MODUS OPERANDI TINDAK PIDANA *PHISHING* DAN PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA *PHISHING* DI SURABAYA

(STUDI PUTUSAN PENGADILAN)

SKRIPSI

Diajukan Untuk Memenuhi Sebagian Persyaratan Guna Memperoleh Gelar Sarjana (Strata-1) pada Fakultas Hukum
Universitas Islam Indonesia
Yogyakarta

Oleh :

MAULIDA DIAH LAURENTINA

No. Mahasiswa: 18410617

PROGRAM STUDI HUKUM PROGRAM SARJANA

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2022

MODUS OPERANDI TINDAK PIDANA *PHISHING* DAN PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA *PHISHING* DI SURABAYA

(STUDI PUTUSAN PENGADILAN)

SKRIPSI

Oleh :

MAULIDA DIAH LAURENTINA

No. Mahasiswa: 18410617

PROGRAM STUDI HUKUM PROGRAM SARJANA

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2022

بسم الله الرحمن الرحيم

HALAMAN PENGESAHAN TUGAS AKHIR PRA PENDADARAN

MODUS OPERANDI TINDAK PIDANA *PHISHING* DAN PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA *PHISHING* DI SURABAYA

(STUDI PUTUSAN PENGADILAN)

Telah Diperiksa dan Disetujui oleh Dosen Pembimbing Skripsi untuk Diajukan ke Depan Tim Penguji dalam Ujian Tugas Akhir/Pendadaran

Pada tanggal: 28 November 2022

Yogyakarta, 28 November 2022

Dosen Pembimbing Skripsi,

Ari Wibowo, S.HI., S.H., M.H.

NIK. 124100101

بسم الله الرحمن الرحيم

HALAMAN PENGESAHAN TUGAS AKHIR

MODUS OPERANDI TINDAK PIDANA *PHISHING* DAN PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA *PHISHING* DI SURABAYA

(STUDI PUTUSAN PENGADILAN)

Telah Dipertahankan di Hadapan Tim Penguji dalam

Ujian Tugas Akhir/Pendadaran

Pada Tanggal 14 Desember 2022 dan dinyatakan **LULUS**

Yogyakarta 14 Desember 2022

Tim Penguji			**Tanda Tangan**
1. Ketua	:	Ari Wibowo, S.HI.,S.H.,M.H	
2. Anggota	:	Dr. Aroma Elmina Martha, S.H.,M.H	
3. Anggota	:	Ayu Izza Elvany, S.H.,M.H	

Mengetahui

Universitas Islam Indonesia Yogyakarta

Fakultas Hukum

Dekan

Prof. Dr. Budi Agus Riswandi, S.H., M.Hum.

NIK. 014100109

HALAMAN MOTTO

“Maka nikmat Tuhanmu yang manakah yang kamu dustakan?”

(QS. Ar-Rahman: 13)

Rasulullah SAW bersabda: "Waktu bagaikan pedang. Jika engkau tidak memanfaatkannya dengan baik (untuk memotong), maka ia akan memanfaatkanmu (dipotong)."

(HR. Muslim)

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan kepada

Alm.Bapak, Ibu, dan Kakakku

Keluarga besarku

Sahabat, Teman, dan semua yang tidak pernah putus dalam memberikan dukungan dan semangat hingga tahap ini

Serta diri sendiri yang terus berjuang untuk menyelesaikan ini

Terima kasih.

CURRICULUM VITAE

1. Nama Lengkap : Maulida Diah Laurentina
2. Tempat Tanggal Lahir : Ngawi, 14 Juni 2000
3. Jenis Kelamin : Perempuan
4. Golongan Darah : B
5. Agama : Islam
6. Alamat Terakhir : Desa Gandri RT. 05/ RW. 03, Kecamatan Pangkur, Kabubaten Ngawi.
7. Alamat Asal : Desa Gandri RT. 05/ RW. 03, Kecamatan Pangkur, Kabubaten Ngawi.
8. *E-mail* : ulimaulida13@gmail.com
9. Identitas Orang Tua
   a. Nama Ayah : Alm. Daryono
      Pekerjaan Ayah : -
   b. Nama Ibu : Hartatin
      Pekerjaan Ibu : Wiraswasta
10. Riwayat Pendidikan
    a. TK : TK Dharma Wanita
    b. SD : SD Negeri Gandri 2
    c. SMP : SMP Negeri 1 Karangjati
    d. SMA : SMA Negeri 2 Ngawi
11. Organisasi dan Pengalaman Lainnya:
    a. Bendahara UKM Bola Basket FH UII 2019-2020
    b. Manager UKM Bola Basket FH UII 2021-2022
    c. Magang Legal SDM PT. INKA Multi Solusi Madiun, September-Oktober 2020

SURAT PERNYATAAN

Orisinalitas Karya Tulis Ilmiah/Tugas Akhir Mahasiswa Fakultas Hukum

Universitas Islam Indonesia

Yang bertanda tangan di bawah ini, saya:

Nama : **MAULIDA DIAH LAURENTINA**

No. Mahasiswa : **18410617**

Adalah benar-benar mahasiswi Fakultas Hukum Universitas Islam Indonesia Yogyakarta yang telah melakukan penulisan Karya Tulis Ilmiah (Tugas Akhir) berupa skripsi dengan judul: **Modus Operandi Tindak Pidana Phishing dan Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Phishing di Surabaya (Studi Putusan Pengadilan).**

Karya Tulis Ilmiah ini akan saya ajukan kepada Tim Penguji dalam Ujian Pendadaran yang diselenggarakan oleh Fakultas Hukum Universitas Islam Indonesia. Sehubung dengan tersebut, dengan ini saya menyatakan:

1. Bahwa karya tulis ilmiah ini adalah benar-benar karya saya sendiri yang dalam penyusunan tunduk dan patuh terhadap kaidah, etika, dan norma-norma penulisan sebuah karya tulis ilmiah sesuai dengan ketentuan yang berlaku;
2. Bahwa meskipun secara prinsip hak milik atas karya tulis ilmiah ini ada pada saya, namun demi untuk kepentingan-kepentingan yang bersifat akademik dan pengembanganya, saya memberikan kewenangan kepada Perpustakaan Fakultas Hukum Universitas Islam Indonesia dan perpustakaan di lingkungan Universitas Islam Indonesia untuk mempergunakan karya tulis ilmiah saya tersebut.

Selanjutnya berkaitan dengan hal di atas (terutama penyertaan pada butir nomor 1 dan 2, saya sanggup menerima sanksi administratif, akademik, bahkan sanksi pidana, jika saya terbukti secara kuat dan meyakinkan telah melakukan perbuatan yang menyimpang dari pernyataan tersebut. Saya juga akan bersifat kooperatif

untuk haadir, menjawab, membuktikan, melakukan pembelaan terhadap hak-hak saya serta menandatangani berita acara terkait yang menjadi hak dan kewajiban saya, di depan “Majelis” atau “TIM” Fakultas Hukum UII yang ditunjuk oleh pimpinan fakultas apabila tanda-tanda plagiat disinyalir ada atau terjadi pada karya ilmiah saya oleh pihak Fakultas Hukum UII. Demikian surat pernyataan ini saya buat dengan sebenar-benarnya dan dalam kondisi sehat jasmani dan rohani, dengan sadar serta tidak ada tekanan dalam bentuk apapun dan oleh siapapun.

Yogyakarta, 17 November 2022

Yang membuat pernyataan

(Maulida Diah Laurentina)

NIM. 18410617

KATA PENGANTAR

Assalamuallaikum Wr. Wb.

Segala puji bagi Allah SWT Tuhan semesta Alam yang telah memberikan rahmat dan hidayah-Nya kepada kita semua. Tak lupa shalawat serta salam tercurahkan kepada junjungan kita, Nabi Muhammad SAW dan semoga syafa'atnya akan selalu mengalir kepada keluarganya, sahabatnya, dan insyallah kita semua. Alhamdulillah atas doa dan dukungan dari orang-orang tercinta, akhirnya penulis dapat menyelesaikan tugas akhir yang berjudul Modus Operandi Tindak Pidana Phishing dan Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Phishing di Surabaya (Studi Putusan Pengadilan).

Meskipun dalam proses penyelesaian tugas akhir ini penulis mendapatkan banyak hambatan, tetapi hal ini tidak berarti berkat dukungan dari orang-orang terdekat penulis dari awal hingga terselesaikannya tugas akhir ini. Penulis menyadari bahwa tanpa ada dukungan tersebut penulis tidak akan sampai pada titik ini. Selain itu, skripsi ini masih terdapat kelemahan dan kekurangan dalam penulisannya.

Penulis juga ingin mengucapkan terima kasih kepada berbagai pihak yang telah memberikan doa, bantuan dan bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin sampaikan ucapan terima kasih kepada:

1. Allah SWT beserta Rosul-Nya.
2. Kepada keluarga tercinta; Alm. Bapak, Ibu Hartatin dan Kakak Nana dan Alvan. Terima kasih atas doa, nasehat, dan dukungannya. Tiada kesuksesan tanpa restu dari kalian.

3. Prof. Dr. Budi Agus Riswandi, S.H., M.Hum selaku Dekan Fakultas Hukum Universitas Islam Indonesia.
4. Bapak Ari Wibowo, S.HI., S.H., M.H. selaku dosen pembimbing skripsi yang telah meluangkan waktu, tenaga dan pikirannya. Terima kasih telah sabar dalam membimbing dan mengarahkan penulisan tugas akhir ini.
5. Ibu Dr. Aroma Elmina Martha, S.H., M.H dan Ibu Ayu Izza Elvany, S.H., M.H. selaku dosen penguji yang telah memberikan saran dan arahan dalam tugas akhir ini.
6. Seluruh Dosen dan Karyawan Fakultas Hukum Universitas Islam Indonesia yang dengan ketulusan hatinya memberikan ilmu dan informasi dalam berbagai mata kuliah ilmu hukum kepada penulis.
7. Sepupuku Aurel, Mustika, Bobby, Lian dan seluruh kelurga besar Mbah Kami, serta sahabatku Berlin terima kasih atas segala dukungan dan bantuannya selama penulis berjuang menyelesaikan tugas akhir ini.
8. Sahabat-sahabatku satu almamater yang telah membantu dan memberikan masukan dalam penulisan tugas akhir ini; Nabila, Shania, Rizky, Nadya, Khansa, Amel, Audi, Aji, Cindy, Dahlia, Nina, dan Meysi.
9. Seluruh pihak, yang telah berjasa dalam hidup penulis yang tidak bisa penulis sebutkan satu persatu.

DAFTAR ISI

ABSTRAK

Studi ini bertujuan untuk menganalisis modus operandi dan pertanggungjawaban pidana terhadap pelaku tindak pidana *phishing* yang terjadi di Surabaya melalui studi putusan Pengadilan Negeri Surabaya. Rumusan masalah yang diajukan yaitu: Bagaimana modus operandi tindak pidana *phishing* yang terjadi di Surabaya?; Bagaimana pertanggungjawaban pidana pelaku tindak pidana *phishing* yang terjadi di Surabaya?. Penelitian ini termasuk tipologi penelitian hukum normatif. Data penelitian dilakukan dengan studi pustaka yang mengkaji literatur seperti buku dan jurnal ilmiah, dan studi dokumen yang mengkaji peraturan perundang-undangan serta putusan pengadilan terkait permasalahan yang akan diteliti. Analisis dilakukan dengan pendekatan perundang-undangan dipadukan dengan pendekatan kasus. Hasil studi ini menunjukkan bahwa modus operandi *phishing* dilakukan dengan terlebih dahulu menentukan target sebelum selanjutnya membuat *website phishing* dengan teknik *script scampage*. *Website* palsu kemudian disebarkan melalui SMS dan/atau *e-mail* kepada target berupa *link* dengan pesan tersirat yang mengarah kepada pengelabuan. Ketika target mengunjungi *link* dan mengikuti seluruh instruksi didalamnya, maka tujuan seorang *phishers* telah tercapai dan dapat mengambil alih informasi pribadi serta data akun yang disertakan. Pertanggungjawaban pidana adalah pertanggungjawaban atas kejahatan yang dilakukan. Hasil penelitian menunjukkan bahwa seluruh terdakwa telah memenuhi unsur pertanggungjawaban pidana, sehingga atas perbuatannya dapat dimintai pertanggungjawaban. Dalam hal ini di sebutkan beberapa cara turut serta melakukan tindak pidana, yaitu: *pleger, medepleger, dan uitlocker* dianggap sebagai pelaku atau pembuat tindak pidana (*daader*), sehingga ancaman hukumannya adalah sama. Menindaklanjuti penelitian yang telah dilakukan, penulis berpendapat bahwa pentingnya dibuat regulasi khusus yang berkaitan dengan kejahatan siber dan kejahatan transnasional lain. Edukasi terhadap masyarakat juga diperlukan untuk meminimalisir korban kejahatan siber, dan lembaga penegak hukum diharapkan lebih tegas dalam menindak para pelaku kejahatan siber.

Kata Kunci: modus operndi, pertanggungjawaban pidana, *phishing*

BAB I

PENDAHULUAN

A. Latar Belakang

Adanya revolusi industri 4.0 disertai dengan meluasnya persebaran covid-19 ke seluruh penjuru negeri, menjadikan penggunaan teknologi oleh masyarakat menjadi tidak terkendali. Kecanggihan teknologi yang menggiring *technology based* berkembang di Indonesia telah berhasil mengubah *mindset* masyarakat. Teknologi yang terus berkembang akan melindas siapapun yang tidak memahaminya, sehingga melakukan digitalisasi adalah sebuah keharusan.

Pesatnya perkembangan teknologi memberikan kemudahan bagi penggunanya dalam mengakses informasi, memunculkan inovasi dalam berbagai bidang serta digitalisasi transaksi yang menjadi sangat praktis. Pemanfaatan perkembangan teknologi juga berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat.

Fakta bahwa pesatnya perkembangan teknologi yang menyeluruh ke berbagai bidang, tidak menutup kemungkinan jika tindak kejahatan juga mengikuti perkembangan tersebut. Tindak kejahatan yang dilakukan tidak lagi menggunakan metode-metode konvensional, melainkan dengan metode

yang lebih efisien dan *tricky*. Hingga dikenalnya bentuk kejahatan dalam internet atau dunia maya yang seringkali disebut sebagai *Cybercrime*. *Cybercrime* adalah segala bentuk kejahatan yang terjadi di dunia maya atau internet (*cyberspace*). *Cybercrime* merupakan tindak kriminal yang melibatkan komputer dan jaringan, di mana keduanya memainkan peran penting dalam dilakukannya kejahatan.[1]

Salah satu unsur dari tindak pidana dalam ilmu hukum adalah unsur perbuatan yang dilakukan secara melawan hukum.[2] Perbuatan melawan hukum (*wederrechtelijk)* terjadi apabila suatu perbuatan yang dilakukan seseorang telah melanggar peraturan perundang-undangan serta menimbulkan kerugian terhadap pihak-pihak lain sehingga timbul gugatan dari pihak-pihak tersebut.[3] Meskipun *cybercrime* bukan merupakan kejahatan baru dan telah ada sejak tahun 1980 dengan fokus penyerangan di bidang perbankan, tetapi dengan berkembangnya teknologi tentu bentuk kejahatannya semakin beragam dan luas cakupannya.

