sebagian besar kejahatan dunia maya biasanya dimulai dengan phising sehingga pengguna internet harus selalu waspada. *Phising* juga biasanya menyasar pengguna *online banking* karena pengguna data pengguna dan kata sandi tidak menutupkan kemungkinan dialihkan ke pengguna *online* lainnya. Saat pengguna memasukkan kredensial pengguna dan kata sandi mereka kedalam formulir login yang merupakan formulir login palsu, penjahat dunia maya dapat mengetahuinya dalam bentuk *phising*.[7]

Phising biasanya dilakukan melalui media sosial yang terhubung dengan internet seperti melalui email atau SMS dan *website*. Penipuan dilakukan dengan mengelaburasi target dengan maksud untuk mencuri akun target yang biasanya meminta password akun. Disini yang berperan menyamar menggunakan forum login atau situs palsu untuk memancing memasukan data-data milik korban seperti *user id* dan password tersebut. Pengetahuan pengguna yang minim tentang alat teknologi informasi yang digunakan adalah yang mendorong *phising*.

Phising dapat terjadi di berbagai *platform*, termasuk media sosial, situs *web* dan juga aplikasi. Hal ini pun dimanfaatkan oleh orang tidak bertanggung jawab dan menggunaka\n nya untuk kejahatan. Pada pengguna aplikasi, penjahat mencoba mengirimkan pesan ke nomor tertentu. Pesan ini mungkin berisi tentang informasi bahwa nomor ini telah dipilih sebagai pemenang dan ketika pengguna menekan link tersebut, mereka diminta untuk menginformasikan melalui link tersebut.

[7] Kadek Odie Kharisma Putra , *Op.cit.,* Halaman 78.

Pengguna akan dibawa kesitus web berbahaya yang telah di modifikasi oleh pelaku. Mirip dengan aplikasi *WhatApp* ataupun *Instagram* yang dimana Tindakan kriminal ini dapat dilakukan melalui pesan langsung dan komentar pada postingan dimana salah satu pengguna akan memposting foto atau video yang berisi informasi tentang insiden yang menarik bagi pengguna lain. Jadi pengguna yang lain akan dibuat penasaran mengenai informasi lengkap dari postingan tersebut sehingga pengguna yang lain akan mengirimkan sebuah link dimana pengguna tersebut meyakinkan bahwa kita akan mendapatkan informasi lengkap dari postingan yang telah dibuat sehingga pengguna yang lainnya akan mencoba mengirimkan sebuah link dan meyakinkan pengguna lainnya untuk menekan link tersebut dikarena kan pada link tersebut terdapat informasi lengkap mengenai apa yang dijelaskan pada postingan tersebut. Padahal link tersebut bisa saja terdapat virus atau pengguna akan dibawa kesitus berbahaya yang dapat mengancam keamanan pengguna yang mengakses.

Kejahatan bisa terjadi di mana saja bahkan di dunia maya. Jadi pengguna harus selalu waspada dalam menggunakan internet karena masih banyak orang yang belum memiliki pengetahuan yang cukup untuk mengakses internet dan oknum-oknum yang tidak bertanggung jawab mencoba memanfaatkan orang-orang tersebut.[8] Ketidaktahuan pengguna mengenai hal-hal yang ada di internet yang membuat pengguna terjerumus dalam korban tindakan kejahatan dunia maya. Oleh karena itu, saat bertukar pesan dengan orang asing atau mendapatkan informasi yang dikirim oleh orang lain pengguna harus selalu waspada dan memastikan

[8] *Ibid.,* Halaman 78.

bahwa pengguna dapat memverifikasi keakuratan informasi yang diberikan. Pengguna harus selalu memastikan bahwa informasi yang dikirimkan oleh orang lain benar atau tidak melalui situs-situs resmi dan juga jangan mudah percaya apabila menerima informasi bahwa pengguna memenangkan suatu hadiah dan orang tersebut mengirimkan sebuah link karena bisa saja link tersebut terdapat hal-hal yang berbahaya yang dapat mengancam keselamatan perangkat dan pengguna.[9]

Kejahatan *pishing* ini biasanya dapat menyerang korban melalui email, media sosial, panggilan telepon, dan sms dengan mengatas namakan perusahaan untuk memperoleh data pribadi.

Cybercrime dalam bentuk pishing saat ini di Indonesia dimungkinkan dapat dikenakan Pasal 35 jo Pasal 51 ayat (1) Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik karena pishing merupakan kejahatan siber yang membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu.

Cybercrime dalam bentuk *pishing* ini juga dapat dikenakan Pasal 28 ayat (1) jo Pasal 45A ayat (1) Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik 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 memperbarui informasi pribadinya yang rahasia ke dalam situs palsu yang telah dibuat oleh pelaku *phising* sehingga informasi

[9] *Ibid.,* Halaman 78.

pribadinya yang rahasia tersebut diketahui oleh pelaku *phising* dan menyebabkan orang tersebut mengalami kerugian.[10]

Undang-Undang Nomor 19 tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini selain membuat aturan tentang pishing, Undang-Undang ini juga membuat aturan terhadap perbuatan-perbuatan kejahatan yang merugikan orang lain yang membuat aturan terhadap perbuatan-perbuatan kejahatan yang merugikan orang lain yang terjadi di dunia maya melalui transaksi elektronik yang dapat diketahui bahwa perkembangan teknologi informasi semakin pesat.[11]

Phishing termasuk dalam kejahatan siber dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan cari paling mudah untuk di jadikan serangan, meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang *hacker*.

Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan hingga kini banyak sekali akun sosial media yang sudah terjebak dalam *phishing*. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh fake link pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan. Dengan hal tersebut penyerang dapat mengambil

[10] Ardi Saputra Gulo, Dkk , Cyber Cyber Dalam Bentuk Phising Berdasarkan Undang Informasi Dan Transaksi Elektronik, Journal of criminal , Vol. 1 No. 2 ,2020 , Halaman 72.

[11] Ardi Saputra Gulo, *Op.cit.*, Halaman 73.

informasi pengguna dan menggunakannya untuk mencari keuntungan misalnya untuk mengambil uang dari rekening pengguna atau menggunakan rekening untuk pembayaran *online*.

Tindak pidana *phising* merupakan kejahatan penipuan. Pengaturan mengenai tindak pidana *cybercrime phising* diatur dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[12]

Pada kasus yang peneliti amati yakni kasus Bareskrim Polri menangkap 13 tersangka terkait kasus penipuan berkedok modifikasi APK dan link *phising* dengan total kerugian Rp 12 miliar, korban penipuan ini mencapai 439 orang. Para tersangka yang ditangkap mempunyai peran berbeda mulai dari pengembang *package* KIT, mengumpulkan database korban, menguras rekening korban hingga melakukan penarikan dana pada rekening korban. Pembuat aplikasi diancam penjara paling lama 8 tahun dan denda paling banyak 800 juta rupiah. Tersangka lainnya diancam hukuman 20 tahun penjara. Polri mengimbau agar masyarakat lebh bijak menginstal aplikasi dan waspada memberikan nomor telepon pribadi pada pihak tak dikenal.[13] Berdasarkan latar belakang di atas, maka penyusun tertarik untuk meneliti masalah kejahata dunia maya atau *cybercrime* ini dengan judul **"TINJAUAN KRIMINOLOGI MENGENAI KEJAHATAN DUNIA MAYA**

[12] Nur Fatimah. "Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime" Jurnal *of Education And Information Communication Technology*, Vol. 1 No. 1,2017 , Halaman 2.

[13] Kompas TV, "Bareskrim Tangkap 13 Tersangka Penipuan Modifikasi APK dan Link Phising" https://www.kompas.tv/video/369886/bareskrim-tangkap-13-tersangka-penipuan modifikasi-apk-dan-link-phishing, diakses pada tanggal 20 Juli 2023 Pukul 20.26 WIB.

BERMODUS PENGELABUAN (PHISING) DALAM BENTUK MENGIRIMKAN SUATU LINK"

1. Rumusan Masalah

Berdasarkan uraian diatas dapat di tarik beberapa permasalahan yang akan menjadi batasan pembahasan dari penelitian ini nantinya, adapun permasalahannya yaitu :

a. Bagaimana modus kejahatan pengelabuan (*phising*) dalam bentuk mengirimkan suatu link ?
b. Apakah Faktor-faktor penyebab terjadinya kejahatan dunia maya bermodus pengelabuan (*phising*) dalam bentuk mengirimkan suatu link ?
c. Bagaimana pencegahan kejahatan pengelabuan (*phising*) dalam bentuk mengirimkan suatu link ?

2. Faedah Penelitian

Penelitian ini diharapkan dapat memberikan manfaat secara teoritis dan praktis yaitu:

a. Secara teoritis, dengan adanya penelitian ini diharapkan dapat memperoleh pengetahuan mengenai dasar, sumber, dan tinjauan kriminologi mengenai kejahatan dunia maya bermodus pengelabuan (*phising*) dalam mengirimkan suatu link yang dijelaskan dengan pemikiran-pemikiran secara teoritis yang diharapkan sekurang-kurangnya dapat menjadi referensi ilmiah/sumbangan pemikiran yang bermamfaat dalam perkembangan ilmu hukum serta sebagai sumbangan pemikiran dalam dunia pendidikan.

b. Secara praktis, hasil penelitian ini diharapkan dapat menjadi masukan bagi pihak-pihak yang terkait termasuk bagi kepentingan negara, bangsa, masyarakat dan para praktisi hukum menambah literatur yang membahas tentang kejahatan dunia maya bermodus pengelabuan (*phising*) dengan mengirimkan suatu link.

B. Tujuan Penelitian

Tujuan Penelitian ini adalah sebagai berikut :

1. Untuk mengetahui modus-modus kejahatan pengelabuan (*phising*) dalam bentuk mengirimkan suatu link.
2. Untuk mengetahui faktor-faktor yang menjadi penyebab terjadinya kejahatan dunia maya bermodus pengelabuan (*Phising*) dalam bentuk mengirimkan suatu link.
3. Untuk mengetahui bagaimana pencegahan terhadap kejahatan dunia maya bermodus pengelabuan (*Phising*) dalam bentuk mengirimkan suatu link.

C. Definisi Operasional

Definisi operasional atau kerangka konsep adalah kerangka yang menggambarkan hubungan antara definisi-definisi atau konsep-konsep khusus yang akan diteliti.[14] Konsep merupakan salah satu unsur konkrit dan teori. Sesuai dengan judul penelitian yang akan diajukan yaitu : **"Tinjauan Kriminologi Mengenai Kejahatan Dunia Maya Bermodus Pengelabuan (*Phising*) Dalam**

[14] Ida Hanifah dkk, 2018. *Pedoman Penulisan Tugas Akhir Mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara (UMSU),* Medan : Pustaka Prima, halaman 17.

Bentuk Mengirimkan Suatu Link" maka dapat dijelaskan definisi operasional penelitian, yaitu :

1. Kriminologi adalah ilmu pengetahuan yang mmepelajari atau mencari sebab musabab kejahatan, sebab-sebab terjadinya kejahatan, akibat-akibat yang ditimbulkan dari kejahatan untuk menjawab penyebab seseorang melakukan kejahatan.[15] Dalam hal ini yang dimaksud dengan tinjauan kriminologi adalah perbuatan kejahatan yang dilakukan didalam kejahatan yang mengirimkan suatu link yang berbahaya.
2. *Cybercrime* (kejahatan dunia maya) adalah kejahatan digital yang dilakukan untuk menuai keuntungan melalui internet sebagai media, setiap aktivitas kriminal yang terjadi di dunia digital atau melalui jaringan internet disebut sebagai kejahatan internet, *Cybercrime* juga mengacu pada aktivitas kriminal pada computer dan jaringan. Kejahatan dunia maya (*cybercrime*) muncul seiring dengan perkembangan teknologi digital, komunikasi dan informasi yang berkembang begitu pesat. Kejahatan siber yang sudah sering terdengar di kalangan masyarakat.[16]
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 lamgsung memberikan semua informasi yang dibutuhkan oleh penjebak.[17] Disini

[15] Nursariani Simatupang & Faisal, 2017, *Kriminologi* Medan:CV. Pusaka Prima , Halaman 3.

[16] Andysah Putera Utama Siahaan, Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia, Jurnal Ilmiah, Vol. 5 No. 1 , 2018, Halaman 1.

[17] M. Yusuf DM dkk, "*Analisis terhadap modus-modus dalam hukum cybercrime"* Jurnal Hukum, Politik dan Ilmu Sosial, 2022, Vol. 2 No. 2, halaman 2.

dapat disimpulkan bahwa *phising* ialah kejahatan pengelabuan yang dilakukan pelaku terhadap seseorang dalam mengirimkan suatu link yang berbahaya.

D. Keaslian Penelitian

Kejahatan dalam dunia maya *cybercrime* bermodus pengelabuan (*phising*) dalam mengirimkan suatu link berbahaya. Bukan suatu hal yang baru dibahas. Oleh karena nya, penulis meyakini telah banyak peneliti-peneliti sebelumnya yang mengangkat tentang Tinjauan Kriminologi Mengenai Kejahatan Dunia Maya Bermodus Pengelabuan (*phising*) dalam mengirimkan suatu link. Sebagai tajuk dalam berbagai penelitian. Namun berdasarkan bahan kepustakaan dari lingkungan Universitas Muhammadiyah Sumatera Utara dan penguruan tinggi lainnya. Penulis tidak menemukan penelitian yang sama dengan tema dan pokok bahasan yang penulis teliti terkait : **"Tinjauan Kriminologi Mengenai Kejahatan Dunia Maya Bermodus Pengelabuan (*Phising*) Dalam Mengirimkan suatu link".** Beberapa judul penelitian yang pernah dibahas dan dikaji oleh peneliti sebelumnya, ada satu judul yang hampir mendekati dengan penelitian yang akan penulis teliti ini antara lain :

1. Skripsi HILMAN MURSIDI, NIM 02011381419348 Mahasiswa Fakultas Hukum Univerita Sriwijaya Tahun 2019 yang berjudul "PertanggungJawaban Pidana Terhadap Pelaku Tindak Pidana *Cybercrime Phising* (Studi Kasus Putusan Pengadilan Negeri Medan Nomor : 3006/Pid.Sus/2017/PN.Mdn)" Skripsi ini merupakan penelitian yang

menggunakan pendekatan perundang-undangan yang lebih menekankan terhadap pertanggungjawaban dari tindak pidana cybercrime phising.

2. Skripsi ADHI DHARMA ARRYAGUNA, NIM B 111 12 358 Mahasiswa Fakultas Hukum Unversitas Hasanuddin Makassar Tahun 2017 yang berjudul "Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (Studi Kasus Unit *Cyber Crime* Reskrimsus Polda Sulsel)" Skripsi ini menggunakan penelitian yang menggunakan pendekatan yuridis empiris yang lebih menekankan pada analisis faktor yang menyebabkan terjadinya kejahatan penipuan berbasis online khususnya di sulawesi selatan tepatnya pada unit *cybercrime* reskrimsus polda sulawesi selatan

E. Metode Penelitian

Penelitian merupakan suatu rangkaian kegiatan ilmiah yang dalam proses pembuatannya sudah semestinya menggunakan metode-metode ilmiah untuk mengkaji dan memecahkan suatu permasalahan yang akan dibahas atau untuk menemukan suatu kebenaran maupun fakta-fakta yang bertujuan untuk menjelasakan bagaimana penelitian tersebut dilakukan agar memperoleh hasil yang faktual.[18] Dan dalam hal ini, penulis dalam mempersiapkan penelitian ini menggunakan metode yang dapat penulis uraikan sebagai berikut:

1. Jenis dan Pendekatan

Penelitian ini menggunakan jenis penelitian yuridis normatif, Soerjono Soekanto dan Sri Mamudji , menjelaskan penelitian hukum normatif adalah "penelitian hukum yang dilakukan dengan cara meneliti bahan kepustakaan (data

[18] Ida Hanifah, dkk. *Op. Cit*, halaman 19.

sekunder).[19] Sedangkan pendekatan penelitian ini menggunakan pendekatan perundang-undangan. Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang terkait dengan isu hukum yang sedang dibahas(diteliti).[20]

2. Sifat Penelitian

Sifat penelitian yang digunakan dalam menyelesaikan penelitian ini adalah deskriptif yaitu penelitian yang hanya semata-mata melukiskan keadaan objek atau peristiwanya tanpa suatu maksud untuk mengambil kesimpulan-kesimpulan yang berlaku umum dengan menggunakan pendekatan yuridis normatif yang menggambarkan secara sistematis data mengenai masalah yang akan dibahas. Data yang terkumpul kemudian dianalisis secara sistematis sehingga dapat ditarik kesimpulan dari keseluruhan hasil penelitian.[21]

3. Sumber Data

Sumber data yang digunakan sehingga rampungnya penelitian ini dapat penulis uraikan sebagai berikut:

a. Data yang bersumber dari Hukum Islam yang digunakan sebagai sumber data pada penelitian ini ialah Q.S. Al-Maidah 5: 64 , Q.S Al – Ahzab (33) ayat 70-71 dan HR. Ibnu Hibban 2 : 326.
b. Data sekunder, merupakan data yang diperoleh dari berbagai kepustakaan yang mencakup dokumen-dokumen resmi, publikasi tentang hukum yang meliputi kamus-kamus hukum, buku-buku teks, serta jurnal-jurnal hukum dan

[19] Muhaimin , 2020, Metode Penelitian Hukum, Mataram : Mataram University Press, Halaman 47.
[20] *Ibid.*, Halaman 47.
[21] Ida Hanifah , dkk. *Op. Cit*, halaman 20.

komentar-komentar terhadap putusan pengadilan maupun yurisprudensi.[22] Dan dalam proses penelitian ini, yang menjadi data primernya antara lain :

1) Bahan hukum primer, yaitu bahan-bahan yang terdiri dari peraturan perundang-undangan, yaitu, Undang –Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Pasal 378, Pasal 263, dan Pasal 262 KUHP.
2) Bahan hukum sekunder adalah bahan yang memberikan penjelasan mengenai bahan hukum primer. Bahan-bahan yang memberikan penjelasan mengenai bahan hukum primer, seperti tulisan, jurnal dan buku-buku yang dianggap berkaitan dengan pokok permasalahan yang akan diangkat dalam penelitian ini.
3) Bahan hukum tersier, yaitu bahan yang memberikan petunjuk ataupun penjelasan terkait bahan hukum primer maupun bahan hukum sekunder, seperti kamus hukum ataupun ensiklopedia.[23] baik menggunakan via internet atau dari buku secara langsung.

4) Alat Pengumpul Data

Penelitian ini, alat pengumpul data yang dipergunakan dapat dilakukan dengan dua cara yaitu:

a. *Offline*, yaitu dengan mengumpulkan data dari studi kepustakaan (*library research*) secara langsung dengan mengunjungi, perpustakaan Universitas

[22] *Ibid.*, Halaman 20.
[23] Muhaimin, *Op.*cit., Halaman 62.

Muhammadiyah Sumatera Utara serta toko-toko buku, guna memperoleh data sekunder yang dibutuhkan dalam proses penelitian ini.

b. *Online*, yaitu studi kepustakaan (*library research*) yang dilakukan dengan cara mencari melalui media internet seperti *e-book*, *e-journal* dan hal-hal terkait tema penelitian dengan tujuan mengumpulkan data sekunder yang akan dibutuhkan dalam proses penelitian ini.

5) Analisis Data

Analisis data merupakan suatu rangkaian kegiatan memfokuskan, mengabstraksikan dan mengorganisasikan data secara rasional dan sistematis guna mendapatkan bahan pemecah permasalahan yang ada dalam penelitian ini.[24] Dan dalam hal melakukan penelitian ini proses analisis data yang digunakan ialah secara kualitatif yakni dengan pemilihan teori-teori, norma-norma, asas-asas, serta doktrin dan pasal-pasal didalam suatu perundang-undangan yang relevan dan berkaitan dengan permasalahan penelitian yang diangkat. Data yang diperoleh dari kepustakaan tadi kemudian dianalisis secara kualitatif guna menghasilkan data yang sistematis dan lalu diolah dalam bentuk deskriptif yang mencakup pemecah rumusan masalah yang menjadi pembahasan dalam penelitian.

[24] Ida Hanifah, dkk. *Op. Cit*, halaman 21.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Kriminologi

Kriminologi dilahirkan pada pertengahan abad ke-19, sejak dikemukakannya hasil penyelidikan Casere Lambroso (1876) tentang teori mengenai atavisme dan tipe penjahat serta munculnya teori mengenai hubungan kausalitas bersama Enrico Ferri sebagai tokoh aliran lingkungan dari kejahatan. Kriminologi pertengahan abad XX telah membawa perubahan pandangan. Kriminologi menyelidiki kausa jahat dalam masyarakat kemudian mulai mengalihkan pandangannya kepada proses pembentukan perundang-undangan yang berasal dari kekuasaan (negara) sebagai penyebab munculnya kejahatan dan para penjahat baru dalam masyarakat.

Istilah kriminologi untuk pertama kali digunakan oleh seorang ahli antropologi Perancis yang bernama Paul Topinard. Secara umum, istilah kriminologi identik dengan perilaku yang dikategorikan sebagai suatu kejahatan. Kejahatan dimaksudkan disini adalah suatu tindakan yang dilakukan orang-orang dan atau instansi yang dilarang oleh suatu undang-undang. Pemahaman tersebut diatas tentunya tidak bisa disalahkan dalam memandang kriminologi yang merupakan bagian dari ilmu yang mempelajari suatu kejahatan.[25] Secara etimologis, kriminologi berasal dari bahasa Yunani, *crime* (kejahatan) dan Jogos

[25] Sahat Maruli T. Situmeang, 2021. "*Buku Ajar Kriminologi*" Depok : PT. Rajawali Buana Pusaka, halaman 1

(ilmu), dengan demikian kriminologi adalah ilmu pengetahuan yang mempelajari tentang kejahatan.[26]

Kriminologi juga merupakan pengertian hukum yaitu perbuatan manusia yang dapat dipidana oleh hukum pidana. Tetapi kriminologi bukan semata-mata merupakan batasan undang-undang artinya ada perbuatan-perbuatan tertentu yang oleh masyarakat dipandang sebagai jahat tetapi undang-undang tidak menyatakan sebagai kejahatan atau tidak dinyatakan sebagai tindak pidana, begitu pula sebaliknya. Kriminologi dapat ditinjau dari dua segi yaitu kriminologi dalam arti sempit yang hanya mempelajari kejahatan dan kriminologi dalam arti luas yang mempelajari teknologi dan metode-metode yang berkaitan dengan kejahatan dan masalah prevensi kejahatan dengan tindakan-tindakan yang bersifat punitif.

Beberapa ahli hukum pidana juga mengemukakan pengertian kriminologi menurut pendapat masing-masing. Menurut Wood, kriminologi adalah keseluruhan pengetahuan yang diperoleh berdasarkan teori atau pengalaman yang berkaitan dengan perbuatan jahat dan penjahat dan termasuk reaksi masyarakat terhadap perbuatan jahat dan penjahat tersebut. Noach mengatakan bahwa kriminologi adalah ilmu pengetahuan tentang perbuatan jahat dan perilaku tercela yang menyangkut orang-orang yang terlibat dalam perilaku jahat dan perbuatan tercela tersebut. Walter Reckless mengatakan bahwa kriminologi adalah pemahaman ketertiban individu dalam tingkah laku delinkuen dan tingkah laku jahat serta pemahaman tentang bekerjanya sistem peradilan pidana.

[26] *Ibid.,* Halaman 1.

Berbagai definisi mengenai kriminologi menurut para sarjana salah satunya menurut M. P. Vrij yang mendefinisikan kriminologi sebagai ilmu yang mempelajari kejahatan, mula-mula mempelajari kejahatan itu sendiri, kemudian sebab-sebab serta akibat dari kejahatan itu sendiri.[27]

J.Constant memberikan definisi kriminologi sebagai ilmu pengetahuan yang bertujuan menentukan faktor-faktor yang menjadi sebab-musabab terjadinya kejahatan atau penjahat. Ilmu pengetahuan yang bertujuan untuk menyelidiki gejala kejahatan seluas-luasnya, Bonger membagi kriminologi menjadi 2 (dua) yaitu:

1. Kriminologi murni atau krimologi teoretis Secara teoretis, kriminologi terdiri dari (lima) cabang, yaitu:

a. Antropologi kriminal yaitu suatu ilmu pengetahuan yang mempelajari tentang manusia yang jahat (*sornatic*), atau ilmu pengetahuan yang mempelajari tanda-tanda fisik yang menjadi ciri khas penjahat. Misalnya menurut Lambroso, ciri-ciri penjahat antara lain adalaah tengkoraknya panjang, rambutnya lebat, tulang pelipisnya menonjol ke luar dan lain-lain.
b. Sosiologi kriminal yaitu suatu ilmu yang mempelajari kejahatan sebagai suatu gejala sosial. Sosiologi kriminal mempelajari faktor-faktor sosial yang menyebabkan timbulnya reaksi masyarakat dan akibat kejahatan, keadaan sosial dan ekonomi yang buruk menimbulkan kejahatan. Ilmu ini berkembang dalam kriminologi sehingga melahirkan mashab lingkungan yang dirintis oleh Perancis. Sosiologi kriminal, antara lain mencakup :

[27] *Ibid.,* Halaman 2.

1. Etiologi sosial, yaitu ilmu yang mempelajari tentang sebab-sebab timbunya suatu kejahatan.
2. Geografis, yaitu ilmu yang mempelajari pengaruh timbal balik antara letak suatu daerah dengan kejahatan.
3. Klimatologis, yaitu ilmu yang mempelajari hubungan timbal balik antara iklim dan kejahatan.
4. Meteorologis, yaitu suatu ilmu yang mempelajari pengaruh timbal balik antara cuaca dan kejahatan.

c. Psikologi kriminal yaitu suatu ilmu yang mempelajari kejahatan dari sudut ilmu jiwa. Psikologi kriminal meneliti sebab kejahatan terletak pada penyimpangan kejiwaan, meneliti relasi watak, penyakit (jiwa) dengan bentuk kejahatan serta situasi psikologis yang mempengaruhi tindakan jahat juga meneliti aspek psikis dari para oknum yang terlibat dalam persidangan (jaksa, hakim, panitera dan terdakwa) yang termasuk dalam kategori ini adalah :

1. Tipologi, yaitu ilmu pengetahuan yang mempelajari golongan-golongan penjahat.
2. Psikologi sosial kriminil, yaitu suatu ilmu pengetahuan yang mempelajari kejahatan dari segi ilmu jiwa sosial.

d. Psikopatologi dan Neuropathologi Kriminil, yaitu suatu ilmu yang mempelajari tentang penjahat yang sakit jiwa Neuropatologi kriminologi meneliti penyimpangan syaraf terhadap timbulnya kejahatan. Ahli yang bergerak dalam bidang ini berpendapat ketidakberesan susunan urat syaraf mendorong seseorang untuk berbuat jahat.

e. Penologi. Penologi adalah ilmu yang membahas timbul dan pertumbuhan hukum, arti hukuman dan faedah hukuman.[28]

2. Kriminologi Terapan atau Kriminologi Praktis Yaitu suatu ilmu pengetahuan yang berguna untuk memberantas kejahatan yang timbul dalam masyarakat. Cabang dari kriminologi praktis, diantaranya adalah:

a. Hygiene Crimineel (Higiene Kriminil), yaitu cabang kriminologi yang berusaha untuk mencegah terjadinya kejahatan, memberantas faktor penyebab timbulnya kejahatan, misalnya dengan meningkatkan perekonomian rakyat, usaha pemerintah untuk menetapkan undang-undang, adanya sistem jaminan hidup dan kesejahteraan yang dilakukan sematamata untuk mencegah terjadinya kejahatan.

b. Politik Kriminil, yaitu cabang kriminologi yang mempelajari tentang cara menetapkan hukuman yang sebaik-baiknya kepada terpidana agar terpidana tersebut dapat menyadari kesalahannya dan berniat untuk tidak berbuat kejahatan lagi.

c. Kriminalistik, yaitu ilmu pengetahuan tentang pelaksanaan penyidikan teknik kejahatan dan pengusutan kejahatan. E.H. Sutherland merumuskan kriminologi sebagai keseluruhan ilmu pengetahuan yang bertalian dengan perbuatan jahat sebagai suatu gejala sosial (*the body of knowledge regarding crime as a social phenomenon*). Sutherland selanjutnya berpendapat bahwa kriminologi mencakup proses-proses

[28] *Ibid.,* Halaman 3.

pembuatan hukum, pelanggaran hukum dan reaksi atas pelanggaran hukum. Sutherland membagi kriminologi ke dalam 3 (tiga) cabang utama, yaitu:

1. Sosiologi hukum menurut sosiologi hukum, kejahatan adalah perbuatan yang oleh hukum dilarang dan diancam dengan suatu sanksi. Jadi yang menentukan bahwa suatu perbuatan merupakan kejahatan adalah hukum. Menyelidiki mengenai sebab-sebab kejahatan berarti juga harus menyelidiki faktor-faktor yang menyebabkan perkembangan hukum, khususnya hukum pidana.
2. Etiologi kejahatan merupakan cabang kriminologi yang mencari sebab dari kejahatan. Etiologi kejahatan merupakan kajian utama dalam kriminologi.
3. Penologi pada dasarnya merupakan ilmu tentang hukuman, tetapi Sutherland memasukkan hak-hak yang berhubungan dengan usaha pengendalian kejahatan, baik represif maupun preventif. [29]

Kriminologi sebagai ilmu sosial yang mempersoalkan segala macam gejala sosial beserta ruang lingkup gejolak arti itu sendiri sehingga para ahli kriminologi memberikan pengertian menurut disiplin ilmunya masing-masing. Kriminologi dapat diartikan sebagai ilmu pengetahuan yang mempelajari tentang kejahatan.[30]

Hukum sebagai sarana perubahan sosial adalah adagium yang terkenal di di dalam referensi hukum. Meskipun sebaliknya, perubahan sosial juga berpengaruh untuk

[29] *Ibid.*, Halaman 3.