Kesulitan dalam menjaring berbagai kejahatan siber sehingga turut mengalami perkembangan merupakan sebab dari perumusan hukum yang ada belum dapat menjangkau perkembangan kejahatan yang dilakukan di

---

[1] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime*, *Cybercrime: Investigating High-Technology Computer Crime*, Cetakan kedua, Abingdon, New York, 2014, hlm. 4.

[2] JM. Van. Bemmelen, *Hukum Pidana 1-Hukum Pidana Material Bagian Umum*, terj. Hasnan, Cetakan keenam, Bina Cipta, Bandung, 1984, hlm. 99.

[3] Titin Apriani, "Konsep Perbuatan Melawan Hukum Dalam Tindak Paidana", *Jurnal Hukum*, Edisi No. 1 Vol. 13, Fakultas Hukum Universitas Mahasaraswati Mataram, 2019, hlm. 45.

dunia maya.[4] Peraturan terkait *cybercrime* di Indonesia masih mengacu pada Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (yang selanjutnya disebut dengan UU ITE), terkhusus yang termuat dalam Pasal 27 hingga Pasal 30 tentang Perbuatan yang Dilarang. Walaupun UU ITE diklasifikasikan sebagai undang-undang administratif, namun legislator telah memasukkan beberapa ketentuan tentang tindak pidana.[5] Dengan demikian *cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum dalam ranah hukum pidana dengan memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.

Perusahaan Acronis Cyber Protect yang merupakan pemimpin global dalam produk perlindungan *cyber* telah merilis laporan *Acronis Cyberthreats Report* tahunan untuk 2022 yang berisi tinjauan mendalam mengenai tren serta ancamanan keamanan siber atau *cybersecurity* di seluruh dunia.[6] Dari berbagai jenis dan bentuk serangan *cybercrime*, dikatakan *phishing* telah menduduki posisi tertinggi untuk serangan siber.

---

[4] Dewi Bunga, 'Politik Hukum Pidana Terhadap Penanggulangan', *Jurnal Legislasi Indonesia*, Edisi No. 1 Vol. 16, Fakultas Hukum Universitas Gadjah Mada, 2019, hlm. 3.

[5] Vidya Prahassacitta, *Konsep Kejahatan Siber Dalam Sistem Hukum Indonesia*, terdapat dalam https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/ , diakses tanggal 22 Maret 2022, pukul. 23.47.

[6] Dave Kostos, *Acronis Cyberthreats Report 2022 unveils cyberthreat predictions*, terdapat dalam https://www.acronis.com/id-id/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/, diakses tanggal 24 Maret 2022, pukul. 20.07.

Kejahatan dilakukan dengan memanfaatkan *malware* untuk dapat mengelabui pengguna agar membuka lampiran atau tautan yang berbahaya.[7]

Badan Siber dan Sandi Negara (BSSN) pada tahun 2019 melaporkan 290 juta kasus serangan siber. Jumlah tersebut 25% lebih banyak jika dibandingkan tahun sebelumnya ketika kejahatan siber menyebabkan kerugian sebesar US$ 34,2 miliar di Indonesia.[8] Dari banyaknya kerugian serta korban akibat *phishing*, penelitian ini akan memfokuskan pada kejahatan siber berupa *phishing*.

Phishing (*password harvesting fishing)* merupakan penipuan yang dilakukan dengan cara mengelabui target sehingga pelaku bisa mendapatkan data sensitif dan bersifat rahasia. Tindakan yang dilakukan *phishers* sebagai pelaku kejahatan *phishing* mengincar informasi sensitif pengguna untuk digunakan oleh pihak yang tidak berwenang.[9] *Phishers* sendiri merupakan bagian dari *Black Hat Hackers* karena termasuk ke dalam kategori peretas yang menyebabkan kerugian pada orang lain dengan mencari celah keamanan yang belum maksimal dalam suatu *software* untuk menyusup dan merusak sistem perangkat lunak tersebut.[10]

---

[7] Dave Kostos, *Acronis Cyberthreats Report 2022 unveils cyberthreat predictions*, terdapat dalam https://www.acronis.com/id-id/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/, diakses tanggal 24 Maret 2022, pukul. 20.07.

[8] Noor Halimah Anjani, "*Ringkasan Kebijakan No. 9 : Perlindungan Keamanan Siberdi Indonesia*, terdapat dalam https://www.cips-indonesia.org/publications/perlindungan-keamanan-siber-di-indonesia?lang=id, diakses tanggal 24 Maret 2022, pukul. 20.30.

[9] I.Radiansyah, Candiwan and Y.Priyadi, "Analisis Ancaman *Phishing* Dalam Layanan Online Banking", *Jurnal Pengabdian dan Pemberdayaan Masyarakat*, Edisi No. 1 Vol. 7, Fakultas Ekonomi Bisnis Universitas Telkom, 2016, hlm. 5.

[10] Vikran Fasyadhiyaksa Putra Y. "Modus Operandi Tindak Pidana *Phishing* Menurut UU ITE", *Jurnal Hukum*, Edisi No. 6 Vol. 4, Fakultas Hukum Universitas Airlangga, 2021, hlm. 2528.

Modus operandi *phishing* biasanya menggunakan halaman *website* palsu (*fake webpage*) atau surel palsu untuk mengelabui dan mencuri data-data pribadi pengguna. Setelah korban atau target memberikan informasi yang diminta, *phishers* akan dapat mengambil alih akun, melakukan transaksi keuangan, mencuri uang, mengajukan pinjaman utang ataupun tindakan lain yang mengakibatkan pemilik identitas mengalami kerugian finansial. *Phishers* dalam hal ini menguasai mengenai sistem komputer dan juga sangat ahli dalam mencari celah-celah keamanan dalam sebuah sistem komputer, dapat dikatakan mereka memiliki penguasaan dalam komputer lebih daripada orang pada umumnya.[11]

Besarnya dampak serta korban yang terlapor maupun tidak terlapor, menjadikan kejahatan mayantara berupa *phishing* perlu ditindak lanjuti. Upaya penindakan harus dilakukan penegak hukum dengan mengetahui dan memahami modus operandi atau cara beroperasinya terlebih dahulu, tujuannya untuk mengetahui siapa dalangnya beserta motifnya. Perlu diketahui bahwa modus operandi *phishing* ini berbeda dengan tindak kejahatan konvensional. Perbedaan yang mencolok terdapat dalam *locus delicti* atau tempat kejahatan perkara, karena sangat sulitnya melokalisir jaringan internet. Dalam hal ini, pengkajian penelitian akan dilakukan dengan menelaah modus operandi berdasarkan kasus yang telah terjadi di wilayah hukum Pengadilan Negeri Surabaya.

[11] Vikran Fasyadhiyaksa Putra Y. "Modus Operandi Tindak Pidana *Phishing* Menurut UU ITE", *Jurnal Hukum*, Edisi No. 6 Vol. 4, Fakultas Hukum Universitas Airlangga, 2021, hlm. 2535.

Di Pengadilan Negeri Surabaya terdapat beberapa kasus tindak pidana *phishing*. Dari *website* Pengadilan Negeri Surabaya diperoleh 8 putusan pengadilan dalam perkara tindak pidana *phishing*, yaitu:[12]

1. Putusan Nomor : 1193/Pid.Sus/2021/PN.Sby.
2. Putusan Nomor : 2205/Pid.Sus/2021/PN.Sby.
3. Putusan Nomor : 1855/Pid.Sus/2021/PN.Sby.
4. Putusan Nomor: 1194/Pid.Sus/2021/PN.SBY.
5. Putusan Nomor: 2182/Pid.Sus/2021/PN.SBY.
6. Putusan Nomor: 2206/Pid.Sus/2021/PN.SBY.
7. Putusan Nomor: 1837/Pid.Sus/2021/PN.SBY.
8. Putusan Nomor: 1872/Pid.Sus/2021/PN.SBY.

Pemberantasan kejahatan *phishing* di Indonesia saat ini tidak lepas dari peran penting aparat penegak hukum, salah satunya adalah lembaga peradilan. Kehadiran peran hakim diharapkan dapat mengurangi kasus pidana *phishing* yang dapat melibatkan pelaku kejahatan berupa hukuman yang berat dan tepat sasaran. Hakim menentukan hukuman bagi *phishers* dengan melihat pasal-pasal yang dilanggar. Dari 8 (delapan) putusan yang menjadi objek penelitian, Hakim telah memutuskan kasus tersebut dan menemukan bahwa semua terdakwa dinyatakan bersalah secara sah dan meyakinkan secara bersama-sama dan sendiri-sendiri atas kejahatan

[12] Direktori putusan Mahkamah Agung RI, terdapat dalam https://putusan3.mahkamahagung.go.id/search.html?q=*phishing*&court=098111PN340, diakses tanggal 22 Oktober 2021, Pukul : 21.20

phishing yang dilakukan. Mengenai hukuman yang diberikan kepada terdakwa, penentuan hukuman pidana sebagai bentuk pertanggungjawaban pidana dan menetapkan kesalahan terdakwa menjadi persoalan yang menarik untuk dikaji.

Sebelum mengambil keputusan dalam suatu perkara pidana, hakim terlebih dahulu harus memperhatikan perincian bagian hukum pidana dan menyatakan bahwa Ia bersalah atas dakwaan tersebut. Setelah terbukti bahwa terdakwa melakukan kejahatan dan melanggar pasal tertentu, hakim menganalisis apakah kejahatan tersebut dapat dituntut. Apabila tindak pidana yang dilakukan oleh terdakwa terbukti sesuai dengan dakwaan dan pertanggungjawaban pidana, hakim dapat menjatuhkan pidana yang dijatuhkan kepada terdakwa. Dalam memutuskan pidana yang akan dijatuhkan kepada terdakwa, hakim harus mempertimbangkan apakah putusan itu sesuai dengan tujuan pemidanaan dan apakah sesuai dengan hukum yang berlaku atau tidak.

Perkara tindak pidana *phishing* tersebut diatas, semuanya melibatkan lebih dari satu pelaku. Suatu perbuatan pidana dapat dilakukan oleh beberapa orang untuk melakukan suatu perbuatan melawan hukum dengan peran yang berbeda serta bervariatif. Hal tersebut dapat dicermati berdasarkan peran serta mereka melakukan perbuatan tersebut berdasarkan atas kaidah delik pernyertaan atau *deelneming*. Karena pelakunya lebih dari satu, maka selalu junctokan dengan Pasal 55 ayat (1) Kitab Undang-Undang

Hukum Pidana (yang selanjutnya disebut KUHP). Masing-masing pelaku akan dipertanggungjawabkan sesuai dengan perannya.

Delik penyertaan diartikan sebagai turut sertanya seseorang dalam suatu perbuatan pidana, sehingga harus dipastikan bahwa seluruh pelaku kejahatan berdasarkan peranan masing-masing turut diberikan sanksi. Seluruh pelaku wajib menanggung konsekuensi atas perbuatannya karena telah melakukan suatu kejahatan yang merugikan sebagai wujud pertanggung jawaban pidana.

Kejahatan phishing tergolong kejahatan dunia maya yang memiliki modus operandi yang kompleks dan juga dapat berdimensi transnasional apabila dilakukan antar negara dan wilayah yang berbeda. Sehingga dapat menimbulkan kejahatan yang meluas dan kerugian yang sangat besar. Berdasarkan penjelasan di atas, maka penulis bermaksud untuk melakukan penelitian dengan judul "MODUS OPERANDI TINDAK PIDANA *PHISHING* SERTA PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA *PHISHING* DI SURABAYA".

B. Rumusan Masalah

Berdasarkan pemaparan latar belakang di atas, rumusan masalah yang akan diteliti sebagai berikut:

1. Bagaimana modus operandi tindak pidana *phishing* yang terjadi di Surabaya?
2. Bagaimana pertanggungjawaban pidana pelaku tindak pidana *phishing* yang terjadi di Surabaya?

C. Tujuan Penelitian

Tujuan dari dilakukan perumusan masalah dalam penelitian ini adalah untuk:

1. Menganalisis modus operandi pada kejahatan *phishing* dilakukan dan sebagai edukasi masyarakakat terkait waspada terkena *phishing*.
2. Menganalisis pertanggungjawaban pidana pelaku tindak pidana *phishing* yang terjadi di Surabaya.

D. Manfaat Penelitian

Kegunaan dalam melakukan penelitian terhadap masalah di atas adalah memberikan kegunaan secara teoritis maupun praktis, yaitu:

1. Manfaat Teoritis

   Hasil penelitian ini diharapkan dapat menjadi bahan pembelajaran serta menambah wawasan dan pengetahuan mengenai modus operandi dan pertanggungjawaban pidana bagi pelaku tindak pidana *cybercrime*

terkhusus kejahatan *phishing* di Indonesia, serta diharapkan juga sebagai sarana pengembangan ilmu pengetahuan yang dapat dipelajari.

2. Manfaat Praktis

Hasil dari penelitian ini diarapkan dapat menjadi bahan informasi terkait bahaya *phishing* oleh seluruh masyarakat dengan mengetahui segala bentuk modus operandi yang digunakan serta diharapkan dapat memberi sumbangan agar masyarakat meningkatkan kewaspadaan akan bahaya *cybercrime* terutama kejahatan *phishing*.