[30] Samosir, A. (2020). "*Penegakan Hukum Tindak Pidana Narkotika ditinjau dari Perspektif Kriminologi"*. Logika: Jurnal Penelitian Universitas Kuningan, 11c(02), halaman 90.

mengubah keadaan hukum. [31] Kemampuan bertanggung jawab dapat diartikan suatu keadaan psikis sedemikian rupa, sehingga penerapan suatu upaya pemidanaan , baik ditinjau secara umum maupun dari sudut orangnya dapat dibenarkan.[32]

Menurut Andi Zainal, bahwa kriminologi adalah ilmu pengetahuan yang mempelajari faktor-faktor penyebab kejahatan dan cara bagaimana menanggulanginya. Bonger menyatakan kriminologi adalah ilmu pengetahuan yang bertujuan menyelidiki gejala-gejala kejahatan seluas-luasnya. Mabel Elliot, mendefinisikan bahwa kriminologi adalah kejahatan keseluruhan kelakuan yang dilarang dan dipidana oleh negara sebagaimana dirumuskan dalam undang-undang. Selanjutnya, secara etimologis kriminologis berasal dari kata "*crime"* yang artinya kejahatan, sedangkan "*logos*" yang artinya ilmu pengetahuan. Secara lengkap, kriminologi dapat diartikan sebagai ilmu pengetahuan yang mempelajari tentang kejahatan.[33]

Setiap masyarakat mempunyai suatu sistem aturan-aturan yang diundangkan oleh golongan penguasa atau golongan dominan untuk mengatur perilaku anggota-anggotanya. Dalam masyarakat demokratis, warga negara mempunyai suara dalam menentukan aturan-aturan dan memperluas penerapan aturanaturan itu. Sedangkan pada masyarakat oligarkhi atau berkediktatoran, satu atau lebih pemimpin yang mempunyai keputusan menentukan. Tingkat konsensus yang mendukung perilaku yang diatur oleh undang-undang berbeda-beda.

---

[31] Awaludin Marwan, 2022. Pengantar Filsafat Hukum , Yogyakarta : Thafa Media , Halaman 38.

[32] Teguh Prasetyo,2019. "Hukum Pidana", Depok : PT. Rajagrafindo Persada , Halaman 85.

[33] Samosir A, *Op.cit.,* halaman 90.

Andaikata terdapat konsensus umum, senantiasa terdapat sejumlah warga negara yang melanggar aturan-aturan itu. Jika aturan-aturan formal ini diundangkan oleh mereka yang melaksanakan kekuasaan politik dan jika pelanggaran itu dihukum atas nama negara atau pemerintah, maka pelanggaranpelanggaran itu dianggap sebagai kejahatan. Pelbagai cara aturan itu dilanggar, respons negara atau masyarakat atas pelanggaranpelanggaran itu, akibat pelanggaran-pelanggaran itu atas perubahan sosial dalam masyarakat, identifikasi dan pembinaan pelanggar hukum, semuanya adalah aspek-aspek masalah kejahatan. Kriminologi merupakan suatu usaha sistematik untuk memahami gejala ini.[34]

Unsur-unsur pokok untuk menyebutkan sesuatu perbuatan sebagai kejahatan ada 7 yaiu :

a. Ada perbuatan yang menimbulkan kerugian

b. Kerugian yang ada tersebut telah diatur didalam KUHP

c. Harus ada perbuatan

d. Harus ada maksud jahat

e. Ada peleburan antara maksud jahat dan peruatan jahat

f. Harus ada perbauran antara kerugian yang telah diatur di dalam KUHP

g. Harus ada sanksi pidana yang mengancam peruatan tersebut.[35]

[34] Nursariani Simatupang & Faisal, *Op.cit*, halaman 9.
[35] A.S Alam ,2018 , Kriminologi , Jakarta : Prenadamedia Group , Halaman 32

Kriminologi diamalkan untuk kepentingan memahami kejahatan dan berbagai perilaku yang menyimpang dan bukanlah sarana yang diterapkan bagi peradilan semata-mata seperti kriminalistik, melainkan sebagai pure *science* yang hasil penelitiannya secara objektif dapat dimanfaatkan bagi kepentingan praktis. Kriminologi itu suatu gabungan (*complex*) ilmu-ilmu lain yang dapat disebut ilmu bagian (*deelwetenschap)* dari kriminologi. Kriminologi adalah ilmu yang menyelidiki dan membahas asal-usul kejahatan (*etiologi* kriminal, *criminale aetiologi*) dimana kejahatan dapat dipandang sebagai sesuatu yang bukan hanya pelanggaran hukum saja namun sebagai tindakan manusia dan suatu gejala sosial.[36]

B. Kejahatan Dunia Maya *(cybercrime)*

Secara etimologi *cybercrime* berasal dari dua rangkaian kata, yaitu *cyber* dan *crime*. Menurut Kamus Bahasa Inggris-Indonesia cyber berarti maya sedangkan crime diartikan dengan kejahatan.[37] Menurut D*ictionary of Contemporary English*, *crime* adalah *an offence which is punishable by law* (suatu kejahatan yang dihukum oleh hukum), *illegal activity in general* (kegiatan ilegal pada umumnya), atau *a bad, immoral, or dishonourable act* (tidak terhormat, tidak bermoral atau tindakan yang buruk). Secara kebahasaan *cybercrime* samakna dengan "kejahatan dunia maya" atau "kejahatan mayantara". Pembangunan nasional di Indonesia telah mencapai era tinggal landas, hal ini ditandai dengan meningkatnya era globalisasi yaitu adanya pertumbuhan ekonomi dan

[36] *Ibid*., Halaman 33.

[37] Mohammad Haidar Ali. (2012) " Cybercrime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang ITE (Perspektif Hukum pidana Islam)". (Tesis) Fakultas Hukum Islam Uin Alauddin Makassar , Halaman 31

perkembangan pemanfaatan Ilmu Pengetahuan (IPTEK). Dalam hal ini produk IPTEK tersebut yang berkembang adalah teknologi komputer yang hampir menguasai seluruh aspek masyarakat modern. Perkembangan teknologi dewasa ini semakin pesat, khususnya teknologi telekomunikasi dan teknologi komputer yang menghasilkan internet dengan berbagai multifungsi menggiring kita berfikir ke arah yang tanpa batas (*bordelles way of thinking*).[38] Era informasi ditandai dengan aksesibilitas informasi yang sangat tinggi sebagai komoditi utama yang diperjual belikan sehingga akan muncul berbagai *network and information company* yang akan memperjualbelikan berbagai fasilitas bermacam jaringan dan berbagai basis data informasi berbagai hal yang dapat diakses oleh pengguna dan pelanggan.[39] Bahwa internet menghadirkan *cybercpace* dengan realitas virtual banyak menawarkan kepada masyarakat dengan berbagai macam dan harapan, dimana ada sisi negatif maupun positif. Sehingga timbul permasalahan kejahatan yang disebut *cyber crime*, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran maupun komputer itu sendiri yang menjadi sasaran kejahatan. Informasi telah menjadi komoditi utama sehingga berbagai upaya sangat diperlukan untuk melindungi dari tindak kejahatan. *Cybercrime* merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet sebagai perbuatan melawan hukum yang dilakukan menggunakan internet yang berbasis pada kecanggihan teknologi, komputer, dan telekomunikasi baik untuk memperoleh keuntungan ataupun tidak dengan merugikan pihak lain. [40]

---

[38] Endang Prastini , *Kebijakan Kriminal Pemerintah Terhadap Kejahatan Dunia Maya (Cybercrime) di Indonesia* , jurnal surya kencana 2, 2018, Vol 5, No 2, Halaman 2.

[39] *Ibid*., halaman 3.

[40] *Ibid*., halaman 58

Di Indonesia, masalah dari *cybercrime* juga bisa dikatakan mulai diperhatikan sebagai suau masalah yang serius dengan masuknya Indonesia kedalam era globalisasi. *Cybercrime* adalah kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet. Berdasarkan pengertian tersebut terlihat bahwa *cybercrime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet. Definisi ini tidak menyebutkan secara spesifik dari karakteristik *cybercrime*, definisi ini mencakup segala kejahatan yang dalam modus operandinya menggunakan fasilitas internet. Dikatakan Barda Nawawi Arif, bahwa kejahatan *cybercrime* dibagi menjadi 2 (dua) kategori, yaitu *cybercrime* dalam pengertian sempit (kejahatan terhadap sistem komputer) dan *cybercrime* dalam pengertian luas (mencakup kejahatan terhadap sistem komputer dan kejahatan menggunakan sarana komputer).

Karakteristik *cybercrime* dalam kejahatan konvensional terbagi menjadi 2 (dua) jenis kejahatan, yaitu: kejahatan kerah biru (*Blue Collar Crime*) dan Kejahatan kerah putih (*White Collar Crime*). Kejahatan kerah biru merupakan kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti: perampokan, pembunuhan, pencurian, dan lain-lain. Sedangkan kejahatan kerah putih terbagi menjadi kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu. *Cybercrime* sebagai kejahatan yang muncul akibat adanya komunitas dunia maya di internet yang memiliki karakteristik unik dari kejahatan

di dunia maya, antara lain: ruang lingkup kejahatan, sifat kejahatan, modus, dan jenis-jenis kerugian yang ditimbulkan.[41]

Cybercrime sebagai suatu masalah bukanlah hal yang mudah untuk diselesaikan. Hal ini dikarenakan *Cybercrime* sebagai suatu jenis kejahatan yang merupakan suatu tindakan yang dilakukan didalam dunia yang tidak mengenal batas wilayah hukum dan kejahatan teserbut.Mengingat terus meningkatnya kasus-kasus *cybercrime* di Indonesia, maka pemerintah mengambil kebijakan untuk menaggulangi kejahatan tersebut. Bahwa kebijakan menentukan suatu perbuatan tindak pidana, sehubungan dengan kenyataan bahwa undang-undang memberikan wewenang dan dasar legitimasi kepada penegak hukum untuk menyatakan apakah perbuatan seseorang merupakan kejahatan atau tidak. Tetapi undang-undang dapat juga merupakan faktor kriminogen apabila tidak konsisten dengan kenyataan, terpisah dengan nilai-nilai masyarakat sehingga muncul sikap tidak percaya mengenai efektivitas sistem hukum tersebut.[42]

C. Pengelabuan (*phising*)

Sejarah *phising* telah mengganggu dunia maya selama lebih dari 2 dekade, dimulai pada tahun 1995 dengan *America Online* (AOL) 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 phishing dilakukan *oleh Lastdrager*

[41] Bima Guntara , 2020. *Cybercrime* : penghinaan dan pencemaran nama baik melalui dunia maya , jawa tengah : Cv. Pena Persada, Halaman 3.

[42] *Ibid*., Halaman 2.

dimana dia mengidentifikasi definisi *phishing* yang disepakati: "*Phishing* 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. Serangan *phishing* 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 *phishing* 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 di sektor 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 *phishing* ini serius, menarik untuk mengetahui secara detail vektor serangan phishing saat ini dan Informasi ini akan sangat berharga dalam pengembangan teknik anti phishing serta untuk menciptakan kesadaran publik.[43] Tentang teknik *phishing* dan cara kerjanya, Keterkaitan antara media

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

phishing, vektor atau saluran yang digunakan dan pendekatan teknis yang diterapkan dalam pelaksanaan operasi *phishing* dibahas. Interlink tersebut adalah:

1. Interlink antara media *phishing* dan vektor dan
2. Interlink antara vektor dan pendekatan teknis. Tautan pertama menunjukkan elemen dalam media yang dieksploitasi dan digunakan dalam serangan *phishing*. Phising adalah upaya untuk mendapatkan informasi tentang data pribadi dengan menggunakan teknik *phising*, data *phising* mencakup informasi pribadi (nama, alamat, jenis kelamin, tanggal lahir). *Phising* merupakan kejahatan digital yang menargetkan informasi atau data sensitif korban melalui *email*, unggahan media sosial, atau pesan teks dengan kata lain *phising* merupakan sebuah serangan yang dilakukan untuk menipu atau memancing korban agar mau mengklik link atau tautan serta menginput informasi kredential seperti *username* dan *password*.[44]

Pelaku *phising* biasanya menampakkan diri sebagai pihak atau institusi yang berwenang, mereka menyisipkan tautan di dalam narasi yang disebarkan dan menggiring korban agar mengklik tautan tersebut. Data yang menjadi sasaran *phising* adalah data pribadi seperti nama, usia, alamat dan data akun seperti *username* dan *password* serta data finansial seperti informasi kartu kredit atau rekening bank. Informasi data yang diperoleh dari aktivitas *phising* nantinya akan dimanfaatkan untuk menipu orang bagi yang tidak bertanggungjawab. Data tersebut juga dapat dijual untuk melakukan tindakan yang tidak bertanggung jawab seperti penyalahgunaan akun.[45]

---

[44] *Ibid*, halaman 6.

[45] Ni Komang Arista Tri Wahyuni, dkk, *Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zhiphiser, Shellphish dan Whphiser* , Jurnal Teknik Mesin Elektro Dan Ilmu Computer , Vo. 3 no. 1, 2023 halaman 24

Menurut laporan, 32% pencurian data selalu melibatkan kegiatan phising. Bahkan, di awal Tahun 2020 saja, Anti Phishing Working Groupmencatat sudah ada 165.772 website phising yang siap menjaring korban.[46]

Phishing termasuk dalam kejahatan *cybercrime* dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan cari paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang hacker.[47]

Pengaturan perlindungan data pribadi telah diatur dalam Undang-undang perlindungan data pribadi yang disahkan jadi Undang-undang dalam rapat praipurna DPR RI pada tanggal 20 september 2022. Dalam Undang-undang ini terdapat 16 Bab dan 78 Pasal, pembahasan Bab dalam Undang-undang Perlindungan Data Pribadi diantaranya yaitu: [48]

1. Ketentuan Umum
2. Asas
3. Jenis data Pribadi
4. Subjek Data Pribadi
5. Pemrosesan Data Pribadi
6. Kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi dalam Pemrosesan Data

[46] *Ibid*, halaman 24.

[47] Annisa Indah Pertiwi, *Tindak Pidana Cyberspace dalam akses illegal terhadap bocornya data informasi public*, Jurnal Ilmu Hukum Vol. 1 No 2 , 2023, halaman 143

[48] *Ibid*, halaman 144

7. Transfer data pribadi
8. Sanksi Administratif
9. Kelembagaan
10. Kerja Sama Internasional
11. Partisipasi Masyarakat
12. Penyelesaian Sangketa dan Hukum Acara
13. Larangan dalam Penggunaan Data Pribadi
14. Ketentuan Pidana
15. Ketentuan Peralihan
16. Ketentuan Penutup

Pentingnya undang-undang PDP ini karena data warga negara ialah hal yang paling yang paling mendasar dan diperhatikan agar data dikelola dengan baik dan benar. Undang-undang PDP ini begitu penting karena untuk melengkapi transformasi di era digital ini dan juga agar dapat jaminan hukum yang benar-benar jelas dan tegas pada kasus-kasus kebocoran data yang muncul. Faktor penyebab kebocoran data bisa disebabkan oleh 2 sumber yaitu: [49]

1. Faktor eksternal
2. Faktor internal dalam penyebab kebocoran data biasanya dikarenakan faktor kelalaian diri sendiri di era digital saat ini, masyarakat telah diperkenalkan dengan salah satu kecanggihan teknologi berupa sosial media atau dunia maya. Hal tersebut menyebabkan meningkatnya kejahatan di dunia maya

[49] Mekarsign, Apa Itu Kebocoran Data Dan Penyebab Dan Cara Mengatasinya, https://mekarisign.com/blog/apa-itu-kebocoran-data/ di akses melalui tanggal 20 Juli 2023 pukul 21.00 wib.

atau bisa disebut dengan *cyberspace*. Sedangkan Faktor eksternal dalam penyebab kebocoran data biasanya disebabkan oleh:[50]

1. Perangkat Fisik yang Tidak Dijaga Seperti meninggalkan *handphone*, laptop dan alat elektronik lainnya di sembarang tempat sehingga dapat menimbulkan terjadinya penyadapan berupa menautkan perangkat pribadi ke perangkat lainnya seperti halnya fitur dalam *whatsapp* dan telegram yang memungkinkan untul tertautnya perangkat pribadi kita ke perangkat orang yang ingin menyadap.
2. Terserang *malware* adalah program yang dibuat oleh penyadap untuk merusak perangkat dan juga mencuri data. *Malware* akan menyerang melalui *email, website*, maupun aplikasi. Dalam masyarakat sendiri malware itu sering terjadi berupa *phising*.
3. Sistem yang bermasalah karena sistem yang dibuat terlalu lemah dan bermasalah sehingga akan memberikan celah keamanan yang bisa dimanfaatkan oleh oknum-oknum dari luar yang tidak bertanggung jawab.
4. *Human error* disebabkan oleh ketidaksengajaan yang dikarenakan ulah diri sendiri. Tindakan penyadapan tersebut membuat masyarakat menimbulkan protes dengan tegas karena tindakan itu sama saja dengan perbuatan yang tercela atau buruk. Terlihat jelas yang hanya mementingkan diri sendiri, tidak hanya itu tetapi juga melanggar HAM.

[50] Annisa Indah Pertiwi,*Op.cit*, halaman 145

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Modus Terjadinya Kejahatan Dunia Maya Pengelabuan (*Phising*) Dalam Bentuk Mengirimkan Suatu Link

Perkembangan masyarakat era kini merupakan industrialisasi, serta ditopang perkembangan teknologi telekomunikasi, maka hubungan antar negara sudah bersifat mendunia yang kemudian menciptakan dunia tatanan baru. Internet merupakan salah satu aspek yang mengalami perkembangan yang sangat pesat. Internet sudah menjadi salah satu kewajiban dalam hidup saat ini. Fakta tersebut juga mempengaruhi terhadap perkembangan kejahatan. Kasus kejahatan siber di Indonesia sudah banyak terjadi, mulai dari penipuan identitas hingga yang bahkan tidak pernah dilakukan. Berbagai kejahatan siber ini pun banyak dilakukan melalui media sosial, seperti *Facebook, WhatsApp, Instagram*, dan masih banyak lagi**.**[51]

Terjadinya kejahatan maka ada pelaku kejahatan yaitu orang yang telah melakukan kejahatan yang sering pula disebut "penjahat". Penjahat adalah orang yang sering melakukan kejahatan.[52]

Cybercrime dalam bentuk *phising* adalah suatu kejahatan kejahatan siber yang membuat pemalsuan data di suatu *website* palsu yang tampilannya mirip dengan *website* aslinya, tetapi mempunyai tujuan yang sama untuk mendapatkan

[51] Mohd. Yusuf DM, *Analisis Terhadap Modus-Modus Dalam Hukum Cyber Crime,* Jurnal Hukum, Politik Dan ilmu Sosial Vol, No.2, 2022, halaman 64.

[52] Mhd. Teguh Syuhada Lubis, *Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Penyeludupan Manusia ,* De Lega Lata, Volume 2, Nomor 1,2017 , halaman 95.

informasi mengenai indentitas orang lain yang akan digunakan dengan illegal tanpa sepengetahuan pemilik asli tersebut.[53]

Modus kejahatan dunia maya termasuk ancaman dunia maya seperti rekayasa sosial, eksploitasi kerentanan perangkat lunak, dan serangan jaringan**.**

Cybercrime adalah kegiatan kriminal di dunia maya yang menggunakan jaringan komputer sebagai alatnya dan internet sebagai medianya dalam arti yang lebih luas, kejahatan dunia maya adalah aktivitas ilegal yang terjadi di jaringan komputer atau internet untuk menghasilkan keuntungan dengan mengorbankan orang lain. Selanjutnya, *cybercrime* yang di definisikan secara sempit adalah aktivitas ilegal yang ditujukan untuk menyerang sistem keamanan komputer dan data yang diproses oleh sistem komputer.[54]

Awal mula terjadinya *phising* tidak cukup dengan menirukan tampilan sebuah web, masih ada beberapa modus tambahan lainnya yang ditujukan untuk mendukung suksesnya terjadinya *phising* yaitu dengan menyebarkan link agar orang bersedia membuka link / URL yang berisikan halaman palsu tersebut, dengan demikian link / URL yang anda miliki perlu menyamarkan dirinya terutama sekali dalam hal ini memodifikasi URL. Salah satu point yang dengan menggunakan nama yang mirip misalnya *Facebook.com* diubah menjadi *facebook.com* dan sebagainya untuk menyamarkan sebuah URL sehingga terlihat seolah-olah URL yang asli.[55]

Phising adalah jenis penipuan dunia maya yang bertujuan mencuri akun korban. Tentu saja, sebagian besar kejahatan dunia maya biasanya dimulai dengan phising sehingga pengguna internet harus selalu waspada.[56]*Phising* juga biasanya

[53] Andrew Christian Banjarnahor, *Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo*, Hermeutika : Jurnal Ilmu Hukum, Vol. 6 , No. 1 , 2022 halaman 33.

[54] Ferry Irawan , Op.cit., Halaman 185.

[55] Efvy zam, 2014, Phising, Jakarta : Mediakita , halaman 146.

[56] Kadek Odie Kharisma Putra , Op.cit., Halaman 78.

menyasar pengguna *online banking* karena penggunaan data pengguna dan kata sandi tidak menutup kemungkinan dialihkan ke pengguna *online* lainnya.

Phising biasanya dilakukan melalui media sosial yang terhubung dengan internet, seperti melalui email atau SMS dan *website*. Pengetahuan pengguna yang minim tentang alat teknologi informasi yang digunakan adalah yang mendorong *phising*. *Phishing* dapat terjadi di berbagai *platform*, termasuk media sosial, situs *web*, dan juga aplikasi. [57]

Saat ini, banyak orang yang menggunakan aplikasi *WhatsApp* sebagai aplikasi untuk bertukar pesan, dan *Instagram* sebagai aplikasi yang memungkinkan pengguna untuk mengambil foto dan video serta membagikannya untuk diperlihatkan kepada banyak orang. Hal ini pun dimanfaatkan oleh orang tidak bertanggung jawab dan menggunakannya untuk kejahatan. Pada *WhatsApp*, penjahat mencoba mengirim pesan ke nomor tertentu. Pesan ini mungkin berisi informasi bahwa nomor ini telah dipilih sebagai pemenang lotre dan ketika pengguna menekan link tersebut, mereka diminta untuk mengonfirmasi melalui link tersebut. Pengguna akan dibawa ke situs *web* berbahaya yang telah dimodifikasi oleh pelaku. Selain dari media sosial, *website* juga merupakan salah satu target para *hacker* untuk melakukan phising dengan memanfaatkan iklan dan icon palsu pada *website* yang dapat di klik oleh pengguna, maka pengguna akan diarahkan pada suatu link yang sudah dikonfigurasi oleh hacker untuk mencuri data. Sangat banyak kasus seperti ini khususnya pada kalangan pelajar, penipuan yang pernah terjadi adalah penerimaan kuota gratis yang diselenggarakan oleh Kemendikbud.

[57] Ibid, Halaman 78.

Phishing merupakan ancaman menggunakan teknik rekayasa sosial dengan mengelabui pengguna. Pelaku mengelabui pengguna dengan mengaku sebagai penjual dan melakukan penawaran palsu melalui *e-mail*, pesan singkat dan panggilan telepon. Setelah mendapatkan data pribadi pengguna, selanjutnya pelaku menggunakan data korban untuk keuntungan pribadi. Pelaku *phising* tidak mempunyai ciri khas, kecuali berhubungan dengan kemahirannya dalam menggunakan komputer dengan teknologi inforrmasinya.[58] Demikian pula korban *phising* adalah individu dan lembaga (bisnis maupun negara) yang memanfaatkan teknologi informasi. Banyak ahli kriminologi yang menempatkan *phising* sebagai dimensi khusus dari *white collar crime* karena sifat khusus dari kejahatan tersebut yang tidak mungkin dilakukan oleh sembarang orang.

Pelaku melakukan modus *phising* dengan cara:

1. *Phising* melalui telepon Pelaku menggunakan telepom yang mengatas namakan pihak bersangkutan. Menanyakan maupun meminta hal yang bersifat pribadi baik *user id* maupun *password* yang digunakan korban serta kode OTP yang digunakan pelaku dalam mengakses handphone yang digunakan korban.
2. *Web Forgery* Situs web yang dibuat oleh pelaku yang digunakan untuk menipu korban dengan tampilan yang sangat mirip dengan *website* aslinya. Digunakan pelaku untuk mengetahui *user id* maupun *password* korban yang biasanya korban diharuskan mengisi data diri di *website* palsu tersebut. Data yang telah dimasukkan korban ah yang akan dimanfaatkan pelaku untuk disalah gunakan.

[58] Irvan Hadi Ramadhan , Analisis Ancaman Phising Dalam Layanan *E-commerce* , Jurnal SNAST, 2022 , Halaman 34.