E. Orisinalitas Penelitian

Sejarah penelusuran peneliti, penelitian ini memiliki kemiripan dengan judul penelitian yang telah dilakukan oleh:

No	Peneliti & Judul Penelitian	Rumusan Masalah	Hasil Penelitian
1	**Hilman Mursidi** Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Cybercrime Phishing* (Studi Kasus Putusan PN Medan No :	1. Bagaimana pengaturan tindak pidana *cybercrime phishing* ditinjau dalam hukum positif Indonesia? 2. Bagaimana pertanggungjawaban	Dalam penelitian ini lebih memfokuskan terhadap peran hukum positif Indonesia dalam mengatur tindak

	3006/Pid.Sus/2017/PN. Mdn)	pidana terhadap pelaku tindak pidana *cybercrime phishing*?	pidana *cybercrime phishing*,
2	**Vikran Fasyadhiyaksa Putra Y** Modus Operandi Tindak Pidana *Phishing* Menurut UU ITE	1. Bagaimana aktivitas Tindak Pidana *Phishing* dalam Undang-Undang ITE?	Dalam penelitian ini lebih memfokuskan untuk menganalisis dan menjelaskan terkait tahapan dan modus operandi pelaku tindak pidana *phishing* menurut UU ITE.
3	**Nur Khalimatus Sa'diyah** Modus Operandi Tindak Pidana *Cracker* Menurut Undang-Undang Informasi DanTransaksi Elektronik	1. Bagaimana terbentuknya jaringan komputer di tengah masyarakat? 2. Bagaimana modus	Dalam penelitian ini selain menganalisis modus operandi *cracker* dan aktivitas *cracking* di internet, juga menganalisis terkait factor-

		operandi *craking*? 3. Jelaskan faktor-faktor yang mempengaruhi terjadinya *cracker!*	faktor yang mempengaruhi maraknya terjadi *craking* di wilayah Indonesia.

Berdasarkan penelusuran di atas, ada beberapa kemiripan yang sudah membahas mengenai tindak pidana *phishing*, tetapi belum ada yang khusus menangani tentang modus operandi dan juga pertanggungjawaban pidana *phishing* dengan studi kasus putusan pengadilan. Terjadi kesamaan pembahasan terkait pertanggungjawaban pidana melalui studi kasus putusan pengadilan, namun penulis lain menggunakan putusan pengadilan yang berbeda dan daerah peradilan yang berbeda pula.

F. Tinjauan Pustaka

1. Tindak Pidana *Phishing*

Tindak pidana bahwasanya merupakan suatu perbuatan yang mengandung unsur-unsur perbuatan yang dilarang oleh undang-undang yang dapat menimbukan akibat hukum atau dapat dikenai sanksi pidana (hukuman), dan orang yang melakukannya mampu mempertanggung

jawabankan perbuatan yang dilakukan tersebut. Tindak pidana (*Strafbaar Feit*) dikaji dalam suatu ilmu hukum yang disebut hukum pidana. Ilmu hukum pidana adalah aturan-aturan hukum yang mengatur mengenai perbuatan-perbuatan yang termasuk dalam delik (perbuatan pidana). Hukum pidana yang berlaku di Indonesia sekarang ini ialah hukum pidana yang telah dikodifikasi, yaitu *Wetboek van Strafrecht* atau KUHP.

Tindak pidana dalam perkembangannya disebut sebagai kegiatan yang menyimpang dan semakin beragam macamnya. Dampak dari semakin pesatnya teknologi antara lain memunculkan fenomena kejahatan yang semakin beragam dan semakin sulit ditangani akibat cara kerjanya yang *invisible* dan *borderless*. Salah satu jenis kejahatan yang banyak terjadi dan tak sedikit yang menjadi korban adalah kejahatan *phishing*.

Phishing merupakan proses penipuan atau pengelabuan dengan tujuan untuk mencuri informasi rahasia dari pengguna yang biasanya melibatkan penggunaan situs web palsu. Pelaku yang melakukan pengelabuan melalui kejahatan *phishing* di sebut dengan *phishers*. *Phishers* akan memancing seorang target untuk memasukkan informasi pribadi yang bersifat rahasia 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. *Phishers* menggunakan informasi dari korban tersebut untuk dilakukan tindakan

pencurian atau pembobolan melalui data pribadi korban yang telah bocor tersebut.

Mengenai hal ini yang menjadi perhatian penting bukan hanya pada keamanan fitur berbasis virtual, namun pengetahuan yang dimiliki pengguna teknologi juga harus berkembang seiring dengan perkembangan tekhnologi itu sendiri. Mengingat penanganannya sangat berbeda dengan kejahatan konvensional.

Perbedaan signifikan antara kejahatan konvensional dengan *cybercrime* adalah jika kejahatan siber dapat dilakukan tanpa adanya kontak fisik antara pelaku dan korban, tidak ada perhitungan jarak antara pelaku dengan target kejahatan sehingga dapat dilakukan dimana saja sepanjang terdapat komputer yang tersambung dalam jaringan internet sebagai objek kejahatan. Adanya globalisasi pula membuat kejahatan siber dapat melintasi batas negara. Kejahatan siber dapat melibatkan beberapa pelaku yang berada di beberapa wilayah yurisdiksi negara yang berbeda dengan target korban yang berada di negara lain pula.[13]

2. Modus Operandi Tindak Pidana *Cybercrime*

Modus operandi berasal dari bahasa latin, artinya prosedur atau cara bergerak atau berbuat sesuatu. Pengertian modus operandi adalah teknik cara-cara beroperasi yang dipakai oleh penjahat. Pada dasarnya objek yang digunakan dalam melakukan kejahatan siber adalah perangkat

[13] Dewi Bunga, *Op. Cit,* hlm. 2.

komputer yang tersambung dalam jaringan. Modus operandi dalam *cybercrime* sangat beragam macam dan tujuannya, antara lain:[14]

a) Dengan cara memasuki atau menyusup ke dalam suatu system jaringan computer secara tidak sah dengan tujuan nya adalah sabotase atau pencurian indormasi penting (*Unauthorized Access to Computer System and Service).*
b) Dengan cara menyebarkan berita hoax untuk kepentingan pribadi atau propaganda (*illegal contents*).
c) Dengan cara memanfaatkan jaringan internet untuk kegiatan memata-matai pihak lain (*cyber espionage*).
d) Dengan cara membuat kerusakan, gangguan atau penghancuran terhadap suatu dengan virus atau *malware* (*cyber sabotage and extortion*).
e) Dengan cara mencuri informasi atau data pribadi orang lain untuk mendapatkan informasi krusiaal seperti *username* beserta *password,* data finansial, dengan cara pengelabuan atau penyamaran, yang nantinya informasi tersebut akan digunakan untuk kepentingan pribadi. Dalam hal ini biasanya digunakan teknik dengan cara membuat *script* tampilan suatu *website* yang menyerupai *website* asli/resmi yang gunanya agar target yang melihat *scampage* tersebut tertipu dan mengisi data-data pribadi

[14] Redaksi, *Jenis Modus Operandi Cybercrime*, terdapat dalam https://jurnalsecurity.com/jenis-modus-operandi-cybercrime/, diakses tanggal 5 Juli 2022, pukul. 17.38.

yang dibutuhkan *phishers* (*script scampage*) untuk kemudian digunakan secara melawan hukum.

Berdasarkan bahan hukum berupa putusan yang digunakan sebagai bahan penelitian dapat diketahui bahwa modus operandi pelaku tindak pidana *phishing* di wilayah hukum Pengadilan Negeri Surabaya relatif sama yang mana seorang *phishers* harus mendapatkan data pribadi target dengan cara pengelabuan baik melalui email ataupun website (*script scampage*).

3. Pertanggungjawaban Pidana dalam Delik Penyertaan

Liability atau di dalam Bahasa Indonesia berarti pertanggungjawaban pidana (*toereken-baarheid*) ialah kewajiban individu atau korporasi untuk menanggung konsekuensi atas perbuatannya karena telah melakukan suatu kejahatan yang merugikan. Suatu perbuatan dapat dimintai pertanggungjawaban pidana manakala perbuatan tersebut bersifat melawan hukum, atau perbuatan tersebut dikuahifikasi sebagai perbuatan pidana oleh undang-undang pidana. Selain itu, bagi pembuatnya dapat dimintakan pertanggungjawaban pidana manakala telah melakukan perbuatan pidana dan terdapat kesalahan dalam dirinya.

Ajaran penyertaan sebagai ajaran yang memperluas dapat dipidananya orang yang tersangkut dalam timbulnya suatu perbuatan pidana. Di samping itu ada delik-delik biasa seperti penyertaan yang memperluas dapat dipidananya orang yang tersangkut dalam timbulnya

suatu perbuatan pidana. Dalam hal ini dikenal dengan istilah pertanggung jawaban pidana (*toereken-baarheid*) yang merupakan kewajiban untuk menanggung konsekuensi atas perbuatannya karena telah melakukan suatu kejahatan yang merugikan

Berdasarkan ketentuan Pasal 55 dan 56 KUHP dapat ditarik kesimpulan bahwa penyeetaan adalah apabula oramg yang tersangkut untuk terjadinya suatu perbuatan pidana atau kejahatan itu tidak hanya satu orang saja, melainkan melibatkan lebih dari satu orang. Selain itu dalam ajaran penyertaan yang didasarkan pada Pasal 55 KUHP menyebutkan beberapa golongan yang dapat dipidana, yaitu:[15]

a) Pembuat (*daader*)

Dader berasal dari kata daad yang di dalam bahasa belanda memiliki arti sebagai tindakan. Orang melakukan suatu daad disebut dengan *dader*, atau lazimnya dikenal dengan sebutan pelaku.

1) Pelaku (*pleger*)

Pleger adalah mereka yang memenuhi seluruh unsur yang ada dalam suatu perumusan karakteristik delik pidana dalam setiap pasal.[16] *Pleger* adalah orang yang secara materiil dan *persoonlijk* nyata-nyata melakukan perbuatan yang secara sempurna memenuhi semua unsur dari rumusan

[15] Pasal 55 Kitab Undang-Undang Hukum Pidana.

[16] A.F. Lamintang & Fraciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana di Indonesia*, Cetakan keenam, Sinar Grafika, Jakarta, 2014, hlm. 611.

delik yang terjadi.[17] Oleh karena itu, pada dasarnya ia adalah orang yang baik secara sendiri maupun terkait dengan orang lain, telah dapat dijatuhi sanksi pidana.

2) Yang menyuruh melakukan (*doenpleger*)

Doen Pleger adalah orang yang menyuruh orang lain untuk melakukan suatu perbuatan pidana, dimana secara yuridis orang yang disuruh dan akhirnya secara nyata melakukan perbuatan pidana tersebut harus merupakan orang yang tidak dapat dipertanggungjawabkan secara pidana.[18]

3) Turut serta melakukan (*medepleger*)

Medepleger adalah orang yang melakukan kesepakatan dengan orang lain untuk melakukan suatu perbuatan pidana dan secara bersama-sama pula iaturut beraksi dalam pelaksanaan perbuatan pidana sesuai dengan yang telah disepakati.[19]

4) Penganjur (*uitlokker*)

Setiap orang yang menggerakkan atau membujuk orang lain (*pleger*) untuk melakukan suatu tindak pidana dengan menggunakan sarana-sarana yang telah ditentukan undang-

[17] Chant S. R. Ponglabba, "Tinjauan Yuridis Penyertaan Dalam Tindak Pidana Menurut KUHP", Jurnal Hukum, Edisi No. 6, Vol. 6, Fakultas Hukum Universitas Sam Ratulangi, 2017, hlm. 34.

[18] *Ibid.*

[19] *Ibid.*

undang secara limitatif, yaitu dengan memberikan atau menjanjikan sesuatu, menyalahgunakan kekuasaan atau martabat, kekerasan, ancaman, atau penyesatan dengan memberi sarana atau keterangan.[20] *Uitlokker* tidak mewujudkan tindak pidana secara materiil atau langsung tetapi melalui orang lain (*pleger*). Dalam hal ini pembuat mateiil dapat dimintai pertanggungjawaban.

G. Definisi Operasional

Penelitian ini menggunakan pembatasan beberapa definisi, sebagai berikut:

1. Tindak pidana *phishing* adalah tindakan melawan hukum berupa pengelabuan guna mendapatkan informasi data pribadi korban dengan menggunakan komputer dan internet sebagai objek kejahatan. Penyalahgunaan data pribadi dilakukan oleh *phishers* setelah korban pengelabuan memberikan informasi data pribadi tersebut yang diberikannya secara sukarela akibat ketidaktahuannya.
2. Modus operandi adalah cara atau teknik yang berciri khusus dari seorang atau kelompok penjahat dalam melakukan perbuatan jahatnya yang melanggar hukum dan merugikan orang lain, baik sebelum, ketika, dan sesudah perbuatan kriminal tersebut dilakukan.[21]

[20] Pasal 55 ayat (1) angka 2e Kitab Undang-Undang Hukum Pidana.

[21] Kurniawan and Pujiyono, "Modus Operandi Korupsi Pengadaan Barang Dan Jasa Pemerintah Oleh PNS.", *Jurnal Law Reform*, Edisi No. 1 Vol. 14, Fakultas Hukum Universitas Diponegoro, 2018, hlm. 119.

3. Pertanggungjawaban pidana (*toereken-baarheid*) adalah kewajiban individu atau korporasi untuk menanggung konsekuensi atas perbuatannya karena telah melakukan suatu kejahatan yang merugikan.

H. Metode Penelitian

1. Jenis Penelitian

   Jenis penelitian yang digunakan adalah penelitian hukum normatif. Metode penelitian hukum normatif diartikansebagai sebuah metode penelitian atas aturan-aturan perundangan baik ditinjau dari sudat hirarki perundang-undangan (*vertikal*), maupun hubungan harmoni perundang-undangan (*horizontal*).[22] Penelitian hukum ini dilakukan dengan cara mengkaji asas-asas hukum, teori hukum, bahan-bahan hukum kepustakaan yang berasal dari peraturan perundang-undangan, dan berbagai literatur hukum yang berkaitan dengan substansi penelitian.

2. Objek Penelitian

   Objek dalam penelitian ini adalah:

   a. Modus operandi tindak pidana *phishing* yang terjadi di Surabaya.
   b. Pertanggungjawaban pidana pelaku tindak pidana *phishing* yang terjadi di Surabaya.

[22] Muhaimin, *Metode Penelitian Hukum*, Ctk. Pertama, Mataram University Press, NTB, 2020, hlm. 30.

3. Metode Pendekatan

Metode pendekatan yang digunakan dalam penelitian ini adalah:

a. Pendekatan perundang-undangan (*statute approach*) merupakan penelitian yang mengutamakan bahan hukum berupa perundang-undangan. Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan yang bersangkut paut dengan permasalahan (isu hukum) yang sedang dihadapi.

b. Pendekatan kasus (*case approach*) adalah penelitian yang membangun argumentasi hukum dalam prespektif kasus konkret yang terjadi dilapangan.