Dan dalam hal ini penulis meneliti modus phising yang dilakukan dengan cara mengirimkan suatu link atau situs *web*.[59]

Phising pelaku biasanya akan mengaku dari lembaga resmi melalui sambungan telepon, *email* atau pesan teks. Mereka memanipulasi korban supaya mau memberikan data pribadi yang akan digunakan untuk mengakses akun penting milik korban, *Phishing* bisa mengakibatkan berbagai kerugian, antara lain pencurian identitas pribadi. [60]

Phising merupakan kejahatan digital yang menargetkan informasi atau data sensitif korban melalui *email,* unggahan media sosial, atau pesan teks. Dengan kata lain, *phising* merupakan sebuah serangan yang dilakukan untuk menipu atau memancing korban agar mau mengklik link atau tautan serta menginput informasi kredential seperti username dan password. Pelaku *phising* biasanya menampakkan diri sebagai pihak atau institusi yang berwenang. Mereka menyisipkan tautan di dalam narasi yang disebarkan dan menggiring korban agar mengklik tautan tersebut. Data yang menjadi sasaran phising adalah data pribadi seperti nama, usia, alamat dan data akun seperti username dan *password,* serta data finansial seperti informasi kartu kredit atau rekening bank. Informasi data yang diperoleh dari aktivitas phising nantinya akan dimanfaatkan untuk menipu orang bagi yang tidak bertanggungjawab. [61]

Cara kerja *phising* tahap awal kegiatan *web phising* akan dimulai dengan menentukan siapa calon korbannya. Pada umumnya, korban yang disukai adalah

[59] Andrew Christian Banjarnahor , *Op.cit* , Halaman 34.
[60] Mohd. Yusuf DM , *Op.Cit* , Halaman 67.
[61] Ni Komang Arista Tri Wahyuni , *Op.cit*., Halaman 24.

pengguna *platform* pembayaran *online* seperti *Ovo, PayPal*, dan lainnya. Tidak hanya itu saja, banyak pelaku phising yang mengincar pengguna *platform* yang memiliki celah keamanan. Kasus terbaru terjadi pada platform komunikasi *Zoom*.[62]

Setelah mendapatkan calon korban yang potensial, pelaku akan mulai memikirkan apa yang akan dicapai dari kegiatan *web phising* yang dilakukan. Apakah akan *menarget username* dan *password* pengguna untuk menguasai akun. Apa malah mendapatkan semua informasi korban melalui sebuah prosedur yang disiapkan. Pada contoh aksi *phising PayPal*, pelaku menginginkan semua informasi dari pengguna platform tersebut. Seperti ditunjukkan *welivescurity.com*, pengguna akan menerima *email* untuk mengkonfirmasi data diri melalui sebuah link *website* palsu yang di sediakan untuk melancarkan aksinya pelaku akan mulai menyiapkan *website* palsu untuk melakukan aksi *phising*, mulai dari mendesain *website* palsu, memilih nama domain yang mirip dengan domain asli hingga menyiapkan konten dengan tulisan yang meyakinkan. Pada prakteknya, pelaku kadang membuat *website* yang sangat menyerupai halaman *website* resmi tapi menggunakan nama domain yang jauh berbeda seperti terlihat di contoh atas. Namun, pada contoh kasus *phishing* Danamon *Online* beberapa waktu lalu, Anda akan langsung melihat bahwa domain yang digunakan mirip sekali dengan *website* resminya dengan tampilan *website* dan informasi yang meyakinkan, tak sedikit calon korban yang akhirnya mengakses *website phising* milik pelaku. Langkah ini biasanya di dahului dengan mengajak calon korban melalui *email* phising atau link yang disebarkan via SMS

[62] *Ibid*., Halaman 24.

atau akun media sosial. Inilah kunci dari terjadinya aksi phising jika calon korban melakukan instruksi yang diberikan pelaku maka pelaku akan berhasil mencapai tujuannya. Sebagai contoh, pada halaman *website* yang disediakan, calon korban diminta melakukan *update* informasi pribadi hingga data pembayaran pada akun yang digunakan. Pada saat selesai mengisi data dan melakukan submit saat itulah semua informasi korban berhasil dimiliki. Jika aksi *web phising* berhasil, pelaku akan memanfaatkan data yang telah diterima. *Website phising* merupakan situs *web* yang dirancang untuk melakukan pengelabuan terhadap korban dengan cara percobaan untuk mendapatkan informasi sensitif, seperti nomor ip akun web, kata sandi aplikasi media sosial dan lainnya. [63]

Terdapat beberapa tahapan yang dilakukan *hacker* untuk mengelabuhi korban dengan cara melakukan *web phising*, diantaranya sebagai berikut:

1. Mencari dan melengkapi informasi, informasi-informasi yang dicari kemudian dikumpulkan oleh *hacker* sebagai tahap awal dilakukannya serangan *phising* ini tujuanya adalah untuk mendapatkan nama, nama akun korban.
2. Tahap kinerja, tahap ini bisa juga dikatakan dengan tahap eksekusi, dimana pada tahap ini pelaku hacker akan melakukan serangan *phishing* dengan cara menggunakan *tools phishing* kemudian memberikan link kepada korban. sehingga *hacker* dapat mencuri data korban. *Tools* yang dianalisis meliputi *ZPhisher, Shellphish* dan *WhPhisher*, akan ada analisis, pengukuran dan pengujian dalam metode penelitian ini.

[63] *Ibid*, Halaman 24.

a. *Zphisher*-Analisis *Zphisher* adalah *tools Phishing* berupa *open-source* yang kuat. *Tools* ini menjadi sangat populer saat ini yang digunakan untuk melakukan serangan phishing pada Target. *Zphisher* lebih mudah daripada *toolkit* rekayasa sosial.
b. *Shellphish*-Analisis *ShellPhish* adalah alat *phishing* yang ditulis dalam *bash* oleh *thelinuxchoice. Shellphish* menawarkan total 18 situs *web phishing* dan satu situs *web* khusus yang dapat dikirim ke target. Hal yang baik tentang alat ini adalah kita tidak perlu bersusah payah menyiapkan layanan *hosting* atau penerusan portal.
c. *WhPhishe*r-Analisis *WhPhisher* merupakan salah satu *tools* terbaik untuk melakukan *phising* dengan halaman yang paling terkenal yang telah diperbarui.[64]

Berikut beberapa tata cara modus phising terjadi :

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, *phishing* menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima *email*. Penyerang akan mengirimkan jutaan *email* ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut. Pastinya serangan-serangan

[64] *Ibid* , Halaman 25.

tersebut menggunakan *email* palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi.

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.
3. *Malware* cara penyerangan dengan berpura-pura meminta karyawan untuk men-*download* suatu file yang di kirim oleh *phiser* sebagai penetralisir *malware* di komputer nantinya.[65]

Herbert L. Parker pernah mengingatkan bahwa penggunaan sansksi pidana secara serangan sembaranagan / menyamaratakan dan digunakan secara paksa (coercively) akan menyebabkan sarana hukum.[66]

Beberapa metode *phising* yang ada, antara lain :

1. Spam *email* media *phising* paling umum untuk mencari korban. Penjahat dapat mengirimkan jutaan *email* sehari tanpa menghabiskan banyak uang, *phisher* juga suka menggunakan server bajakan untuk tindakan mereka. *Email* tersebut tidak memiliki konfirmasi, sehingga pelaku dapat mengubah "Dari" menjadi apa pun yang mereka inginkan. Pelaku dapat membuat

[65] Mohd Yusuf DM , Op.cit., Halaman 8021
[66] Faisal, 2021. Hukum Pidana , Jakarta : Kencana , Halaman 8.

email dengan mengambil format *email* resmi, membuatnya lebih meyakinkan , dan hanya mengubah bagian yang diperlukan.

2. Trojan *phising* mengelabui korban agar memasang kuda troya atau mengelabui korban dengan kuda troya. Trojan ini memberikan korban kendali penuh atas komputer mereka dan memungkinkan mereka untuk diarahkan ke situs *web* yang menawarkan jebakan. Pelaku *phising* Trojan juga dapat mengelabui korban agar memasang kuda troya dan menggunakan kuda troya untuk mengelabui korban. Trojan ini memberikan korban kendali penuh atas komputer mereka dan memungkinkan mereka untuk diarahkan ke situs *web* yang menawarkan jebakan. *Instant messaging* , media *chat* popular juga bertindak sebagai agen *phising*, mengirimkan alamat intersepsi kepada korban. Pelaku biasanya mengirimkan link tersebut tanpa pandang bulu, namun beberapa bahkan mengunjungi halaman palsu sebelum mengirimkan informasi tersebut. Beberapa serangan phising sebagai berikut :
    1. *Man in the middle* dengan teknik ini, *hacker* menempatkan dirinya diantara korban dan halaman *web* asli yang sedang diakses. Peretas menerima data komunikasi yang dapat mereka modifikasi sesuai keinginan mereka. Serangan *Man in the middle* dapat terjadi di jaringan lokal atau jaringan internet global.
    2. URL *Obfuscation URL* (*Uniform Resource Locator*) merupakan alamat *web* yang diketik di *browser* untuk membuka *website*. *Obfuscation*

adalah teknik menyamarkan alamat URL agar tidak terlihat mencurigakan bagi pengguna.

3. Gambar yang menyesatkan, *phiser* menggunakan berbagai teknik yang sangat berbahaya untuk mengelabui korban, tetapi URL yang ditampilkan di *browser* anda adalah senjata utama anda untuk mengidentifikasi alamat palsu. *Phiser* membuat *addres bar* yang menyerupai aslinya, dan *address bar* asli disembunyikan oleh *phisher*, sehingga semua URL di *browser* terlihat asli dan tanpa huruf atau karakter aneh.

B. Faktor-Faktor Yang Menjadi Penyebab Terjadinya Kejahatan Dunia Maya Bermodus Pengelabuan (Phising) Dalam Bentuk Mengirimkan Link

Era kemajuan teknologi informasi ditandai dengan meningkatnya pengguna internet dalam setiap aspek kehidupan manusia. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, di sisi lain meudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana. Munculnya kejahatan dengan mempergunakan internet sebagai alat bantunya *cybercime* lebih banyak disebabkan oleh faktor keamanan pelaku dalam melakukan kejahatan , masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam *cybercrime.*

Berbicara mengenai kejahatan, merupakan bagian dari sifat buruk manusia yang memberikan kesusahan bagi orang lain. Kejahatan menimbulkan kerugian baik moral maupun materiil kepada orang lain yang disebabkan karena keinginan manusia yang besar untuk membuat dirinya bahagia dengan menyakiti

orang. Seiring dengan perkembangan teknologi, kajahatan manusia tidak hanya dilakukan di dunia nyata saja, melainkan dilakukan di dunia maya atau biasa disebut dengan *cybercrime*. Munculnya Internet sebagai media komunikasi baru dikaitkan dengan klaim yang saling bertentangan tentang munculnya pola-pola baru interaksi sosial.[67]

Cybercrime merupakan kejahatan yang timbul karena dampak negatif pemanfaatan teknologi internet. *Cybercrime* ini bukan hanya kejahatan terhadap komputer tetapi juga kejahatan terhadap sistem jaringan komputer dan pengguna. Pelaku *cybercrime* saat ini melakukan kejahatan tersebut bukan hanya karna mempraktikkan keahlian yang dimiliki tetapi juga karena motif lain seperti uang, dendam, politik, iseng, dan sebagainya. *Cybercrime* dilakukan oleh orang-orang yang memiliki kemampuan tinggi terhadap komputer dan jaringannya. Oleh karena itu dalam penanggulangannya dibutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut, selain itu juga diperlukan adanya kerja samadengan lembaga khusus untuk memberikan informasi tentang *cybercrime*, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *cybercrime*.

Kesadaran hukum masyarakat proses penegakan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. Melalui sistem peradilan pidana dan sistem pemidanaan. Pada

[67] Ferry Irawan Febriansyah, *Op.cit.*, Halaman 184.

dasarnya hak-hak warga negara yang terganggu akibat perbuatan melawan hukum seseorang akan diseimbangkan kembali.[68]

Faktor penegak hukum sering menjadi penyebab maraknya kejahatan siber (*cybercrime*). Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku, terlebih apabila kejahatan yang dilakukan memiliki sistem pengoperasian yang sangat rumit.[69]

Cybercrime adalah sebuah perbuatan yang tercela dan melanggar kepatutan di dalam masyarakat serta melanggar hukum, meskipun undang-undang secara khusus mengatur *cybercrime*, akan tetapi belum sepenuhnya dapat dipatuhi dan disadari oleh seluruh pengguna layanan teknologi informasi sebagai instrumen hukum. Oleh karena itu, peran masyarakat dalam upaya penegakan hukum terhadap *cybercrime* adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cybercrime*.[70]

Sampai saat ini, kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cybercrime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan *cybercrime*. Lack of information ini menyebabkan upaya penanggulangan *cybercrime* mengalami kendala, dalam hal ini kendala yang

[68] Mohammad Haidar Ali. (2012) " Cybercrime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang ITE (Perspektif Hukum Piidana Islam)". (Tesis) Fakultas Hukum Islam Uin Alauddin Makassar , Halaman 74.

[69] *Ibid*., Halaman 77.

[70] Ibid, Halaman 77.

berkenaan dengan penaatan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cybercrime*.[71]

Mengenai kendala yang pertama yaitu mengenai proses penaatan terhadap hukum. Jika masyarakat di Indonesia memiliki pemahaman yang benar akan tindak pidana *cybercrime,* maka baik secara langsung maupun tidak langsung masyarakat akan membentuk suatu pola penaatan. Pola penaatan ini dapat berdasarkan karena ketakutan akan ancaman pidana yang dikenakan bila melakukan perbuatan *cybercrime* atau pola penaatan ini tumbuh atas kesadaran mereka sendiri sebagai masyarakat hukum.[72]

Phising adalah upaya untuk mendapatkan informasi tentang data pribadi dengan menggunakan teknik *phising,* Data phising mencakup informasi pribadi (nama, alamat, jenis kelamin, tanggal lahir), informasi akun (nama pengguna dan kata sandi) dan informasi keuangan (informasi kartu kredit, akun). Aktivitas *phising* bertujuan untuk mengelabui orang agar secara sukarela memberikan informasi pribadi tanpa sepengetahuan mereka) Namun, informasi yang dibagikan akan digunakan untuk bertujuan jahat. Adapun beberapa alasan mengapa penipuan phising ini terus berlanjut dan menelan begitu banyak korban : [73]

1. Ketidaktahuan atau kurang pengetahuan tentang teknologi komputer memudahkan *phisher* untuk mendapatkan mangsanya.
2. Representasi yang menyesatkan dan palsu sangat mudah untuk memalsukan situs *web* dan gambar di internet dan pengguna biasa-biasanya tidak

[71] Ibid , Halaman 78.
[72] Ibid, Halaman 78.
[73] *Ibid.* , Halaman 78

menyadarinya. Salin dan tempel sederhana akan langsung membuat situ *web* seperti aslinya. *Phisher* juga dapat membuat situs *web* komentar pengguna yang sangat bagus, tetapi ini semua fiktif untuk meyakinkan calon korban.

3. Kurang memperhatikan indikator keamanan sangat sering, pesan yang ditampilkan tidak dibaca oleh pengguna. Pesan-pesan ini biasanya terlalu teknis untuk pengguna pemula, jadi selalu klik tombol "OK" untuk melanjutkan. Jenis praktik ini menawarkan keuntungan unik bagi *phisher* karena dapat menipu situs *web* dan memberikan informasi berharga dai korban

Faktor pengetahuan dan kesadaran pengguna terhadap ancaman serangan *phishing* mengenai pengetahuan pengguna untuk mengidentifikasi *website phishing*. Pengetahuan pengguna terhadap domain, link atau *website* palsu yang menyerupai aslinya sangat minim sehingga pengguna tidak menyadari bahwa telah menggunakan situs palsu.[74]

Salah satu faktor penyebab serangan *phising* di antaranya adalah karena minimnya pengetahuan pengguna akan pentingnya menjaga keamanan data. Pengguna dianggap tidak memiliki pengetahuan yang baik mengenai sistem komputer terutama membedakan domain yang resmi dan palsu. Faktor mengapa pengguna menjadi korban serangan phising adalah mayoritas pengguna memiliki pengetahuan yang minim terhadap ancaman kriminalitas *online*, tidak memiliki pengetahuan yang baik mengenai ancaman *phising* tidak memiliki strategi yang baik dalam mengenali serangan *phising*, fokus terhadap konten dibandingkan

[74] Irvan Hadi Ramadhan, 2022. *Analisis Ancaman Phising Dalam Layanan E-Commerce Prosiding Seminar Nasional Aplikasi Sains & Teknologi*, halaman 34.

indikator pada *website* dan tidak mengetahui prosedur layanan *online* yang dipakai sehingga terjebak ketika mendapatkan *email* dari layanan *online* yang mereka gunakan terkait informasi *maintenance* dan informasi- informasi lainnya yang dimanfaatkan *phisher* untuk mendapatkan data-data sensitif pengguna.[75]

Menyatakan bahwa pengguna merupakan faktor utama penyebab terjadinya *phishing*. Terdapat empat alasan mengapa phishing terjadi pada pengguna.