4. Sumber Data

Karena merupakan penelitian hukum normatif maka digunakan data sekunder. Data Sekunder bersumber pada bahan-bahan kepustakaan. Data sekunder terdiri atas:

a. Bahan Hukum Primer

Bahan hukum primer adalah bahan hukum yang mempunyai kekuatan mengikat secara umum (perundang-undangan) atau mempunyai kekuatan mengikat bagi pihak pihak berkepentingan (kontrak, konvensi, dokumen hukum, dan putusan hakim). [23] Dalam penelitian ini bahan hukum primer yang digunakan adalah:

[23] Bachtiar, *Metode Penelitian Hukum*, Ctk.Pertama, UNPAM PRESS, Tangerang Selatan, 2018, e-book, hlm. 141.

1) Putusan Nomor 1193/Pid.Sus/2021/PN.SBY dengan terdakwa Michael Zeboth Melki Sedek Boas Purnomo.
2) Putusan nomor 1194/Pid.Sus/2021/PN.SBY dengan terdakwa Shofiansyah Fahrur Rozi.
3) Putusan Nomor : 2205/Pid.Sus/2021/PN.SBY dengan terdakwa Rico Aprianza Bin Totok Markistian.
4) Putusan nomor 2182/Pid.Sus/2021/PN.SBY dengan terdakwa Gabriel Fransisco.
5) Putusan nomor 2206/Pid.Sus/2021/PN.SBY dengan terdakwa Thofan Permana.
6) Putusan Nomor : 1855/Pid.Sus/2021/PN.SBY dengan terdakwa Rohmat Hidayat.
7) Putusan nomor 1837/Pid.Sus/2021/PN.SBY dengan terdakwa Harry Togu Setiawan.
8) Putusan nomor: 1872/Pid.Sus/2021/PN.SBY dengan terdakwa Alik Dakirin.
9) Kitab Undang-Undang Hukum Pidana.
10) Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

b. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberi penjelasan terhadap bahan hukum primer (buku ilmu hukum, jurnal hukum, laporan hukum, dan media cetak, atau elektronik).[24]

c. Hukum Tersier

Bahan hukum tertier adalah bahan hukum yang memberi penjelasan terhadap bahan hukum primer dan bahan hukum sekunder (rancangan undang-undang, kamus hukum, dan ensiklopedia).[25]

5. Metode Pengumpulan Data

Adapun metode pengumpulan data yaitu dengan berdasarkan studi pustaka dan studi dokumen. Studi pustaka mengkaji literatur seperti buku dan jurnal ilmiah. Sedangkan studi dokumen mengkaji peraturan perundang-undangan dan putusan pengadillan terkait dengan permasalahan yang akan diteliti.

6. Teknik Analisis Data

Analisis data yang digunakan dalam penelitian ini adalah data deskriptif kualitatif yang meliputi kegiatan mengklasifikasikan data, editing, penyajian hasil analisis dalam bentuk narasi, dan pengambilan kesimpulan.

[24] *Ibid.*
[25] *Ibid.*

I. Kerangka Skripsi

Penelitian ini dituangkan dalam bab-bab yang disusun secara sistematis sebagai berikut.

BAB I yaitu pendahuluan yang akan menjelaskan mengenai Latar Belakang Masalah, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Orisinalitas Penelitian, Tinjauan Pustaka, Metode Penelitian dan Kerangka Skripsi.

BAB II menguraikan tinjauan Pustaka mengenai hal-hal yang dikaji berdasarkan judul, berisi tinjauan umum tentang tindak pidana *phishing*, modus operandi, pertanggungjawaban pidana, delik penyertaan, dan tindak pidana *phishing* dalam islam.

BAB III menjelaskan hasil penelitian pada objek yang ditetapkan pada penelitian ini sesuai dengan judul dan rumusan masalah yang telah dicantumkan yaitu modus operandi dan pertanggungjawaban pidana *phishing* melalui studi putudan pengadilan dari Putusan Pengadilan Surabaya.

BAB IV sebagai bab terakhir yang memuat kesimpulan berupa ringkasan jawaban atas permasalahan yang telah diteliti serta memuat saran yang berisi hal-hal sebagai usulan untuk dilakukan perbaikan kedepannya.

BAB II

TINDAK PIDANA *PHISHING*, MODUS OPERANDI, PERTANGGUNGJAWABAN PIDANA, DAN DELIK PENYERTAAN

A. Tindak Pidana *Phishing*

1. Pengertian Dan Unsur-Unsur Tindak Pidana *Phishing*

Phishing merupakan salah satu bentuk kejahatan internet berupa upaya seseorang untuk mendapatkan atau mencuri informasi atau data pribadi *(identity theft)* yang bersifat rahasia dengan cara pengelabuan. Pengelabuan yang dimaksud adalah percobaan penipuan dengan cara menyamar sebagai seseorang atau suatu ensitas terpercaya *(legitimate organization)* yang biasanya berkomunikasi melalui media komunikasi elektronik, seperti surat elektronik atau pesan instan. Informasi yang diperoleh tersebut dapat langsung dimanfaatkan untuk melakukan tindakan tidak bertanggung jawab seperti penyalahgunaan akun ataupun dijual kepada pihak lain.

Menurut kamus besar bahasa indonesia (KBBI), arti data pribadi adalah data yang berkenaan dengan ciri seseorang, misalnya nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.[26] Selain data pribadi, yang menjadi sasaran seorang *phishers* adalah data akun berupa u*sername* beserta kata sandi, dan data finansial berupa informasi kartu kredit ataupun rekening.

[26] https://kbbi.lektur.id/data-pribadi, diakses tanggal 25 Mei 2022, pukul: 11.47.

Di Indonesia sendiri, Perlindungan terhadap data pribadi telah diatur dalam bentuk Peraturan Menteri (PERMEN) No 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDP) ditetapkan 7 November 2016, diundangkan dan berlaku sejak 1 Desember 2016. Diundangkannya Peraturan Perlindungan Data Pribadi diharapkan pemerintah dapat mencegah *profiling* dan eksploitasi data pribadi masyarakat Indonesia serta penghapusan data pribadi yang diperoleh secara melawan hukum.[27]

Pada praktiknya, *phishing* umumnya dilakukan secara sistematis dengan riset terlebih dahulu malalui akun media sosial seperti *Facebook*, *LinkedIn*, dan berbagai media lain untuk mendapatkan informasi target dan jaringan sosialnya.[28] Selanjutnya, *phishers* akan melakukan penyamaran identitas dengan mengangkat topik yang relevan dan menarik untuk memikat target sehingga mendapatkan kepercayaan mereka untuk mengisi *link* yang dikirimkan tersebut. Pengiriman tautan berupa link atau surat elektronik (surel) yang telah dimodifikasi oleh *phishers* dapat dikirimkan melalui media sosial atau media komunikasi berbasis internet komersial yang umum digunakan.

Berkenaan dengan unsur-unsur *phishing*, kegiatan *phishers* haruslah mengandung suatu unsur melawan hukum dan unsur kesalahan untuk dapat

---

[27] Edmon Makarim, *Perlindungan Privacy dan Personal* Data, terdapat dalam https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114522-4891.pdf, diakses tanggal 8 Juni 2022 pukul:18.45.

[28] Algonz D.B. Raharja, *Phishing: Pengertian, Jenis, Ciri dan Tips yang Penting Untuk Menghindarinya*, terdapat dalam https://www.ekrut.com/media/*phishing*-adalah, diakses tanggal 8 Juni 2022, pukul:19.00.

dikategorikan sebagai suatu tindak pidana. Unsur melawan hukum dalam *phishing* terletak pada cara mendapatkan informasi elektronik maupun informasi pribadi korban yang dilakukan secara ilegal. Kegiatan atau cara-cara ilegal tersebut yang selanjutnya disebut dengan modus operandi. Perlu di ketahui bahwa terdapat perbuatan mengakses informasi elektronik milik orang lain yang diperbolehkan menurut hukum. Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1997 tentang Perbankan yang tercantum dalam Pasal 41 menentukan bahwa suatu informasi dapat ditujukkan kepada pejabat pajak untuk kepentingan perpajakan. [29]

Unsur kesalahan dalam tindak pidana dibedakan menjadi tindak pidana yang dilakukan dengan sengaja dan/atau tidak sengaja. Kejahatan *phishing* merupakan perbuatan yang dilakukan dengan adanya komputer yang tersambung pada jaringan, unsur kesalahan dalam kejahatan ini menjadi relatif lebih mudah untuk dikategorikan. Kategori yang dimaksud adalah kejahatan yang dilakukan menggunakan komputer dan jaringan, diperlukan pengetahuan, serta kemampuan yang lebih dibidang teknologi informasi daripada orang kebanyakan.

Kejahatan yang memanfaatkan teknologi dapat dikatakan dengan pasti bahwa dilakukan dengan suatu unsur kesengajaan. Dengan kata lain, kegiatan *phishing* mutlak sepenuhnya mengandung unsur kesengajaan

[29] Destya Fidela Pratiwi, "Pertanggungjawaban Tindak Pidana Skimming", *Jurnal Hukum*, Edisi No.4, Vol. 2, Fakultas Hukum Universitas Airlangga , 2019, hlm. 1216.

karena *phishers* melakukannya secara sadar. Selain itu untuk dapat tindakan pidana tersebut diperlukan suatu perencanaan yang terstruktur dan terarah.

2. Pengaturan Tindak Pidana *Phishing*

Peraturan terkait dengan tindakan-tindakan kriminal berdasarkan hukum positif Indonesaia secara umum diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Ketentuan-ketentuan khusus di bidang pidana saat ini telah ada untuk sektor-sektor tertentu yang dikenal dengan tindak pidana khusus, tetapi belum satu pun undang-undang yang mengatur mengenai kejahatan di bidang teknologi informasi secara khusus. Namun, negara telah mengklasifikasikan kejahatan siber ke dalam dalam KUHP dan Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Pada dasarnya KUHP dan UU ITE mengatur terkait kegiatan atau cara yang dilakukan oleh pelaku kejahatan siber, sehingga untuk mengetahui jenis pelanggarannya perlu di ketahui terlebih dahulu unsur-unsur tindak pidananya. Dalam hal kejahatan siber berupa *phishing*, ditemukan unsur yang tidak hanya melakukan pemalsuan *website* yang di *deface* menyerupai *website* aslinya, namun memiliki tujuan lain yaitu untuk mendapatkan identitas milik orang lain untuk digunakan secara ilegal tanpa diketahui oleh pemilik asli identitas tersebut. Adapun beberapa unsur-unsur tindak pidana yang berpotensi menjerat pelaku *phishing*, antara lain:

a. Penipuan

Kegiatan *phishing* merupakan kegiatan yang pada dasarnya menipu seseorang dengan mengatasnamakan pelaku sebagai orang lain. Penipuan diatur dalam Pasal 378 KUHP, dengan bunyi sebagai berikut:[30]

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

b. Manipulasi

Kegiatan *phishing* memiliki tahap berupa mengirimkan surat elekronik (*e-mail*) yang seolah-olah asli untuk memanipulasi target sehingga mau untuk mengikuti segala instruksi tersirat seorang *phishers*. Dalam hal ini *phishers* dapat dijerat dengan Pasal 35 *jo*. Pasal 51 UU ITE, bahwa:[31]

> Setiap orang yang melakukan penciptaan Informasi Elektronik dan/atau Dokumen Elektronik agar dianggap seolah-olah data yang otentik diancam dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak dua belas miliar rupiah.

c. Penerobosan

Tahap ini merupakan bentuk dari pemanfaatan informasi korban yang telah didapat dengan cara menerobos atau menjebol suatu sistem elektronik melalui jaringan. Penerobosan dengan menggunakan

[30] Pasal 378 Kitab Undang-Undang Hukum Pidana.

[31] Pasal 35 jo 51 PasalUndang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

identitas akun berupa *username* dan *password* korban dengan tanpa hak, *phishers* dapat dijerat dengan Pasal 30 ayat (3) *jo*. Pasal 46 ayat (3) UU ITE yang berbunyi:[32]

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

d. Memindahkan atau Mentransfer

Kegiatan ini berupa pemanfaatan informasi berupa memindahkan atau mentransfer informasi dan/atau dokumen elektronik milik korban, seperti saldo tabungan ataupun menjual informasi korban kepada pihak ketiga. Dalam hal ini *phishers* dapat dijatuhi hukuman berdasarkan Pasal 32 ayat (2) *jo*. Pasal 48 ayat (2) UU ITE, bahwa:[33]

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak, ipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

Segala bentuk kegiatan telah memiliki dasar hukum dapat dijeratnya *phishers* dengan sanksi pemidanaan, namun yang menjadi kendala adalah proses penegakan sebelum masuk ke tahap penuntutan hingga ke meja hijau. Aparat penegak hukum saat ini dituntut untuk meningkatkan keahlian

[32] Pasal 30 ayat (3) jo. Psdsl 46 syst (3) Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

[33] Pasal 32 ayat (2) jo. Pasal 48 ayat (2) Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

dibidang ITE terutama bagi penyidik karena tugasnya untuk mencari dan mengumpulkan bukti agar kasus menjadi terang. Dalam hal ini, kendala penegakan hukum oleh aparat hukum antara lain:[34]

1) Dibutuhkan banyak waktu untuk dilakukannya penyidikan, mengingat *locus delicti* terjadi di dunia maya;
2) Proses penyidikan yang memerlukan ahli ITE mengingat kejahatan *phishing* berbeda dengan kejahatan konvensional;
3) Minimnya informasi *phishers*, mengingat keahliannya dalam menyamar sebagai orang lain;
4) Barang bukti digital yang mudah dihilangkan oleh pelaku sebelum dilakukannya penyitaan;
5) Minimnya sumber daya anggota yang mempunyai keahlian dalam penyelidikan dan penyidikan kasus-kasus ITE;
6) Minimnya peralatan dan laboratorium forensik digital dalam mendukung pengungkapan tindak pidana.

B. Modus Operandi

Pengertian modus operandi dalam lingkup kejahatan adalah penggunaan cara atau teknik yang secara khusus menjadi ciri pelaku kejahatan dalam melakukan kejahatannya. Modus operandi berasal dari Bahasa Latin yang berarti tata cara, cara bergerak atau cara melakukan sesuatu. Sehingga dapat

[34] Puteri Hikmawati, Et.al, *Penegakan Hukum Terhadap Tindak Pidana Dalam UU ITE*, terdapat dalam https://berkas.dpr.go.id/puslit/files/infografis/infografis-public-72.pdf, diakses tanggal 21 Juni 2022, pukul : 01.03.

disimpulkan bahwa modus operandi adalah tindakan yang dilakukan oleh individu atau kelompok kriminal dalam melakukan kejahatan. Istilah ini digunakan untuk menggambarkan kebiasaan dan cara kerja seseorang. Modus operandi dalam Bahasa Inggris sering disingkat dengan "M.O". Istilah ini sering digunakan oleh kepolisian untuk merujuk pada kejahatan dan metode yang digunakan oleh pelaku. Hal ini juga digunakan dalam profil kriminal individu untuk mengeksekusi kejahatan, mencegah deteksi dan/atau memfasilitasi pelarian.[35]

Modus operandi dalam setiap kejahatan tentunya beragam, sehingga perlu diidentifikasi terlebih dahulu bentuk kejahatannya. Menurut Eshleman, J.Ross, dan Barbara G. Gashion dalam bukunya yang berjudul *Sociology* membedakan bentuk-bentuk kejahatan yang dianggap mengganggu keamanan umum dan sering membahayakan bangsa, antara lain:[36]

1. *Blue Collar Crime*

   Kejahatan kerah biru kejahatan yang dilakukan dengan cara tradisional atau konvensional. Kejahatan yang dilakukan identik dengan adanya tindak kekerasan seperti pencopetan, pembegalan, ataupun perampokan. Pelaku kejahatan kebanyakan adalah dari kelas ekonomi bawah.[37]

---

[35] Muhammad Maulana Zaki, "Aspek Pidana Cyberstalking Sebagai Salah Satu Bentuk Cybercrime", *Jurist-Diction*, Edisi No. 3, Vol. 5, Fakultas Hukum Universitas Airlangga, 2022, hlm.5.

[36] Dwi Julianti, *Pengertian dan Jenis-Jenis Kiminalitas*, terdapay dalam https://www.zenius.net/blog/pengertian-jenis-kriminalitas, diakses tanggal 10 Oktober 2022, pukul: 20.20.

[37] Made Sugi Hartono, "Korupsi Kebijakan Oleh Pejabat Publik (Suatu Analisis Perspektif Kriminologi)", *Jurnal Komunikasi Hukum*, Edisi No.2, Vol. 2, Fakultas Hukum Universitas Gadjah Mada, 2016, hlm. 220.

2. *White Collar Crime (WCC)*

   Kejahatan kerah putih merupakan kejahatan yang dilakukan dengan penyalahgunaan jabatan. Dalam hal ini pelaku kejahatan dapat diidentifikasi sebagai seseorang dari kelas ekonomi atas. Tindak pidana korupsi dan kecurangan merupakan contoh dari kejahatan ini.[38]

3. *Victimless Crime*

   Victimless Crime biasa disebut dengan kejahatan tanpa korban. Dalam hal ini diidentifikasikan dengan perbuatan tercela dan merugikan dirinya sendiri.[39] Contoh kejahatan tanpa korban adalah penyalahgunaan narkoba dan minuman keras.

4. *Organized Crime*

   Organized crime merupakan kejahatan berencana atau atau kejahatan yang telah diorganisir sebelumnya. Kejahatan ini identik dengan perbuatan yang dilakukan oleh mafia atau suatu perkumpulan rahasia yang bergerak di bidang kejahatan, seperti bandar narkoba, rentenir, judi, dan bisnis ilegal.[40]

5. *Corporate Crime*

   Corporate crime dalam perkembangannya dapat di inventarisir dengan beberapa bentuk kejahatan dan korban kejahatan korporasi ini berasal dari *WCC* atau kelas ekonomi atas yang menyalahgunakan kewenangannya.

---

[38] *Ibid*, hlm. 219.

[39] Erika Magdalena Chandra, "Victimless Crime in Indonesia: Should We Punished Them?", *Padjadjaran Journal of Law*, Edisi No.2, Vol. 6, Fakultas Hukum Universitas Padjadjaran, 2019, hlm. 217.

[40] *Ibid*, hlm. 223.

Bentuk kejahatan yang dilakukan antara lain, pelanggaran terhadap konsumen, pencemaran lingkungan, pelanggaran adminisratif, finansial, perburuhan, manufaktur, dan perdagangan yang tidak sehat.[41]

6. *Cyber Crime*

   Cybercrime adalah jenis kejahatan baru yang muncul di dunia ini karena globalisasi.[42] Saat ini tidak dapat disangkal bahwa kejahatan ini telah berkembang dari waktu ke waktu dan ada banyak kasus kejahatan ini hingga hari ini. Semua bangsa berlomba-lomba untuk memajukan teknologi mereka untuk hal yang positif, namun banyak orang yang menyalahgunakan teknologi untuk perilaku negatif.[43] *Cybergrooming, Cyber bullying, cyberstalking*, penipuan pekerjaan online, merupakan kejahatan mayantara yang tengah berkembang di dunia internet kebanyakan.

7. Kejahatan Transnasional

   Kejahatan transnasional merupakan terencana dan terorganisir, dimana perencaan, eksekusi, dan korbannya dapat melintasi batas negara. Kejahatan transnasional dalam hubungan internasional bukanlah fenomena yang baru. Beberapa faktor penyumbang kompleksitas perkembangan kejahatan transnasional adalah globalisasi, migrasi atau

---

[41] Rodliyah, "Konsep Pertanggungjawaban Pidana Korporasi *(Corporate Crime)* dalam Sistem Hukum Pidana Indonesia", *Jurnal Kompilasi Hukum*, Edisi No. 1, Vol. 5, Fakultas Hukum Universitas Mataram,2020, hlm. 197.

[42] Massulthan Rafi Wijaya, Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?, *Indonesian Journal Of Criminal Law Studies*, Edisi No.1, Vol. 5, Fakultas Hukum Universitas Negeri Semarang, 2020, hlm. 1.

[43] *Ibid*, hlm. 65.

perpindahan penduduk, dan pesatnya perkembangan teknologi informasi, dan komunikasi.

Globalisasi yang disertai dengan kemajuan teknologi komunikasi yang pesat menciptakan dunia tanpa batas (*borderless world*). Berbagai bentuk kejahatan lintas batas meningkat pesat dan dianggap sebagai ancaman keamanan. Melintasi batas negara dapat diartikan bahwa antara pelaku, korban, dan locus delictinya dilakukan di negara yang berbeda. Kegiatan-kegiatan seperti pencurian data, penyelundupan, dan perdagangan manusia dan senjata adalah tindakan yang sama sekali mengabaikan dan mengancam keamanan manusia, yang pada gilirannya mengancam keamanan nasional.[44]

Berdasarkan bentuk-bentuk kejahatan di atas jika dikaitkan dengan objek penelitian, *phishing* selain masuk ke dalam kejahatan mayantara (*cybercrime*) juga masuk ke dalam bentuk kejahatan transnasional. Adanya perkembangan dalam berbagai bidang yang menjadi pendorong utama pergerakan ke *Industry 4.0*, fenomena *phishing* dalam pada 5 tahun terakhir ini menjadi semakin mencemaskan. Peningkatan kasus tersebut didasarkan pada laporan yang masuk ke Indonesia *Anti-Phishing Data Exchange* (IDADX), bahwa selama lima tahun terakhir telah terjadi 32.296 kasus *phishing* di domain ".ID".[45]

---

[44] Humphrey Wangke, *Kejahatan Transnasional Di Indonesia Dan Upaya Penanganannya*, Cetakan pertama, P3DI Sekertariat Jendral DPR RI, Jakarta Pusat, 2011, hlm. 3.

[45] CNN Indonesia, *3.180 Serangan Phishing Awal 2022, Lembaga Keuangan Jadi Sasaran Utama*, terdapat dalam https://www.cnnindonesia.com/teknologi/20220325194851-192-776315/3180-serangan-*phishing*-awal-2022-lembaga-keuangan-jadi-sasaran-utama, diakses tanggal 25 Mei 2022, pukul:13.00.

Penggunaan non-tunai sebagai metode transaksi praktis saat ini semakin mendorong masyarakat untuk beralih dan meninggalkan metode transaksi tunai seperti sebelumnya. Perubahan tersebut dapat dilihat melalui praktisnya berbelanja menggunakan berbagai aplikasi *e-commerce*, membayar parkir menggunakan *e-money*, serta pembayaran di swalayan menggunakan *QRIS* (*Quick Response Code Indonesian Standard*). Hal tersebut juga merupakan bentuk dari program Gerakan Nasional Non-Tunai yang di canangkan oleh Bank Indonesia (BI).[46] Dalam hal ini, segala bentuk macam pembayaran saat ini mulai beralih ke mode digital dan serba online yang artinya membutuhkan suatu jaringan untuk mengaksesnya. Sehingga seakan-akan menambahkan celah bagi *phishers* untuk lebih menguntungkan dirinya.

Terdapat beberapa alasan mengapa tingkat kejahatn *phishing* cenderung bertambah setiap tahunnya, antara lain:

a. Kurangnya pengetahuan akan apa itu *phishing;*
b. Adanya *curiousity gap* (kesenjangan yang membuat penasaran pembaca meng-klik tautan untuk menjawab keingitahuan mereka); dan
c. Mudah terkena *clickbait* atau umpan klik yang dibuat dalam konten web.

Guna mempermudah menangani kasus kejahatan yang dikenal dengan *phishing* ini, maka pemerintah harus mengetahui dan memahami cara beroperasinya terlebih dahulu. Perlu diketahui bahwa modus operandi *phishing* ini berbeda dengan tindak kejahatan konvensional. Perbedaan yang mencolok

[46] Detik Finance, *Bayar Parkir Elektronik Bisa Pakai Kartu Apa Saja?,* terdapat dalam https://finance.detik.com/moneter/d-2817485/bayar-parkir-elektronik-bisa-pakai-kartu-apa-saja, diakses tanggal 25 Mei 2022, pukul:12.33.

terdapat dalam *locus delicti* atau tempat kejahatan perkara, karena sangat sulitnya melokalisir jaringan internet. Pasal 32 ayat (2) UU ITE telah memberikan sedikit penjelasan mengenai modus operandi tindak pidana *phishing* yaitu dengan memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.

C. Pertanggungjawaban Pidana

1. Pengertian Pertanggungjawaban Pidana

Subjek hukum dalam pertanggungjawaban pidana adalah setiap orang yang melakukan perbuatan pidana. Pertanggungjawaban pidana diterapkan terhadap setiap orang yang melakukan perbuatan pidana. Dengan demikian, terjadinya pertanggungjawaban pidana diakibatkan oleh kesalahan berupa tindak pidana yang dilakukan oleh seseorang, dan telah ada aturan yang mengatur tindak pidana tersebut. Pada hakikatnya yang menjadi pokok pembahasan dari pertanggungjawaban pidana adalah permasalahan dapat atau tidak dapat dipidananya pelaku tindak pidana.

Syarat dalam pembebanan pertanggungjawaban pidana pada pelaku tindak pidana *cybercrime* adalah terpenuhinya segala unsur tindak pidana dan tujuan dari perbuatan tersebut dapat dibuktikan bahwa memang sengaja dilakukan dengan keadaan sadar akan dicelanya perbuatan tersebut oleh undang-undang. Dari pernyataan tersebut dikenal asas *green straf zonder*

schuld atau tiada pidana tanpa kesalahan.[47] Dengan demikian unsur adanya kesalahan merupakan dasar untuk menentukan pertanggungjawaban pidana.[48] Pertanggungjawaban pidana juga akan menentukan dapat dipidananya pembuat sebagai suatu akibat atau konsekuensi dari tindak pidana yang telah dilakukan.[49] Pemidanaan dapat dilaksanakan apabilah telah terbuktinya tidak pidana dan memenuhi unsur-unsur pertanggungjawaban pidana.

Dari segala persiapan yang dilakukan *phishers*, tentu bukanlah hal yang sulit karena keahliannya di bidang teknologi. Siapapun dapat menjadi korban jika *phishers* menerapkan *random* target, sehingga kelalaian seseorang dalam sangat menguntungkan bagi *phishers*. Terdapat sebuah teori yang menyatakan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan (*crime is product of society its self).*[50] Oleh karena itu, masyarakat memerlukan bekal berupa pengetahuan tentang pengoperasian suatu teknologi agar tidak berpotensi menjadi korban kejahatan siber berupa *phishing* ini.

2. Unsur-unsur Pertanggungjawaban Pidana

Moeljatno mendefinisikan suatu perbuatan pidana sebagai perbuatan yang dilarang oleh suatu aturan hukum, dan larangan disertai ancaman

---

[47] Moeljatno, *Asas-Asas Hukum Pidana*, Cetakan ketiga, PT.Bina Aksara, Jakarta, 1995, hlm:153.

[48] Agus Rusianto, *Tindak Pidana dan Pertanggungjawaban Pidana*, Cetakan pertama, Prenadamedia Group, Jakarta, 2016, hlm. 235.

[49] *Ibid*, hlm. 236.

[50] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Cetakan pertama, PT. Refika Aditama, Bandung, 2010, hlm. 39.

(sanksi) yang berupa pidana tertentu bagi barang siapa yang melanggar larangan tersebut.[51] Larangan ditujukan kepada perbuatan (suatu keadaan atau kejadian yang ditimbulkan oleh perbuatan orang).[52] Seseorang disebut telah melakukan perbuatan pidana apabila memenuhi unsur objektif dan subjektif, yaitu :[53]

a. Unsur Objektif atau yang biasa disebut *actus reus* mengarah kepada suatu perbuatan yang bertentangan dengan hukum dan perbuatan pidana yang dilakukan tidak terdapat alasan pembenar atau peniadaan sifat melawan hukum, dan;
b. Unsur Subjektif atau yang biasa disebut *mens rea* mengarah kepada pelaku yang melakukan perbuatan pidana dengan unsur kesalahan dalam bentuk kesengajaan (*opzet*) dan atau kealpaan (*culpa*), sehingga perbuatan yang melawan hukum tersebut dapat dipertanggungjawabkan kepadanya.

Salah satu syarat lain dalam pertanggungjawaban pidana adalah unsur kemampuan bertanggung jawab pelaku perbuatan pidana. Kemampuan untuk bertanggung jawab telah ditegaskan dalam Pasal 44 ayat (1) KUHP, bahwa:[54]

Barang siapa melakukan perbuatan yang tidak dapat dipertanggungjawabkan padanya, disebabkan karena jiwanya cacat dalam

[51] Moeljatno, *Asas-Asas Hukum Pidana,* Cetakan ketiga, PT.Bina Aksara, Jakarta, 1995, hlm: 54.
[52] *Ibid.*
[53] *Ibid*, hlm. 63.
[54] Pasal 44 ayat (1) Kitab Undang-Undang Hukum Pidana.

tumbuhnya (*gebrekkige ontwikkeling*) atau terganggu karena penyakit *(ziekelijke storing*), tidak dipidana.