1. Semakin banyaknya *email* yang di terima pengguna, semakin besar peluang untuk ditipu.
2. Pengguna cenderung membuka *e-mail* dari orang yang mereka kenal. Pengguna yang memiliki hubungan dengan lebih dari satu lembaga bank dan melakukan lebih banyak transaksi online dapat berpeluang menjadi korban *e-mail phishing*.
3. Pengguna yang tidak menyadari akan bahaya serangan *phishing*.
4. Kebiasaan pengguna dalam menggunakan media, Kebiasaan pengguna mengecek *e-mail* pada saat sarapan pagi, hal ini mengakibatkan kurangnya rasa kecurigaan terhadap email *phishing*.

Faktor yang membuat pengguna menjadi korban serangan *phishing* adalah kurangnya pengetahuan korban mengenai informasi kejahatan *phishing* seperti halnya memdedakan nama domain yang resmi dengan yang palsu, selain itu pengguna tidak memperhatikan indikator keamanan *browser*. Pengguna tidak

[75] Rosalia Herlina Sutanti, *Perlindungan Hukum Terhadap Kejahatan Phising Pada Channel E-Banking Melalui Transfer Virtual Account (Studi Kasus Pada Pengguna Internet Banking)* , Jurnal Penelitian Bidang HukumUniversitas Gresik Volume 12 No 3, 2023 , halaman 935.

mengetahui strategi dalam menghadapi serangan *phishing* tidak memberitahukan *email phishing* yang diterima kepada pihak yang menerima. Selain itu, seringnya pengguna menggunakan kata sandi yang sama pada semua layanan di internet yang dapat meningkatkan risiko keamanan data bagi pengguna. [76]

Faktor penyebab terjadinya phising sudah sangat sering kita jumpai dimana pun, baik melalui sosial media, nomor *handphone* ataupun secara langsung. Biasanya penipu atau *cybercrime* akan berpura-pura mengaku dari pihak *e-commerce* resmi, lalu menwarkan hadiah palsu dengan iming-iming tertentu yang mengorbankan data pribadi korban bahkan hingga uang korban. [77]

Cybercrime sendiri biasanya memiliki trik untuk mengelabui korbannya. Namun sebenarnya apa saja faktor terjadinya berikut adalah :

a) Faktor pengetahuan pengguna yang minim perlunya edukasi kepada seluruh masyarakat untuk mengetahui adanya *phising*. Mengingat di era digitalisasi ini, menuntut seluruh orang mau tak mau harus pandai menggunakan digital. Untuk itu, perlu adanya sosialisasi dan pemberitahuan kepada seluruh masyarakat untuk mengetahui lebih memahami phising dengan di sosialisasikan nya gerakan tersebut, setidaknya masyarakat sudah mengetahui motif -motif penipuan.
b) Kebocoran data pengguna hal ini biasanya terjadi karena kesalahan kita sebagai pengguna yang perlu kita perhatikan akan data pribadi tidak bocor adalah jangan pernah memberi data pribadi seperti: ktp, sim, nomor rekening,

[76] Purnama Ramadani Silalah,dkk , *Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. Jurnal Manajemen, Bisnis dan Akuntansi* Vol.1, No.4 , 2022 , halaman 229.

[77] *Ibid*, halaman 229.

kode vertifikasi, dan data pribadi lainnya. Apabila data pribadi kita telah tersebarkan, orang tak bertanggung jawab dapat menggunakannya untuk tindakan yang tak bertanggung jawab. Selain itu, kebocoran data juga dapat disebabkan oleh *hacker*, atau peretas data. Orang yang dapat melakukan hal tersebut biasanya orang yang mengerti teknologi tetapi tidak memanfaatkan dengan baik. *Hacker* juga dapat memanfaat data kita melalui link atau situs situs *online*. Jadi, jika kalian mendapatkan link atau *email* yang tidak pasti isinya apa, jangan pernah membuka link tersebut karena itu bisa saja jebakan dari hacker untuk melakukan tindakannya.

c) Pengguna tergiur dengan hadiah palsu segelintir orang ada sudah paham adanya penipuan, namun masih saja terjebak dengan kasus tersebut. Hal ini biasanya disebabkan oleh, tergiurnya pengguna oleh iming-iming hadiah puluhan juta rupiah ataupun barang mewah lainnya. Itu dapat terjadi karena keadaan yang mendesak pengguna sehingga tergiur oleh hadiah palsu. Misalnya pengguna sedang butuh uang lalu ada penipu yang menawarkan hadiah puluhan juta dengan syarat yang sangat mudah. Tindakan tersebut harus bijak kita hadapi dalam keadaan sesulit apa pun kita harus tetap berfikir rasional.

d) Tingginya angka pengangguran dan kemiskinan, sempitnya lapangan kerja dan persaingan yang ketat membuat sebagaian orang berpikiran pendek untuk melakukan tindakan kejahatan dengan hanya bermodal kan janji palsu, para penipu dapat melancarkan aksinya. Disini perlu perhatian pemerintah terhadap tindakan phising tersebut dengan memperbanyak lapangan pekerja

dan mengurangi angka kemiskinan, akan sejalannya dengan berkurangnya tindakan penipuan.

e) Sistem keamanan dan kurang tegasnya kebijakan pemerintah kasus kebocoran data pada aplikasi *e-commerce* menunjukkan sistem keamanan *e-commerce* Indonesia yang tidak aman. Kurang tegasnya kebijakan pemerintah dalam hal ini menjadikan kesempatan bagi para *cyber crime*. Padahal di Indonesia sendiri sudah ada beberapa undang-undangan dan menteri kominfo yang mengawasi keamanan transaksi *e-commerce*. Namun kebijakan tersebut belum sepenuhnya berhasil, hal itu dapat dibuktikan dengan kasus-kasus penipuan yang marak terjadi. Kita sebagai masyarakat biasa, apabila mendapatkan kasus tersebut kita berhak melaporkan tindakan tersebut kepada pihak berwajib guna mengurangi angka penipuan.

Ada berbagai penipuan online dengan teknik yang sama yaitu pelaku mencoba mengelabui pengguna dengan menjadi pihak dari lembaga ternama dan *website* yang menyerupai lembaga terpercaya melalui *e-mail. Teknik* yang digunakan yaitu teknik penipuan *marketing* dengan membujuk pengguna agar membuka situs palsu. Pengguna akan mendapatkan *e-mail* promosi atau terdapat masalah sehingga pelaku membujuk pengguna untuk melakukan *login* pada *website* palsu yang telah dikirimkan. Pengguna yang mendapatkan *e-mail* akan percaya dan tertarik untuk membuka *website* yang dikirim pelaku melalui *e-mail*. Faktor penyebab terjadinya ancaman serangan *phishing* dikarenakan minimnya pengetahuan pengguna dalam menjaga keamanan data, minimnya pengetahuan pengguna terhadap ancaman kriminalitas *online*, kurangnya pengetahuan

mengenai ancaman *phishing*.[78]

Bahwa pengetahuan proses pengguna dan pengetahuan konseptual dapat mempengaruhi perilaku pengguna dalam menghindari ancaman *phishing*. Pengetahuan prosedural pengguna dinilai berdasarkan kemampuan pengguna dalam mengidentifikasi situs *web phishing* dari lima URL yang disediakan dan pengetahuan konseptual pengguna dinilai dari bagian URL mana yang akan menunjukkan apakah situs *web* tersebut adalah *phishing* atau tidak. Penyebab terjadinya *phishing* yaitu sistem keamanan *platform* yang lemah, gambar halaman *website/platform* sangat mudah untuk ditiru, kurangnya informasi tentang serangan *phishing* yang di hadapi pengguna, serta kurangnya pengetahuan pengguna tentang kejahatan *phishing*.[79]

C. Pencegahan Mengenai Kejahatan Dunia Maya Bermodus Pengelabuan (*Phising*) Dalam Bentuk Mengirimkan Suatu Link

Membahas aturan hukum *cybercrime* merupakan suatu hal yang memiliki tantangan tersendiri. Hal ini dikarenakan perarturan perundang-undangan yang mengatur tentang kejahatan *cyber* di Indonesia masih seumur jagung. Aturan perundang-undangan telah dituangkan dalam Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Sebelum mengkontruksi aturan-aturan hukum nasional secara detail penusunan perangkat hukum tentang *cybercrime* yang dihasilkan oleh the G-8 dalam *communique* tanggal 9-10 desember 1997. Dalam pertemuan itu terdapat 10 butir asas yang dapat dilakukan

[78] *Ibid* , Halaman 35
[79] *Ibid* , Halaman 35

dalam mengantisipasi tindak pidana yang dimaksud yaitu : [80]

a. Tidak akan ada tempat perlindungan yang aman bagi mereka yang penyalahgunakan teknologi informasi.
b. Penyidikan dan penuntutan *high-tech* international *crime* harus di koordinasikan diantara negara-negara yang menarik perhatian tanpa melihat dimana akibat yang merugikan terjadi.
c. Aparat penegak hukum harus dilatih dan dilengkapi dalam menghadapi *high-tech crime*.
d. Sistem hukum harus melindungi kerahasian, integritas, dan keberadaan data dan system dari perbuatan yang tidak sah dan menjamin bahwa penyalahgunaan yang serius harus dipidana.
e. Sistem hukum harus mengizinkan perlindungan dan akses cepat terhadap data elektronik yang sering kali kritis bagi suksesnya penyidikan kejahatan.
f. Pengaturan mutual *assistance* harus dapat menjamin pengumpulan dan pertukaran alat bukti tepat pada waktunya, dalam kasus-kasus yang berkaitan dengan *high-tech crime*.
g. Akses elektronik lintas batas oleh penegak hukum terdapat keberadaan informasi yang bersifat umum, tidak memerlukan pengesahan dari negara dimana data tersebut berada.
h. Standar forensik untuk mendapatkan dan membuktikan keaslian data elektronik dalam rangka penyidikan tindak pidana dan penuntutan harus

[80] Maskun, 2013. *Kejahatan Siber Cyber Crime*, Jakarta : Prenada Media Group, Halaman 41.

dikembangkan dan digunakan.

i. Untuk kepentingan praktis, sistem informasi dan telekomunikasi harus didesain untuk membantu mencegah dan mendeteksi penyalahgunaan jaringan, dan harus memfasilitasi pencarian penjahat dan pengumpulan bukti.

j. Bekerja di lingkungan ini harus berkoordinasi dengan pekerja lain di era informasi yang relavan untuk menghindari duplikasi kebijakan.

Kejahatan bisa terjadi di mana saja bahkan di dunia maya. Jadi pengguna harus selalu waspada dalam menggunakan internet karena masih banyak orang yang belum memiliki pengetahuan yang cukup untuk mengakses internet dan oknum-oknum yang tidak bertanggung jawab mencoba memanfaatkan orang-orang tersebut. Ketidaktahuan pengguna mengenai hal-hal yang ada di internet yang membuat pengguna terjerumus dalam korban tindakan kejahatan dunia maya. Oleh karena itu, saat bertukar pesan dengan orang asing atau mendapatkan informasi yang dikirim oleh orang lain pengguna harus selalu waspada dan memastikan bahwa pengguna dapat memverifikasi keakuratan informasi yang diberikan. Pengguna harus selalu memastikan bahwa informasi yang dikirimkan oleh orang lain benar atau tidak melalui situs-situs resmi dan juga jangan mudah percaya apabila menerima informasi bahwa pengguna memenangkan suatu hadiah dan orang tersebut mengirimkan sebuah link karena bisa saja link tersebut terdapat hal-hal yang berbahaya yang dapat mengancam keselamatan perangkat dan pengguna.

Phishing merupakan upaya untuk mendapatkan informasi sensitif pengguna

melalui *e-mail* atau situs *web* palsu dengan cara meniru tampilan situs *web* yang asli atau resmi. Pelaku menggunakan *e-mail*, spanduk, untuk mengelabui pengguna agar mengarahkannya ke situs *web* palsu dan meminta mereka memberikan informasi pribadi.

Upaya selanjutnya yang dilakukan oleh negara adalah meningkatkan kesadaran masyarakat dalam menggunakan media sosial, menggunakan internet dengan dengan bijak sehingga tindakan pencegahan yang terjadi terkait kejahatan dunia maya dapat di lakukan dengan baik. Solusi selanjutnya yang dapat dilakukan oleh negara adalah meratifikasi beberapa kebijakan-kebijakan antar negara untuk menangani persoalan-persoalan terkait *cybercrime*. [81]

Negara hukum merupakan istilah yang meskipun kelihatan sederhana, namun mengandung muatan sejarah pemikiran yang relatif panjang. Di Indonesia sendiri ada beberapa optimalisasi penegakan hukum terkait dengan kejahatan dunia maya yaitu dengan mengoptimalkan undang-undang tentang informasi dan transaksi elektronik yang sudah ada. Akan tetapi hal ini belum maksimal, dibutuhkan pembaharuan hukum setiap saat untuk mengatasi persoalan tersebut karena persoalan tersebut merupakan persoalan yang serius yang harus ditangani. Korelasi penegakan hukum yang represif dan preventif dalam penegakan hukum dengan dasar undang-undang yang tepat dapat memberikan penyelesaian kepada persoalan kejahatan yang ada di dunia maya. Selain itu ada beberapa kasus juga dilakukan penyelesaian secara *restorative Justice* sehingga tidak semua persoalan-persoalan yang ada di dunia maya harus diselesaikan di muka hukum. Hal tersebut

[81] Ferry Irawan Febriansyah, dkk , *Op.cit* , halaman 193

merupakan sinergi yang baik antara perundang-undangan yang ada dengan penegakan hukum yang dilakukan.[82]

Peraturan perundang-undangan yang mengatur tentang kejahatan didunia maya terutama ini membahas tentang *cyber crime* dalam bentuk *phising* tersebut. *Cyber Crime* dalam bentuk *phising* saat ini di Indonesia dimungkinkan dapat dikenakan 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. *Cyber crime* dalam bentuk *phising* ini juga dapat dikenakan 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 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.[83] Pasal 35 dan Pasal 28 berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang dirumuskan sebagai berikut:

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 agar Informasi

[82] Jimly Asshiddiqie, 2017. "Hak Asasi Manusia Dalam Konstitusi Indonesia" , Kencana : Jakarta, Halaman 17.