Menurut E.Y. Kanter dan S.R. Sianturi yang dapat dikatakan seseorang mampu bertanggungjawab (*toerekeningsvatbaar*), bilamana pada umumnya:[55]

a. Keadaan jiwanya:
   1) Tidak terganggu oleh penyakit terus-menerus atau sementara *(temporair)*;
   2) Tidak cacat dalam pertumbuhan (gagu, idiot, *imbecile*, dan sebagainya), dan;
   3) Tidak terganggu karena terkejut, *hypnotisme*, amarah yang meluap, pengaruh bawah sadar/*reflexe bewenging*, melindur/*slaapwandel*, menganggu karena demam/*koorts*, nyidam dan lain sebagainya. Dengan perkataan lain didalam keadaan sadar.
b. Kemampuan jiwanya:
   1) Dapat menginsyafi hakekat dari tindakannya;
   2) Dapat menentukan kehendaknya atas tindakan tersebut, apakah akan dilaksanakan atau tidak; dan
   3) Dapat mengetahui ketercelaan dari tindakan tersebut.

Perbuatan pidana dalam hal ini hanya merujuk kepada dilarangnya suatu perbuatan. Namun, seseorang yang telah terbukti melakukan suatu perbuatan pidana tidak selalu dapat dijatuhi pidana. Hal ini dikarenakan

[55] E. Y. Kanter & S.R. Sianturi, *Asas -Asas Hukum Pidana di Indonesia dan Penerapannya*, Cetakan ketiga, Storia Grafika, Jakarta, 2012, hlm. 249.

dalam pertanggung jawaban pidana, tidak hanya dilihat dari perbuatannya saja, melainkan dilihat juga dari unsur kesalahannya. Kesalahan dalam hal ini terdiri dari kemampuan bertanggung jawab, kesengajaan, kealpaan, dan tidak ada alasan pemaaf. Hal tersebut memiliki konsekuensi bagi Hakim untuk selalu mempertimbangkan unsur-unsur tersebut. Konsekuensinya adalah apabila tidak ada adanya keadaan-keadaan demikian, hakim harus menyatakan pelaku tidak dipertanggungjawabkan atau menyatakan pembuat dilepaskan dari segala tuntutan hukum (*ontslag van alle rechtsvervolging*).[56]

D. Delik Penyertaan

Kejahatan mayantara pada umumnya tidak dilakukan seorang diri. Dalam hal dilakukannya kejahatan, dikenal yang dinamakan dengan delik penyertaan. Delik pernyertaan (*deelneming*) merupakan orang yang dengan sengaja ikut serta melakukan suatu perbuatan (*medeplegen*) dan pembantuan (*medeplichtigheid*).[57] Delik penyertaan telah diatur dalam hukum yang berlaku, yaitu terdapat dalam Pasal 55 dan Pasal 56 KUHP.

Tindak pidana yang dilakukan oleh dua orang atau lebih, sehingga hubungan orang-orang yang terlibat tersebut dibatasi oleh Pasal 55 ayat (1), yaitu petindak peserta (*mededader*) yang terdiri dari pelaku pelaksana, pelaku penyuruh, pelaku peserta, pelaku penganjur, dan tidak dimaksudkan bagi satu

[56] Agus Rusianto, *Op. Cit*, hlm. 237.

[57] Ike Indra, "Pembantuan Dan Penyertaan (*Deelmening*) dalam Kasus Perkosaan Anak", *Jurnal Hukum Media Iuris*, Edisi No. 2, Vol. 1, Fakultas Hukum Universitas Airlangga, 2018, hlm. 284.

pelaksana dan yang satu pelaku pembantu.[58] Dengan adanya delik penyertaan, antara orang yang melakukan dan orang yang membantu melakukan tindak pidana dapat dikenakan masing-masing jenis sanksi pemidanaan sesuai dengan peran yang dimainkannya.

Berdasarkan pasal-pasal tersebut, penyertaan dibagi menjadi dua pembagian besar, yaitu:

1. Pembuat /*dader* (Pasal 55 KUHP) yang terdiri dari:[59]
   a. Pelaku (*pleger*)

      Pleger adalah orang yang secara materiil adalah seseorang yang melakukan perbuatan yang dapat menimbulkan akibat yang dilarang undang-undang, dan secara *persoonlijk* adalah seseorang yang nyata-nyata melakukan dan menyelesaikan perbuatan yang secara sempurna memenuhi semua unsur dari rumusan delik yang terjadi.[60] Menurut pasal 55 KUHP, yang melakukan perbuatan disini tidak melakukan perbuatan secara pribadi, melainkan dengan bersama-sama dengan orang lain dalam mewujudkan tindak pidana itu.

   b. Yang menyuruh melakukan (*doenpleger*)

      Doen Pleger adalah orang yang menyuruh orang lain untuk melakukan suatu perbuatan pidana, dimana secara yuridis orang

[58] Destya Fidela Pratiwi, "Pertanggungjawaban Tindak Pidana Skimming", *Jurnal Hukum*, Edisi No.4, Vol. 2, Fakultas Hukum Universitas Airlangga , 2019, hlm. 1221.

[59] Pasal 55 Kitab Undang-undang Hukum Pidana.

[60] Fahmi, "Perbedaan Penyertaan/Deelneming", terdapat dalam http://myprojectfamous.blogspot.com/2017/08/perbedaan-penyertaandeelneming-pleger.html, diakses tanggal 4 Juli 2022, pukul: 20.40.

yang disuruh dan akhirnya secara nyata melakukan perbuatan pidana dengan sarana yang tidak ditentukan dalam undang-undang.[61] *Doenpleger* adalah orang yang melakukan suatu tindak pidana dengan perantara orang lain, dan seseorang yang dijadikan perantara tersebut hanya digunakan sebagai alat yang dikendalikan oleh penyuruh. Dengan demikian, ada dua pihak, yaitu pembuat langsung (*manus ministra*), dan pembuat tidak langsung (*manus domina*).

Manus ministra dalam hal ini bertindak sebagai *pleger* yang hanya sebagai "alat instrumen" atau orang yang disuruh melakukan sehingga atas perbuatannya tidak dapat dipertanggungjawabkan.[62] Namun, terdapat kriteria-kriteria orang tersebut tidak dapat dimintai pertanggungjawaban di depan hukum, apabila:

1) Petumbuhan jiwanya tidak sempurna (Pasal 44 KUHP);
2) Perbuatannya dilaksanakan karena adanya paksaan (Pasal 48 KUHP);
3) Perbuatannya disesatkan.

c. Yang turut serta (*madepleger*)

Medepleger (pelaku peserta) merupakan keikutsertaan seseorang dalam melakukan tindak pidana, yang dalam hal ini

[61] Jan Remmelink, *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting KUHP Belanda dan padanannya Dalam KUHP Indonesia*, Cetakan pertama, PT. Gramedia Pustaka Utama, Jakarta, 2003, hlm. 309.

[62] Fahrurrozi, "Sistem Pemidanaan Dalam Penyertaan Tindak Pidana Menurut KUHP", *Jurnal Ilmu Hukum*, Volume 10 Nomor 1, Fakultas Hukum Universitas Muhamadiyah Mataram, 2019, hlm. 53.

tindak pidana yang perbuatan atau tindakannya hanya memenuhi sebagian unsur-unsur delik.[63] *Medepleger* adalah orang yang melakukan kesepakatan dengan orang lain untuk melakukan suatu perbuatan pidana dan secara bersama-sama pula Ia turut beraksi dalam pelaksanaan perbuatan pidana sesuai dengan yang telah disepakati. Dengan demikian, dalam penyertaan bentuk turut serta ini, dua orang atau lebih yang dikatakan sebagai *medepleger* tersebut semuanya harus terlibat aktif dalam suatu kerja sama pada saat perbuatan pidana dilakukan.

Seseorang dalam penyertaannya dapat disebut sebagai medepleger adalah dengan kriteria-kriteria sebagai berikut:

1) Secara sadar mengadakan kerjasama dalam melakukan tindak pidana;
2) Menyepakati untuk bekerjasamameskipun perbuatannya merupakan hal yang dilarang oleh undang-undang;
3) Pelaksanaan perbuatan dilakukan secara bersama-sama hingga berakhir dengan terselesaikannya delik yang bersangkutan.

d. Penganjur (*uitlokker*)

Setiap orang yang menggerakkan atau membujuk orang lain (*pleger*) untuk melakukan suatu tindak pidana dengan

[63] *Ibid*, hlm. 314.

menggunakan sarana-sarana yang telah ditentukan undang-undang secara limitatif, yaitu:[64]

1) dengan memberikan atau menjanjikan sesuatu;
2) dengan menyalahgunakan kekuasaan atau martabat;
3) dengan menggunakan kekerasan;
4) dengan menggunakan ancaman atau penyesatan;
5) dengan memberi sarana atau keterangan.

Penganjur adalah orang yang menghasut orang lain untuk melakukan tindak pidana, dan orang tersebut terhasut atau tergoda oleh usaha penganjur untuk melakukan tindak pidana berdasarkan Pasal 55 ayat (1) angka 2 KUHP. Bentuk penganjuran berupa *actor intelectualis*, yang menganjurkan orang lain (*actor materialis*) untuk melakukan tindak pidana.[65] *Uitlokker* tidak mewujudkan tindak pidana secara materiil atau langsung tetapi melalui orang lain (*pleger*).[66] Dalam hal ini pembuat materiil dapat dimintai pertanggungjawaban.

2. Pembantu /*madeplichtige* (Pasal 56 KUHP) yang terdiri dari:[67]
   a) Pembantu pada saat kejahatan dilakukan
   b) Pembantu sebelum kejahatan dilakukan.

[64] Pasal 55 ayat (1) ke-2 Kitab Undang-Undang Hukum Pidana.
[65] Moeljatno, *Op.Cit*, hlm 155.
[66] *Ibid.*
[67] Pasal 56 Kitab Undang-Undang Hukum Pidana.

Perbedaan antara pembantu pada saat dilakukannya kejahatan dan pembantu sebelum kejahatan dilaksanakan adalah bentuk pembantuan sebelum dilaksanakannya kejahatan dapat berupa memberikan bantuan melalui cara-cara dengan memberi kesempatan, memberi sarana, memberi keterangan.

Terdapat kemiripan makna antara *medeplegen* dan *medeplichtige* dan cara membedakannya tergolong sulit. Undang-undang dalam hal ini juga tidak memuat penjelasan serta batasannya, sehingga untuk memahami keduanya diserahkan kepada ahli ilmu hukum pidana. Turut serta (*medepleger*) dalam Pasal 55 KUHP di atas, dalam kaitannya dengan pertanggungjawaban pidana dihukum sebagai orang yang melakukan. Dengan demikian penyuruh, pembujuk, dan orang yang turut serta melakukan dianggap sebagai pelaku atau pembuat tindak pidana, sehingga ancaman pidananya sama. Sedangkan ancaman pidana pada pembantuan (*medeplicitge*) berdasarkan Pasal 57 ayat (1) dan ayat (2), yaitu maksimum pidana pokok terhaap kejahatan, dikurangi sepertiga, jika kejahatan diancam dengan pidana mati atau seumur hidup, dijatuhkan pidana penjara paling lama 15 (lima belas) tahun.[68]

Adanya pembedaan terhadap jenis-jenis perbuatan tidak hanya sebatas pada peranan yang dilakukan oleh seorang yang terlibat pada terwujudnya tindak pidana, tetapi juga memiliki implikasi pada putusan pengadilan yang membedakan antara turut serta dan pembantuan. Pokok persoalan dalam ajaran penyertaan (*deelneming*) adalah untuk menentukan bentuk hubungan antara

[68] Muladi Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Cetakan kedua, Alumni, Bandung, 1992, hlm. 46.

peserta-peserta tersebut yang kemudian menentukan pula pertanggungjawaban pidana dari masing-masing peserta, karena telah melakukan suatu tindak pidana (delik).

E. Tindak Pidana *Phishing* dalam Perspektif Hukum Islam

Tindak Pidana (*jarimah*) diartikan sebagai perbuatan kriminal yang dilakukan oleh orang-orang *mukallaf* (orang yang dapat dibebani kewajiban) yang mana perbuatan tersebut merupakan tindakan melawan peraturan perundang-undangan yang bersumber dari Alquran dan hadist. Al-Mawardi Mendefinisikan jarimah sebagai berikut:[69]

اَلْجَرَائِمُ مَحْظُوْرَاتٍ شَرْعِيَّةٌ زَجَرَ اللهُ تَعَالَى عَنْهَا بِحَدٍّ أَوْتَعْزِيْرٍ

Artinya: Segala larangan *syara'* (melakukan hal-hal yang dilarang dan atau meninggalkan hal-hal yang diwajibkan) yang diancam dengan hukuman *had* dan *ta'zir*.

Had merupakan segala hukuman yang telah ditentukan oleh *syara*', baik *syara'* yang bersumber dari Hak Allah maupun hak individu. Hak Allah dapat di contohkan dengan hukuman potong tangan untuk *jarimah* pencurian, dera seratus kali untuk *jarimah* zina, dan dera delapan puluh kali untuk *jarimah qadzaf* (menuduh orang lain berbuat zina). Sedangkan Hak Individu meliputi *qishash* dan *diyat*.[70]

[69] H. Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam*, Cetakan pertama, Sinar Grafika, Jakarta, 2004, hlm: 9.

[70] *Ibid*, hlm. 10.

Ta'zir merupakan hukuman yang belum ditentukan oleh *syara',* sehingga penetapan dan pelaksanaan diserahkan kepada *ulil amri* (penguasa) sesuai dengan bidangnya. Dalam hal ini yang memiliki wewenang untuk menetapkan peraturan hukum adalah badan legislatif (DPR), dan dalam hal pelaksanaan penetapan hukumnya diserahkan kepada badan pengadilan.[71] Setiap warga negara dihimbau untuk taat kepada penguasa demi terciptanya kesejahteraan kecuali dalam hal maksiat. Perintah untuk taat kepada Penguasa kecuali pada kemaksiatan terkandung dalam HR. Bukhari no. 7144 dan Muslim no. 1839, bahwa:[72]

> Dari Ibnu 'Umar, dari Nabi shallallahu 'alaihi wa sallam, beliau bersabda: Bagi setiap muslim, wajib taat dan mendengar kepada pemimpin (penguasa) kaum muslimin dalam hal yang disukai maupun hal yang tidak disukai (dibenci) kecuali jika diperintahkan dalam maksiat. Jika diperintahkan dalam hal maksiat, maka tidak boleh menerima perintah tersebut dan tidak boleh taat.

Dalam hal ini, jika terdapat aturan pemerintah, atau undang-undang yang dibuat dan sifatnya *mubah*, tidak menyelisihi ketentuan Allah, aturan tersebut harus dijalankan. Dalam perkembangannya, hukum Islam di Indonesia kemudian dibagi menjadi dua, yaitu:[73]

---

[71] *Ibid.*

[72] Muhammad Abduh Tuasikal, *Muttafaqun 'alaih : Taat pada Pemimpin Selain Perkara Maksiat*, terdapat dalam https://rumaysho.com/3727-taat-pada-pemimpin-pada-selain-perkara-maksiat.html, diakses tanggal 29 Juni 2022, pukul: 22.02.

[73] Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam*, Cetakan pertama, Sinar Grafika, Jakarta, 2004, hlm: 9.

1. Hukum Islam yang bersifat normatif, yaitu yang berkaitan dengan aspek ibadah murni, yang pelaksanaannya sangat tergantung kepada iman dan kepatuhan umat Islam Indonesia kepada agamanya.
2. Hukum Islam yang bersifat yuridis formal, yaitu yang berkaitan dengan aspek *muamalat* (khususnya bidang perdata dan diupayakan pula dalam bidang pidana sekalipun sampai sekarang masih dalam tahap perjuangan), yang telah menjadi bagian dari hukum positif di Indonesia.

Islam sebagai agama yang *rahmatan lil 'alamin* memiliki tujuan sebagai petunjuk dan pelajaran kepada manusia. Rasulullah SAW bersabda: Agama adalah nasihat.

Tindak pidana *phishing* merupakan salah satu metode penipuan atau tipu muslihat yang merupakan upaya seseorang untuk memperdayai orang lain, dengan akal licik dan strategi berupa memanipulasi atau pengelabuan. Dalam praktiknya, *phishers* akan berperan sebagai seseorang atau instansi terpercaya

وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ وَتَكْتُمُوا الْحَقَّ وَاَنْتُمْ تَعْلَمُوْنَ

(*spoofing*) dengan berbagai strategi agar target tidak dapat membedakannya. Tindakan tersebut pada dasarnya mengandung kebathilan atau kebohongan adalah salah satu perbuatan yang di larang, sebagaimana yang terkandung dalam surah Al-baqarah (2): 42, Allah SWT berfirman:[74]

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

[74] https://islam.nu.or.id/tafsir/tafsir-surat-al-baqarah-ayat-42-Tcchv, pada 29 Juni 2022, pukul:00.08.

Phishing merupakan suatu perbuatan yang terdapat unsur merugikan kepentingan umum maka perbuatan tersebut dianggap *jarimah* dan *phishers* layak untuk dikenakan hukuman. Didalam Islam terdapat istilah yang mana hukumannya diserahkan kepada hakim atau penguasa. Dalam *fiqh jinayah* terdapat tiga macam *jarimah*, yaitu:

a. *Jarimah Hudud*

Jarimah hudud adalah *jarimah* yang diancam dengan hukuman *had* atau hukuman yang telah ditentukan oleh *syara'* dan menjadi hak Allah. Dalam hal hukuman tersebut tidak dapat dihapuskan oleh perseorangan atau oleh masyarakat yang diwakili oleh negara.

b. *Jarimah Qisash* dan *Diat*

Jarimah qisash dan *diat* adalah *jarimah* yang diancam dengan hukuman yang telah ditentukan oleh *syara'* dan menjadi hak manusia (individu). Hukuman yang menjadi Hak Individu dapat berupa pembalasan yang setimpal atau pembayaran ganti rugi atas tindak pidana terhadap tubuh dan jiwa. Dalam hal ini hukuman tersebut dapat dihapuskan atau dimaafkan oleh korban atau keluarganya.

Pengertian *qishas* sebagaimana dikemukakan oleh Muhammad Abu Zahrah sebagaimana yang dikutip oleh Djazuli, adalah memberikan hukuman kepada pelaku perbuatan persis seperti apa yang dilakukan terhadap korban. Sedangkan *Diyat* adalah sejumlah harta yang wajib

diberikan karena suatu tindakan pidana kepada korban kejahatan atau walinya. *Diyat* disyariatkan dalam pembunuhan dan penganiayaan.[75]

c. *Jarimah Ta'zir*

Jarimah Ta'zir adalah perbuatan pidana yang bentuk dan ancaman hukumannya ditentukan oleh pengusa (hakim) sebagai pelajaran kepada pelakunya. Dalam pengertian istilah hukum islam merupakan hukuman yang bersifat mendidik yang tidak mengharuskan pelakunya dikenal had. *Jarimah Ta'zir* adalah *jarimah* yang diancam dengan hukuman yang belum ditentukan oleh *syara'*, melainkan diserahkan kepada ulil amri baik dalam hal penentuan dataupun pelaksanaan hukumnya. Hukuman *takzir* dijatuhkan untuk memberikan pelajaran kepadaterpidana atau orang lain agar tidak mengulangi kejahatan yang pernah dia lakukan. Jadi hukuman ini disebut dengan *uqubah mukhayyarah* (hukuman pilihan). Dalam hukuman *takzir* seorang hakim diberikan kebebasan untuk menentukan jenis hukuman *takzir* terhadap terpidana.

Dari berbagai hukum pidana islam di atas, maka tindak pidana *phishing* dalam perspektif *jinayah* masuk ke dalam *jarimah Takzir*. *Takzir* diartikan mencegah dan menolak, karena ia dapat mencegah pelaku *phishing* agar tidak mengulangi perbuatannya. *Takzir* juga diartikan mendidik karena dimaksudkan untuk mendidik dan memperbaiki pelaku agar ia menyadari perbuatan

[75] Mushlihin, *Pengertian Jarimah Qishas dan Diyat*, terdapat dalam https://www.referensimakalah.com/2013/04/pengertian-jarimah-qishas-dan-diyat.html, diakses tanggal 29 Juni 2022, Pukul:00.46.

*jarimah*nya, kemudian meninggalkan dan menghentikannya. Tindak pidana *phisihing* masuk ke dalam *jarimah ta'zir* karena sanksinya belum ditentukan dalam *nash*, sementara perbuatannya sudah ada dalam *nash*. Dengan demikian sanksi yang diberikan diserahkan kepada *ulil amri* baik dalam hal penentuan dataupun pelaksanaan hukumnya.

Pemberian sanksi dalam hal ini menjadi kewenangan penegak hukum dan pemberian sanksi didasarkan pada KUHP dan UU ITE. Alternatif hukuman jarimah *ta'zir* berupa hukuman penjara, skorsing atau pemecatan, pengasingan, ganti rugi, cambuk, teguran dengan kata-kata, dan jenis hukuman lain yang dipandang sesuai dengan pelanggaran yang dilakukan.

BAB III

MODUS OPERANDI TINDAK PIDANA *PHISHING* DAN PERTANGGUNGJAWABAN PIDANA TERHADAP *PHISERS* DI SURABAYA

(STUDI PUTUSAN PENGADILAN)

Perkembangan teknologi berperan besar dalam dinamika kehidupan masyarakat. Teknologi diibaratkan seperti pisau bermata dua yang artinya selain memberikan banyak hal yang bersifat positif, perkembangan teknologi juga menjadi salah satu penyumbang terbesar dampak negatif yang berupa muculnya motif kejahatan kontemporer yang dilakukan dengan memanfaatkan teknologi. Kondisi seperti ini secara tidak langsung membuat hukum sebagai sarana kontrol sosial juga terdapak. Dalam hal ini sudah sepantasnya hukum berkembang sesuai dengan perkembangan masyarakat secara dinamis. Seperti yang disampaikan oleh Satjipto di mana hukum hendaknya mampu mengikuti perkembangan zaman, mampu menjawab perubahan zaman dengan segala dasar di dalamnya, dan juga hukum harus mampu melayani masyarakat dengan menyandarkan pada aspek moralitas dan kemampuan dari sumber daya manusia penegak hukum itu sendiri.[76]

Adanya celah dan peluang yang ditimbulkan akibat laju teknologi namun tidak diimbangi dengan sumber daya manusia berupa tingkat integritas tinggi dapat menjadi salah satu sebab mengapa kasus *cybercrime* terus menngalami peningkatan

[76] Satjipto Rahardjo, *Ilmu Hukum*, Cetakan keenam, Citra Aditya Bakti, Bandung, 2006 hlm.11.

Kesenjangan sosial berupa semakin meningkatnya kebutuhan, jumlah kemiskinan tinggi, dan minimnya lapangan pekerjaan juga menjadi faktor mengapa seseorang memilih melakukan kejahatan siber sebagai ladang penghasilan instan. Dengan perkembangan yang serba digital, hampir seluruh penduduk dunia menggunakan media sosial yang merupakan *platform* sosial sebagai hasil dari penggabungan teknologi dan internet. Masyarakat berbondong-bondong melakukan digitalisasi namun tak banyak pula yang mengerti atau mengetahui bahwa terdapat potensi ia akan terkena kejahatan siber. Kelalaian dan kurangnya pengetahuan disini akan dimanfaatkan oleh pelaku, terutama pada kejahatan siber berupa *phishing*.

Phishing (password harvesting fishing) merupakan penipuan yang dilakukan dengan cara mengelabui target sehingga pelaku bisa mendapatkan data sensitif dan bersifat rahasia. Tindakan yang dilakukan *phishers* sebagai pelaku kejahatan *phishing* mengincar informasi sensitif pengguna untuk digunakan secara melawan hukum. Dengan segala alasan yang tidak dapat dibenarkan, *phishers* dengan sengaja (keadaan sadar) memanfaatkan *platform*/aplikasi untuk digunakan sebagai peluang mendapatkan uang tetapi dengan cara yang salah (di luar batas akal pikiran dan sifat manusia) yang mana hal tersebut termasuk dalam delik yang dituangkan dalam UU ITE. Kejahatan teknologi informasi atau *cybercrime* merupakan masalah yang perlu ditanggapi dengan serius karena dampaknya sangat luas. Jika dibiarkan tanpa penanganan hingga tidak terkendali akan dapat sangat mematikan bagi kehidupan masyarakat, terutama bagi pengguna teknologi.

A. Modus Operandi Tindak Pidana *Phishing* yang Terjadi di Surabaya

Modus operandi *phishing* biasanya menggunakan halaman *website* palsu atau surel palsu untuk mengelabui dan mencuri data-data pribadi pengguna. Modus operandi adalah pola dalam melakukan suatu kejahatan, dengan kata lain dapat diartikan sebagai bagaimana suatu kejahatan dapat terlaksana. Dalam penelitian modus operandi ini, penulis akan meninjau melalui putusan Pengadilan Surabaya yang telah berperkara dan memutus perkara *phishing*. Berdasarkan penelusuran 8 (delapan) putusan yang ditemukan modus operandi *phishing*, yaitu:

1. Putusan Nomor: 1193/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1194/Pid.Sus/2021/PN.Sby.

Secara singkat, terdakwa dengan identitas Michael Zeboth Melki Sedek Boas Purnomo diduga telah turut serta melakukan tindak pidana *phishing*. Penguakan adanya aktifitas *cybercrime* terjadi ketika tim Ditreskrimsus Polda Jatim melakukan *cyber patrol* (patroli siber) dengan sasaran grub facebook "SIG" yang merupakan singakatan dari *silent is god* pada bulan februari 2021.

Adanya postingan grub yang mengarah pada indikasi kejahatan siber berupa jual beli akun twilio, *team cyber patrol* kemudian melakukan *profilling* dan ditemukan fakta bahwa anggotanya adalah para pelaku ilegal akses. Diantaranya adalah terdakwa Michael Zeboth Melki Sedek Boas Purnomo (Putusan Nomor : 1193/Pid.Sus/2021/PN.SBY) dan

Shofiansyah Fahrur Rozi (Putusan Nomor: 1194/Pid.Sus/2019/PN.SBY) yang diketahui baik secara bersama-sama, maupun sendiri-sendiri, sebagai orang yang melakukan, yang menyuruh melakukan atau turut melakukan suatu tindak pidana. Perlu di ketahui bahwa akun twilio merupakan akun yang biasanya digunakan *phishers* untuk mengirim *sms spam*/*phishing* di negara bagian amerika.

Penangkapan dilakukan kepada Shofiansyah Fahrur Rozi terlebih dahulu, yaitu pada hari Senin tanggal 09 Maret 2021, bertempat di Hotel Quest Jl. Ronggolawe No.27–28 Wonorejo Kec. Tegalsari Kota Surabaya. Kemudian disusul dengan penangkapan Michael Zeboth pada hari Rabu, 11 Maret 2021 sekira jam 00.30 yang pada saat itu berada di tempat kost terdakwa di Jl. Kutisari Selatan (*three point laundry*) Surabaya. Dalam hal ini merupakan wilayah hukum Pengadilan Negeri Surabaya.

Rangkaian interogasi didapatkan fakta bahwa pada mulanya Michael Zeboth bertemu dengan sdr.Sourav (DPO/WN India) melalui grub facebook "Kolam Tuyul". Dari pertemanan tersebut, sdr.Sourav mengatakan bahwa dirinya bisa mengolah data-data pribadi milik orang lain, sehingga ia memerlukan bantuan terdakwa untuk membuat *spampage*/ *website* palsu dan untuk imbalannya akan diberikan sejumlah uang. Michael Zeboth diperintahkan untuk mengambil atau mencuri data pribadi milik orang lain di negara bagian Amerika berupa uang bantuan pengangguran yang diberikan Pemerintah Amerika. Nantinya data hasil

phishing akan diolah oleh Sdr.Sourav terlebih dahulu sebelum dijual ke komunitasnya.