[83] Ardi Syahpura Gulo , Op.cit., Halaman 73

Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 28 setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. *Cyber crime* dalam bentuk *phising* ini merupakan kejahatan siber yang tidak hanya melakukan pemalsuan data pada sebuah *website* palsu yang tampilannya menyerupai *website* aslinya, tetapi memiliki suatu tujuan untuk mendapatkan identitas milik orang lain untuk digunakan secara ilegal tanpa diketahui oleh pemilik asli identitas tersebut dan dalam pasal 35 hanya memuat unsur pemalsuan data pada sebuah *website* yang membuat seolah-olah *website* tersebut asli namun telah dideface seperti *website* aslinya dan tidak memuat unsur maksud dan tujuan.[84]

Dapat disimpulkan *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 di deface atau diubah mirip dengan yang asli resminya dengan cara menggunakan *email* yang mengarahkan ke situs *web* palsu guna mendapatkan informasi pribadi rahasia pengguna orang lain, sehingga muncul sebuah pertanyaan apakah dalam menangani *cyber crime* 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

[84] Ardi Syahpura Gulo , Op.cit., Halaman 73.

dan Transaksi Elektronik dan juga mungkin dapat dikenakan dengan pasal-pasal diluar Undang-Undang Informasi dan Transaksi Elektronik seperti KUHP. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini selain membuat aturan tentang *phising*, Undang-undang ini juga membuat aturan terhadap perbuatan-perbuatan kejahatan yang merugikan orang lain yang terjadi didunia maya melalui transaksi elektronik yang dapat diketahui bahwa perkembangan teknologi informasi semakin pesat.[85]

Pengaturan hukum terhadap *cyber crime* dalam bentuk *phising* berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah tidak dapat dikenakan sanksi pidana karena di dalam 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 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. Karena *phising* itu sendiri perbuatan satu kesatuan antara membuat situs yang seolah-olah mirip situs aslinya tetapi situs tersebut palsu dan juga melakukan tindakan kebohongan untuk mengarahkan orang lain mengakses ke situs palsu tersebut untuk memasukkan informasi pribadi rahasia dan kemudian diketahui oleh pelaku *phising*. Oleh sebab itu, telah terjadinya kekosongan hukum mengenai

[85] *Ibid.,* Halaman 73.

pengaturan hukum terhadap *cyber crime* dalam bentuk *phising* berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Kebijakan Hukum terhadap *cyber crime* dalam bentuk phising berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik adalah dilakukannya perubahan terhadap Undang-Undang tentang ITE tersebut dengan merumuskan konsep *phising* dengan jelas dan tegas serta merubah isi dan unsur pada Pasal 35 agar kemudian Pasal 35 tersebut dapat diterapkan dan/atau dikenakan terhadap pelaku *cyber crime* dalam bentuk *phising*[86]

Berdasarkan pengalaman empiris sebelum diberlakukan UU ITE , aturan hukum yang paling sering digunakan di indonesia ketika terjadi *cyber crime* adalah aturan hukum positif (KUHP dan KUHAP). KUHP khususnya masih dipandang sebagai landasan hukum yang cukup memadai, meskipun jika harus jujur bahwa hal tersebut tidak sepenuhnya benar. Akan tetap, tidak ada pilihan lain di tengah kekosongan hukum dibidang teknologi dan informasi.

Dalam merumuskan delik pidana pada pidana phising sendiri, mengacu pada pembahasan mengenai phising sebelumnya, beberapa pasal dalam KUHP yang dijadikan acuan dalam menjatuhkan pidana *phising* yaitu terdapat pada pasal 378, Pasal 263, dan pasal 362 KUHP. Pada pasal 378 KUHP mengenai penipuan yang mengatakan bahwa barang siapa secara melawan hukum menggunakan nama atau martabat palsu untuk menguntungkan diri sendiri atau orang lain dengan tipu

[86] *Ibid*., Halaman 79.

muslihat atau rangkaian kebohongan yang bertujuan menggerakan orang tersebut untuk menyerahkan sesuatu atau memberi sesuatu diancam karena penipuan dengan pidana penjara paling lama empat tahun, maka dari itu pembahasan berikutnya penulis akan membedah mengenai unsur-unsur yang terdapat pada pasal 378 KUHP sehingga dapat dikatakan sebagai pasal yang menjadi salah satu acuan dalam menjatuhi pidana *phising* itu sendiri. Pertama mengenai unsur Barang siapa, yang dimaksud dengan unsur tersebut adalah mengenai subjek hukum itu sendiri, yang mana subjek hukum ini dapat berupa orang maupun badan hukum yang dinilai dapat mempertanggungjawabkan perbuatannya menurut hukum, lalu yang kedua terdapat unsur menguntungkan diri sendiri jika sudah berbicaara mengenai tindak pidana *phising* dapat disimpulkan kebanyakan pelaku *phising* menggunakan kemampuan mereka demi meraup keuntungan dari orang lain walaupun kebanyakan tidak dalam bentuk uang ataupun barang.[87]

Unsur memakai nama palsu atau martabat palsu dengan tipu muslihat atau rangkaian kebohongan, seringkali ditemukan pelaku tindak pidana *phising* menggunakan nama ataupun martabat palsu yang bertujuan untuk mengecoh korbannya telah dijelaskan bahwa pelaku *phising* bertujuan untuk memancing korbannya dengan kata lain pelaku sebisa mungkin harus memakai nama ataupun martabat sebuah organisasi atau perusahaan besar lalu isi *e-mail* maupun *website* palsu tersebut juga harus didesain sedemikian rupa agar mirip dengan aslinya, hal tersebut bertujuan agar korban dapat dengan mudah percaya mengenai keaslian

[87] Vikran Fasyadhiyaksa Putra Y, *Modus Operandi Tindak Pidana Phising Menurut UU ITE*, Jurist Diction 2021 Vol. 4 No. 6, halaman 17.

email atau *website* palsu milik pelaku *phising* yang terakhir unsur menggerakan orang lain untuk menyerahkan suatu barang meskipun dalam konteks *phising* yang menjadi sasaran bukan merupakan sebuah barang melainkan data pribadi korban, namun tetap saja hal tersebut dianggap memenuhi unsur pada pasal 378 KUHP karena pada dasarnya data pribadi juga merupakan sebuah benda yang tidak berwujud namun dapat dibuktikan keberadaannya.[88]

Cyber crime adalah tindakan yang dilarang oleh Allah swt., karena Allah swt. tidak menyukai orang-orang yang membuat kerusakan yang memudharatkan orang lain. Perusakan dalam bentuk apapun tidak dibenarkan, karena perusakan merupakan tindakan yang bertentangan dengan nilai-nilai universal. Allah swt. secara tegas berfirman dalam Q.S. Al-Maidah/5: 64 sebagai berikut: Dan orang-orang Yahudi berkata: “Tangan Allah terbelenggu”. Sebenarnya tangan merekalah yang dibelenggu dan merekalah yang dilaknat disebabkan apa yang telah mereka katakan itu. Padahal kedua tangan Allah terbuka; Dia memberi rezki sebagaimana dia kehendaki. Dan (Alquran) yang diturunkan kepadamu dari Tuhanmu itu pasti akan menambah kedurhakaan dan kekafiran bagi kebanyakan mereka. Dan Kami timbulkan permusuhan dan kebencian di antara mereka sampai hari kiamat. Setiap mereka menyalakan api peperangan, Allah memadamkannya dan mereka berbuat kerusakan dimuka bumi dan Allah tidak menyukai orang-orang yang membuat kerusakan.

Ayat tersebut menegaskan bahwa tindakan perusakan merupakan sesuatu yang dilarang oleh Allah swt. baik dalam bentuk apapun dan di manapun, tetap

[88] *Ibid*, halaman 17.

tidak dibenarkan. Tindakan para hacker menjadi bagian dari perbuatan dan tindakan yang sangat dominan dilakukan oleh para pelaku kejahatan *cyber crime* yang dilarang sebagaimana ayat tersebut. Landasan larangan tersebut mengarah kepada hal-hal yang merugikan dan meresahkan orang lain.

Perintah Allah untuk berkata jujur dalam surah Al Ahzab Ayat 70-71 yang berbunyi: . "Hai orang-orang yang beriman, bertakwalah kamu kepada Allah dan katakanlah perkataan yang benar. niscaya Allah memperbaiki bagimu amalan-amalanmu dan mengampuni bagimu dosa-dosamu. Dan barangsiapa mentaati Allah dan Rasul-Nya, maka sesungguhnya ia telah mendapat kemenangan yang besar." (Al-Ahzab:70-71). Berdasarkan ayat Al-Quran dan diatas, Allah memerintahkan kepada hamba-hamba-Nya yang beriman tetap bertaqwa kepada-Nya dan hendaklah mereka mengucapkan perkataan yang benar, yang jujur, tidak bengkok, tidak pula menyimpang. Nabi Muhammad SAW mengkategorikan orang yang berbuat curang dalam muamalah adalah bukan termasuk golongan kaum muslimin.

Pada saat inilah pelaku memanfatkan ketidakpedulian pengguna untuk mendapatkan informasi pribadi. Phishing bekerja dengan cara memanipulasi tautan sehingga terlihat mirip dengan alamat situs asli. Trik yang umum digunakan pelaku *phishing* adalah menggunakan subdomain palsu. Pelaku akan membujuk pengguna untuk mengungkapkan informasi pribadinya melalui situs palsu yang menyerupai situs asli melalui *e-mail* yang pelaku kirim, halaman situs *web* dibuat semirip mungkin dengan situs resmi sehingga pengguna akan percaya dan memasukan data-data pribadinya.

Kebijakan Penanggulangan kejahatan dan implementasi kebijakan hukum

pidana bukanlah merupakan suatu kebijakan yang berdiri sendiri. Kebijakan hukum pidana merupakan bagian dari pencegahan untuk menanggulangi kejahatan dalam rangka menyesejahterakan masyarakat. Tindakan untuk mengatur masyarakat dengan sarana hukum pidana terkait erat dengan berbagai kebijakan dalam suatu proses kebijakan sosial yang mengacu pada tujuan yang lebih luas. Upaya pencegahan kejahatan adalah dengan tujuan utama perlindungan masyarakat untuk mencapai kesejahteraan masyarakat secara garis besar dapat dibagi dalam dua jalur yaitu jalur penal dan non-penal. Termasuk juga dengan pencegahan tindak pidana penipuan menggunakan metode *phising* ini melindungi masyarakat yang menjadi korbannya. upaya pencegahan dapat ditempuh dengan: [89]

1) Penerapan hukum pidana
2) Pencegahan tanpa pidana
3) Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui media masa.

Untuk kategori pertama dikelompokkan ke dalam upaya pencegahan kejahatan melalui penal, sedangkan kedua dan ketiga termasuk upaya penanggulangan kejahatan melalui jalur non-penal. Upaya melalui jalur penal merupakan upaya represif yang dalam pelaksanaannya mengandung keterbatasan sehingga perlu diimbangi dengan pendekatan non-penal yang cenderung merupakan upaya preventif. Upaya pencegahan kejahatan perlu ditempuh dengan pendekatan kebijakan secara terpadu (integral), dimana terdapat keterpaduan antara

[89] Zainab Ompu Jainah ,2018. Kapita Selekta Hukum Pidana, Tanggerang : Tira Smart , Halaman 68.

kebijakan kriminal dengan kebijakan sosial juga pencegahan dengan sarana penal dan non-penal.

Pada umumnya asas legalitas mengandung tiga makna sebagai pedoman kuasa berlakunya hukum pidana menurut waktu, yakni :

1. Tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal ini terlebih dahulu belum dinyatakan dalam suatu aturan undang-undang

2. Untuk Menentukan adanya perbuatan pidana tidak boleh digunakan analogi

3. Aturan-aturan hukum pidana tidak berlaku surut. [90]

Ada beberapa cara yang bisa digunakan untuk meminimalisir kasus phising antara lain :

1. Mengubah *password* secara rutin
2. Menggunakan *sofware* atau *tools* untuk menghindari *phising*.
3. Jangan mudah percaya dengan orang yang baru dikenal.
4. Melaporkan pada pihak berwajib.

Salah satu cara yang bisa dilakukan yaitu dalam mengubah *password* secara rutin. Selain itu pastikan juga bahwa anda membuat *password* dengan kombinasi yang rumit sehingga sulit ditebak oleh orang lain. Selain itu jangan pernah memberikan *password* kesembarang orang karena hal ini sangat berbahaya sangat penting untuk menjaga kerahasiaan dari *password* setiap akun yang dimiliki. Saat ini, sudah ada beberapa *tools* atau *software* yang bisa digunakan untuk meminimalisir terjadinya tindak kejahatan melalui internet tidak ada salahnya untuk

[90] Andi Sofyan , 2016. Hukum Pidana , Makassar : Pusaka Pena , Halaman 37.

menginstal aplikasi tersebut pada komputer. Selain itu, ada banyak kasus terjadi pada kasus *phising* dialurkan karena para korban terlau mudah percaya dengan orang yang baru di kenal bahkan pada orang yang tidak dikenal juga. Jadi jangan mudah percaya terhadap orang yang baru dikenal.

Formulasi ketentuan pidana yang terbagi dalam delik formil dan delik materil pada gilirannya akan menunjukkan perbedaan pendekatan dalam menganalisis ada atau tiadanya suatu tindak pidana. Dalam mempraktikkan cara mengatasi pencegahan berikut ini bila pernah menjadi korban sehingga kejadian buruk tersebut tidak terulang lagi.[91]

1. Mengambil kembali data-data yang sempat diretas peretasan data dan kerugian lainnya yang disebabkan *cyber crime* pasti membuat Anda panik. Namun, anda tetap harus berpikir jernih agar tidak mengalami kerugian secara masif. Sebaiknya anda lekas berupaya mengambil kembali data-data yang sempat diretas. Hubungi tim support IT untuk membantu mengembalikan data-data yang diretas pelaku *cyber crime*. Bila data-data Anda berhasil diselamatkan, barulah Anda bisa melakukan beberapa cara mengatasi *cyber crime* lainnya sebagai tindak lanjut.
2. Menggunakan gadget untuk kepentingan pribadi penggunaan dari gadget memiliki dampak positif maupun negatif dalam kehidupan manusia. Penggunaan gadget yang dilakukan untuk kepentingan bersama memang rentan membuat anda menjadi korban *cyber crime.* Karena bukan mustahil bila akun anda akan disalahgunakan oleh oknum tak bertanggung jawab.

[91] Imron Rosyadi , 2022. Hukum Pidana. Surabaya : Revka Prima Media , Halaman 71.

Alangkah lebih baik bila Anda menggunakan gadget untuk kebutuhan pribadi. Lindungi gadget dengan *username* dan *password* supaya data-data penting Anda tidak bisa diakses sembarang orang.

3. Memprioritaskan penggunaan software asli anda tak perlu ragu menyiapkan budget demi mendapatka*n software* asli. Karena biasanya *software* bajakan sudah terkontaminasi *malware* atau jenis virus lainnya. Meskipun harga *software* asli lebih mahal, kualitasnya tentu sebanding dengan biaya yang mesti Anda keluarkan. Selain itu, Anda juga bisa mendapatkan update otomatis secara resmi jika menggunakan *software* asli.
4. Melakukan update *software* secara rutin jangan mengabaikan manfaat update *software* secara rutin. Ternyata aktivitas ini merupakan salah satu cara mengatasi *cyber crime* yang ampuh. *Software* terbaru biasanya sudah dilengkapi proteksi keamanan yang lebih baik dari versi *software* sebelumnya. Sehingga penggunaan *software* versi terbaru akan melindungi data-data Anda dari incaran pelaku *cyber crime*. Risiko data hilang akibat virus pun semakin kecil kalau anda rajin melakukan *update software.*
5. Mengaktifkan data encryption manfaat data encryption untuk melindungi data-data penting memang tak boleh dianggap remeh. Anda wajib mengaktifkan data encryption pada jaringan lokal seperti LAN atau nirkabel di rumah dan kantor. Aktivasi data *encryption* akan mencegah akses yang berstatus tidak sah serta meminimalkan risiko penyadapan teks.
6. Menggunakan hosting yang aman anda mesti cermat memilih layanan

hosting yang aman ketika memilih *website.* Biasanya layanan *hosting* berkualitas dilengkapi sistem proteksi khusus untuk melindungi data dari serangan *malware.* Perlindungan ini akan membuat data-data *website* Anda tidak mudah diretas dan disalahgunakan pelaku *cyber crime*.[92] Mengingat bahwa Tindak pidana *cybercrime* melalui *phising* memakan korban yang tidak sedikit jumlahnya, terutama dari sisi finansial. Sebagian besar korban hanya bisa menyesali apa yang sudah terjadi. Ada yang perlu dilakukan sekarang adalah melakukan pencegahan terhadap kemungkinan-kemungkinan yang dapat merugikan terhadap kejahatan tersebut, maka pencegahan yang dilakukan adalah:

a. Memberikan pengetahuan dan pemahaman baru terhadap *Cyber crime* atau kejahatan dunia maya memlalui *phising* dan dunia internet.

b. Menggunakan pemikiran dari sisi *hacker* untuk melindungi sistem setiap pengguna teknologi.

c. Menutup hal-hal yang menjadi kelemahan pada sistem sehingga pelaku *cyber crime* melalui *phising* tidak mampu menjalankan aksi jahatnya.

d. Menentukan kebijakan-kebijakan dan aturan-aturan yang bisa melindungi sistem para pengguna teknologi dari orang-orang yang tidak berwenang untuk mengakses sistem pribadi

Beberapa cara untuk pencegahan serangan phising [93]

a. Kriptografi : seni menyandikan data. Data yang dikirimkan

[92] *Ibid.*, Halaman 71
[93] *Ibid.*, Halaman 71

disandikan terlebih dahulu sebelum dikirim melalui internet di komputer tujuan data dikembalikan ke bentuk aslinya sehingga dapat dibaca dan dimengerti oleh penerima. Hal ini dilakukan supaya pihak-pihak penyerang tidak dapat mengerti isi data yang dikirim.

b. *Internet Farewell*: untuk mencegah akses dari pihak luar ke sistem internal. *Firewall* dapat bekerja dengan 2 cara, yaitu menggunakan *filter* dan *proxy. Firewall filter* menyaring komunikasi agar terjadi seperlunya saja, hanya aplikasi tertentu saja yang bisa lewat dan hanya komputer dengan identitas tertentu saja yang bisa berhubungan. *Firewall proxy* berarti mengizinkan pemakai dalam untuk mengakses internet seluas-luasnya, tetapi dari luar hanya dapat mengakses satu komputer tertentu saja.

c. Menutup *service* yang tidak digunakan.

d. Adanya sistem pemantau serangan yang digunakan untuk mengetahui adanya tamu/seseorang yang tak diundang *(intruder)* atau adanya serangan *(attack).*

e. Melakukan *back up* secara rutin.

f. Adanya pemantau integritas sistem. Misalnya pada sistem UNIX adalah program *tripwire.* Program ini dapat digunakan untuk memantau adanya perubahan pada berkas.

g. Perlu adanya *cyberlaw: Cyber crime* belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting

adanya perangkat hukum khusus mengingat karakter dari *cyber crime* ini berbeda dari kejahatan konvensional.

h. Perlunya dukungan lembaga khusus: Lembaga ini diperlukan untuk memberikan informasi tentang *cyber crime,* melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *cyber crime.*

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Modus kejahatan pengelabuan (*phising*) dalam bentuk mengirimkan suatu link Pengguna akan di bawa ke situs *web* berbahaya yang telah dimodifikasi oleh pelaku, *phising* juga dapat terjadi di berbagai *platform* , termasuk media sosial, situs *web* dan juga aplikasi lainnya.
2. Faktor penyebab terjadinya kejahatan dunia maya bermodus pengelabuan (phising) dalam bentuk mengirimkan suatu link yaitu kurangnya pengetahuan dan kesadaran pengguna terhadap ancaman serangan *phishing* mengenai pengetahuan pengguna untuk mengidentifikasi *website* phishing. Pengetahuan pengguna terhadap domain, link atau *website* palsu yang menyerupai aslinya sangat minim, sehingga pengguna tidak menyadari bahwa telah menggunakan situs palsu.
3. Upaya pencegahan kejahatan perlu ditempuh dengan pendekatan kebijakan secara terpadu (integral), dimana terdapat keterpaduan antara kebijakan kriminal dengan kebijakan sosial juga pencegahan dengan sarana penal dan non-penal. Ada beberapa cara yang bisa digunakan untuk meminimalisir kasus phising antara lain
    1. Mengubah password secara rutin
    2. Menggunakan sofware atau tools untuk menghindari phising.
    3. Jangan mudah percaya dengan orang yang baru dikenal.
    4. Melaporkan pada pihak berwajib.

B. Saran

1. Kepada masyarakat di sarankan kedepannya lebih berhati-hati dalam menggunakan social media khususnya jika menerima suatu link harus memeriksa terlebih dahulu sumber ke akuratan suatu link tersebut agar terhindar dari terjadinya kejahatan dunia maya bermodus phising (pengelabuan).
2. Perkembangan teknologi informasi yang sangat cepat akan berpengaruhi juga pada perkembangan jenis dan pola kejahatan. Tindak pidana *cybercrime* yakni *phising* (pengelabuan), Kini berkembang dengan memanfaatkan teknologi canggih khususnya internet , dengan demikian disarankan agar dilakukannya pengkajian dalam sehingga hukum pidana dapat menjangkau kejahatan phising di dunia maya.
3. Kepada pemerintah selaku pembentuk kebijakan, kedepannya lebih memperhatikan masyarakat yang dalam hal penggunaan sosial media dengan cara memberikan edukasi terkait kejahatan phising tersebut agar kedepannya masyarakat lebih berhati-hati khususnya dalam mengakses suatu link.

Daftar Pustaka

A. Buku

Andi Sofyan , 2016. *Hukum Pidana* , Makassar : Pusaka Pena

A.S. Alam dan Amir Ilyas, 2018. *Kriminologi Suatu Pengantar*, Jakarta : Prenadamedia Group

Awaludin Marwan, 2022. *Pengantar Filsafat Hukum* , Yogyakarta : Thafa Media

Bima Guntara , 2020. *Cybercrime : penghinaan dan pencemaran nama baik melalui dunia maya* , Jawa tengah : Cv. Pena Persada

Efvy zam, 2014. *Phising*, Jakarta : Mediakita.

Faisal, 2021. *Hukum Pidana* , Jakarta : Kencana

Ida Hanifah dkk, 2018. *Pedoman Penulisan Tugas Akhir Mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara (UMSU)*, Medan : CV. Pustaka Prima

Imron Rosyadi , 2022. *Hukum Pidana*. Surabaya : Revka Prima Media

Jimly Asshiddiqie, 2017. *Hak Asasi Manusia Dalam Konstitusi Indonesia* , Kencana : Jakarta

Maskun, 2013. *Kejahatan Siber Cyber Crime*, Jakarta : Prenada Media Group

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

Nursariani Simatupang & Faisal, 2017. *Kriminologi* Medan:CV. Pusaka Prima

Sahat Maruli T. Situmeang, 2021. *Buku Ajar Kriminologi* , Depok : PT. Rajawali Buana Pusaka

Teguh Prasetyo,2019. *Hukum Pidana* , Depok : PT. Rajagrafindo Persada

Zainab Ompu Jainah ,2018. *Kapita Selekta Hukum Pidana* , Tanggerang : Tira Smart

B. Jurnal

Annisa Indah Pertiwi, *Tindak Pidana Cyberspace dalam akses illegal terhadap bocornya data informasi public,* Jurnal Ilmu Hukum Vol. 1 No 2 , 2023.

Andysah Putera Utama Siahaan, Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia, Jurnal Ilmiah, Vol. 5 No. 1 , 2018

Andrew Christian Banjarnahor, *Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo,* Hermeutika : Jurnal Ilmu Hukum, Vol. 6 , No. 1 , 2022.

Ardi Saputra Gulo , *Cyber crime dalam bentuk phising berdasarkan undang-undang informasi dan tranksasi elektronik* , Jurnal *Of Criminal* , Vol. 1 No. 2, 2020.

Endang Prastini , *Kebijakan Kriminal Pemerintah Terhadap Kejahatan Dunia Maya (Cybercrime) di Indonesia* , jurnal surya kencana 2, Vol 5, No 2, 2018

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

Irvan Hadi Ramadhan , Analisis Ancaman Phising Dalam Layanan *E-commerce* , Jurnal SNAST, 2022

Kadek Odie Kharisma Putra. "*Tindakan Kejahatan Pada Dunia Dalam Bentuk Phising*" Jurnal *cybersccurity* dan Forensik Digital, Vol. 5 No 2, 2022.

Mohammad Haidar Ali. (2012) " *Cybercrime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang ITE (Perspektif Hukum Piidana Islam)*". (Tesis) Fakultas Hukum Islam Uin Alauddin Makassar

Mohd. Yusuf DM. "*Kegiatan Phising dalam Dunia Cyber crime dan system hukum di Indonesia"* Jurnal pendidikan dan konseling , Vol. 4 No 5, 2022.

_____. *Analisis Terhadap Modus-Modus Dalam Hukum Cyber Crime,* Jurnal Hukum, Politik Dan ilmu Sosial Vol, No.2, 2022.

Mhd. Teguh Syuhada Lubis, *Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Penyeludupan Manusia* , De Lega Lata, Volume 2, Nomor 1,2017.

Ni Komang Arista Tri Wahyuni, dkk, *Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zhiphiser, Shellphish dan Whphiser* , Jurnal Teknik Mesin Elektro Dan Ilmu Computer , Vo. 3 no. 1, 2023.

_____. "*Kegiatan Phising Dalam Dunia Cyber Crime Dan System Hukum di Indonesia"* Jurnal Pendidikan Dan Konseling, 2022, Vol. 4 No. 5

Nur Fatimah. "Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime" Jurnal *of Education And Information Communication Technology*, Vol. 1 No. 1,2017

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

_____. *Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. Jurnal Manajemen, Bisnis dan Akuntansi* Vol.1, No.4 , 2022.

Rosalia Herlina Sutanti, *Perlindungan Hukum Terhadap Kejahatan Phising Pada Channel E-Banking Melalui Transfer Virtual Account (Studi Kasus Pada Pengguna Internet Banking)* , Jurnal Penelitian Bidang HukumUniversitas Gresik Volume 12 No 3, 2023

Samosir, A. (2020). "*Penegakan Hukum Tindak Pidana Narkotika ditinjau dari Perspektif Kriminologi"*. Logika: Jurnal Penelitian Universitas Kuningan, 11c(02)

Vikran Fasyadhiyaksa Putra Y, *Modus Operandi Tindak Pidana Phising Menurut UU ITE,* Jurist Diction 2021 Vol. 4 No. 6.

C. Perundang-Undangan

Kitab Undang-Undang Hukum Pidana

Undang –Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

D. Internet

Kompas TV, "Bareskrim Tangkap 13 Tersangka Penipuan Modifikasi APK dan Link *Phising*" https://www.kompas.tv/video/369886/bareskrim-tangkap-13-tersangka-penipuan-modifikasi-apk-dan-link-phishing, diakses pada tanggal 20 Juli 2023 Pukul 20.26 WIB.

Mekarsign, *Apa Itu Kebocoran Data Dan Penyebab Dan Cara Mengatasinya*, https://mekarisign.com/blog/apa-itu-kebocoran-data/ di akses melalui tanggal 20 Juli 2023 pukul 21.00 wib.