Michael Zeboth berhasil membuat 14 *spampage* atau *website* palsu yang dibuat dengan teknik *script spampage* dan disebarkan dengan *short message service* (SMS). *Script* adalah suatu bahasa pemrograman yang dibuat untuk membuat suatu tampilan *website*, template bisa menjalankan suatu perintah secara otomatisasi**.** *Script spampage* adalah *script* yang dibuat untuk membuat tampilan suatu *website* yang menyerupai *website* asli/resmi yang dalam hal perkara ini didesain seolah-olah seperti *website* resmi Pemerintah Amerika. Tujuannya adalah agar target yang melihat *spampage* percaya dan menuruti perintah yang ada, sehingga *phishers* dapat mengambil data-data pribadi dari target secara ilegal. Bahwa terdakwa membuat *script spampage* dengan cara :

a. Terdakwa melihat *website* asli yang akan ditiru lewat pencarian *google*, setelah mengetahui *website* aslinya maka dipilih *option inspect*, untuk melihat *source code* atau bahasa pemrograman *website* asli tersebut.
b. Setelah itu terdakwa *copy* semua *source code* dan disimpan lalu diedit dengan menggunakan *software* bernama *php storm* sehingga tampilan *website* palsu mirip dengan *website* yang asli.
c. Selain itu, terdakwa juga memasukkan akun *email* saksi Shofiansyah Fahrur Rozi (akun facebook atas nama ozy localhost) yang akan menerima data data yang akan diisi target. Sehingga apabila target

tertipu maka data pribadi yang dimasukkan ke *spampage/website* palsu buatan terdakwa secara otomatis akan terkirim ke akun saksi Shofiansyah Fahrur Rozi.

d. Cara membedakan *website* asli dengan *website* palsu yang dibuat terdakwa dengan memperhatikan nama domainnya. *Website* asli atau resmi milik pemerintah Amerika Serikat, domainnya adalah ".gov" sedangkan *website* palsu milik terdakwa menggunakan bermacam-macam domain seperti .link, .com, .info dan .net.

e. W*ebsite* yang terdapat kata *ides* kegunaannya untuk memberikan informasi kepada warga mengenai lowongan pekerjaan dan klaim bantuan pra kerja akibat PHK, sedang *website* dengan kode *dmv* atau *bmv* kegunaannya untuk perijinan *driver license* (SIM) online. *Website* yang dibuat terdakwa Michael Zeboth bisa dipastikan palsu karena tidak menggunakan domain .gov, walaupun tampilannya seperti *website* resmi dari pemerintah negara bagian Amerika, contoh http://newyork-dmv.net/ http://onlinenydmv.com/.

f. Setelah *website* berhasil dibuat oleh terdakwa Michael Zeboth, nantinya akan disebarkan oleh Shofiansyah Fahrur Rozi dengan cara:

   1) Terdakwa Shofiansyah mencari nomor hp target yang didapatkan dari *grab phone number* dengan menggunakan *tools software* bernama *python* dan menunggu selama 24 jam sehingga mendapat nomor dalam jumlah banyak. Untuk mencegah

duplikasi nomor hp, terdakwa menggunakan *software* bernama *scriptdedupe.py*.

2) Setelah mendapatkan nomor HP target, terdakwa menyiapkan *tools software sender* bernama *nodejs tools sender* yang digunakan untuk memudahkan pengiriman pesan kepada para target secara bersama-sama.
3) Terdakwa mencantumkan *spampage / website* palsu disertai pesan "*alert from nydmv: we are sorry to inform you due to our regulation compliant update, you must update your contactninformation. For more info visit:ow.ly/3ko2423ko"*, kemudian dikirim kepada target.
4) Jika target tertipu akan mengklik *link url ow.ly/3ko2423ko* yang mana link tersebut terhubung dengan *spampage* atau *website* palsu milik terdakwa Michael Zeboth.
5) Selanjutnya ketika target memasukkan data-data pribadi pada kolom yang ada di *spampage*, data pribadi yang dimasukkan dalam *spampage* secara otomatis akan terkirim ke akun *email* yang dikuasai Terdakwa Shofiansyah.
6) Adapun data-data pribadi yang berhasil didapatkan terdakwa dari kegiatan menyebarkan *spampage / website* palsu kepada target adalah: nama pemilik data SIM, alamat pemilik data SIM, kota pemilik data SIM, kode pos, tanggal lahir, *social security number*, nomor SIM, dan nomor HP.

7) Data-data pribadi milik orang lain yang berhasil didapatkan terdakwa simpan di dalam akun *email result*, diantaranya *result*@dmv-ohio.com dengan url http://162.241.201.10:87 dan *result* "5kusd@newyork-dmv.net" dengan url 167-88-15-102.cprapid.com:2096. Selanjutnya data tersebut oleh Shofiansyah dikirimkan kepada sdr.Sourav (DPO) melalui *chat whatsapp* dan *chat* telegram.

Setelah mengetahui posisi kasus kejahatan *phishing* dalam putusan Putusan Nomor: 1193/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1194/Pid.Sus/2021/PN.Sby**,** identifikasi modus operandinya yaitu:

a) *Phishers* menentukan target

Penentuan target menjadi langkah pertama dikarenakan dalam pembuatan link *phishing* membutuhkan teknik untuk meniru website resmi agar seseorang terkecoh. Dalam hal ini Michael Zeboth dengan perintah dari Sdr. Sourav dengan sepakat menjadikan warga Amerika Serikat yang mendapatkan dana pengangguran oleh pemerintahan untuk menjadi target.

b) Menentukan tujuan *phishing*

Phishers akan menentukan tentang data apakah yang ingin diambil dari target. Dalam hal ini Michael Zeboth atas perintah Sdr.Sourav menentukan bahwa tujuannya adalah untuk mendapatkan data pribadi berupa data kartu kredit. Penentuan tujuan ini diperlukan agar *phishers* mengetahui langkah selanjutnya

yang akan dilakukan, seperti: membuat *email* palsu, desain halaman *website*, atau mempersiapkan *malware*.

c) Membuat *website phishing*

Phishers akan menyiapkan halaman web palsu dengan mendesain halaman web yang serupa dengan *website* aslinya dan memilih nama *domain* yang mirip dengan *domain* aslinya. Bukan hanya itu, *phishers* juga akan meminimalisir kecurigaan dengan menyiapkan konten dan *caption* yang meyakinkan dan tentunya menarik target untuk mengakses web yang dibuat tersebut. Dalam hal ini pesan yang mengecoh adalah adanya perubahan regulasi pada kartu kredit dan hasil pembuatan halaman web serta *domain website* yang sulit dibedakan dengan *website* resminya.

d) Penyebarab *website phishing*

Phishers yang benar-benar mengincar salah satu target akan dengan teliti mencari dan menggali informasi dari target tersebut melalui media internet dan aplikasi pendukung lainnya seperti *Pyton* yang kiranya menunjang informasi terkait target tersebut. Dalam hal ini Shofiansyah Fahrur Rozi dengan keahliannya dalam melakukan *coding* dalam aplikasi *pyton, scriptdedupe.py, dan software sender tools* untuk mendapatkan nomor target. Kemudian *web phishing* dikirimkan melalui *SMS* dengan pesan berupa perubahan regulasi yang harus di konfirmasi oleh semua penerima dana pengangguran yang diberikan oleh pemerintah.

e) Target mengakses *website phishing*

Kerahasiaan data akan dipertaruhkan dalam tahap ini. Bagi seseorang yang memiliki pengetahuan akan kejahatan *phishing*, dan seseorang yang teliti memiliki kesempatan untuk terhindar dari *phishing*. Sebaliknya, seseorang yang lalai dan tidak teliti akan terkecoh untuk mempercayai pesan yang didapatkannya. Pada halaman *website* yang disediakan, target diminta melakukan *update* informasi pribadi hingga data pembayaran pada akun yang digunakan. Ketika seluruh instruksi dilakukan oleh target dan kemudian di *submit*, saat itulah semua informasi target berhasil dimiliki oleh *phishers*.[77] Dalam hal ini *phishers* berasil memainkan perannya.

f) Data korban akan dimanfaatkan

Data yang telah tersubmit tersebut akan otomatis terkirim ke *email phishers* yang nantinya akan dimanfaatkan dengan melawan hukum. Dalam hal ini data kartu kredit dimanfaatkan untuk *carding*.

[77] Suryadi Kurniawan, *Phishing: Pengertian, Cara Kerja dan Langkah Mengatasinya*, terdapat dalam https://www.niagahoster.co.id/blog/mengatasi*phishing*/#Bagaimana_Sebuah_Aksi_*Phishing*_Dijalankan, diakses tanggal 15 Juni 2022, pukul: 22.34.

2. Putusan Nomor: 2205/Pid.Sus/2021/PN.SBY, Putusan Nomor: 2182/Pid.Sus/2021/PN.SBY, Putusan Nomor: 2206/Pid.Sus/2021/PN.SBY

Secara singkat, terdakwa dengan identitas Rico Aprianza diduga telah turut serta melakukan tindak pidana *phishing*. Aktifitas *phishing* terungkap ketika tim *cyber patrol* Ditreskrimsus Polda Jatim melakukan pengembangan penyelidikan setelah Gabriel Fransisco Gerard Tangdiombo ditahan akibat perbuatannya sebagai penyedia jasa rekening bersama (rekber) pada grup facebook *silent is gold* (SIG). Dalam pernyataannya diketahui bahwa terdakwa sebagai pemilik dan pengguna akun facebook atas nama Rico Aprianza adalah orang yang menjual data kartu kredit milik orang lain berupa *email result US* kepada Gabriel Fransisco Gerard Tangdiombo.

Hasil profiling yang dilakukan *team cyber patrol* menemukan fakta lain, yaitu terdakwa dalam melakukan tindakannya di bantu oleh thofan permana yang memiliki peran untuk menjual data hasil *phishing*. Data tersebut dikemas dalam bentuk *email result US, voucher google play card* (GPC) senilai $50 US, dan juga data magento milik orang lain. Dengan adanya fakta dan barang bukti yang ditemukan, pada hari Sabtu tanggal 12 Juni 2021 sekitar jam 10.00, terdakwa di tangkap tengah berada di Hotel Oyo Patraland Urbano, Bekasi, Jawa Barat.

Rangkaian interogasi didapatkan fakta bahwa terdakwa melakukan perbuatannya dengan cara *spamming* atau *phishing* dengan cara mengirim

link palsu kepada seseorang agar orang yang dituju tersebut mengisi *form* yang diberi. Kemudian apabila korban membuka link pada *email* tersebut, maka akan diarahkan untuk memasukkan data *credit card* (CC) yang secara tidak sadar data tersebut masuk ke *email* terdakwa dengan pemberitahuan notifikasi. Dalam hal ini teknik yang digunakan *phishers* adalah *script spampage* dan disebarkan melalui *email*.

Data yang diperoleh kemudian di kemas dalam bentuk *email result* yang di eksekusi oleh terdakwa lain, yaitu Thofan Permana. *Email result* tersebut di dalamnya terdapat *file* berisikan data kartu kredit milik warga negara USA. Dalam perkara ini diketahui bahwa Rico Aprianza menjual data kartu kredit melalui *chat* pada aplikasi *facebook messenger* milik terdakwa lain, yaitu Farnsisco Gerard Tangdiombo yang juga tergabung dalam satu *grub* perkumpulan peretas, yaitu SIG atau "*silent is gold*".

Data kartu kredit yang diperoleh tersebut dapat digunakan untuk melakukan pembelian barang melalui *online shop*. Selain itu, Rico Aprianza juga menggunakan data kartu kredit yang diperolehnya untuk *carding* atau melakukan kegiatan jual beli menggunakan kartu kredit orang lain secara ilegal. Hasil dari pembelian barang/jasa dengan *carding*, terdakwa kemudian menjual kembali berupa *voucher google play card* (GPC) senilai $50 US yang dijual dengan harga Rp. 542.500, dan juga data magento. Dari hasil perbuatannya, para terdakwa mendapat keuntungan sekitar Rp. 100.000.000,- (seratus juta rupiah) yang dipergunakan untuk memenuhi kebutuhan ekonomi keluarga.

Setelah mengetahui posisi kasus kejahatan *phishing* dalam Putusan No: 2205/Pid.Sus/PN.Sby, Putusan No: 2182/Pid.Sus/2021/PN.Sby dan Putusan No: 2206/Pid.Sus/2021/PN.Sby, identifikasi modus operandinya yaitu:

a. *Phishers* menentukan target

Penentuan target menjadi langkah pertama dikarenakan dalam pembuatan link *phishing* membutuhkan teknik untuk meniru website resmi agar seseorang terkecoh. Dalam hal ini Rico Aprianza atas kehendaknya sendiri menjadikan warga sipil Amerika Serikat untuk dijadikan target.

b. Menentukan tujuan *phishing*

Phishers akan menentukan tentang data apakah yang ingin diambil dari target. Dalam hal ini Rico Aprianza menentukan bahwa tujuannya adalah untuk mendapatkan data pribadi berupa data kartu kredit. Penentuan tujuan ini diperlukan agar *phishers* mengetahui langkah selanjutnya yang akan dilakukan, seperti: membuat *email* palsu, desain halaman *website*, atau mempersiapkan *malware*.

c. Membuat *website phishing*

Phishers akan menyiapkan halaman web palsu dengan mendesain halaman web yang serupa dengan *website* aslinya dan memilih nama *domain* yang mirip dengan *domain* aslinya. Bukan hanya itu, *phishers* juga akan meminimalisir kecurigaan dengan menyiapkan konten dan *caption* yang meyakinkan dan tentunya

menarik target untuk mengakses web yang dibuat tersebut. Dalam hal ini pesan yang mengecoh adalah adanya perubahan regulasi pada kartu kredit dan hasil pembuatan halaman web serta *domain website* yang sulit dibedakan dengan *website* resminya.

d. Penyebaran *website phishing*

Rico Aprianza dengan keahliannya mengirimkan *web phishing* dikirimkan secara random melalui *E-mail* dengan pesan berupa perubahan regulasi yang harus di konfirmasi oleh semua pengguna kartu kredit.

e. Target mengakses *website phishing*

Ketika target mehakses *website phishing*, target akan digiring untuk mengikuti instruksi dalam halaman *website* tersebut. Pada halaman *website* yang telah dimanipulasi, target diminta melakukan *update* informasi. Dalam instruksi tersebut memuat laman yang memerintahkan untuk mengisi identitas diri beserta nomor kartu kredit dan kode *exp***.** Ketika seluruh instruksi dilakukan oleh target dan kemudian di *submit*, saat itulah semua informasi target berhasil dimiliki oleh *phishers.* Dalam hal ini *phishers* berasil memainkan perannya.

f. Data korban akan dimanfaatkan

Data yang telah tersubmit tersebut akan otomatis terkirim ke *email phishers* yang nantinya akan dimanfaatkan dengan melawan hukum. Dalam hal ini data kartu kredit dimanfaatkan untuk

berbelanja di *marketplace* dan diolah menjadi *email result* untuk dijual ke komunitas *hacker*.

3. Putusan Nomor: 1855/Pid.Sus/2021/PN.SBY, Putusan Nomor: 1837/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1872/Pid.Sus/2021/PN.SBY.

Secara singkat, terdakwa dengan identitas Rohmat Hidayat diduga telah turut serta melakukan tindak pidana *phishing*. Penguakan adanya aktifitas *cybercrime* terjadi ketika Subdit V Siber Ditreskrimsus Polda Jatim melakukan *cyber patrol* (patroli siber) pada bulan april 2021. Dari tugas tesebut, *team cyber patrol* menemukan sebuah akun facebook dengan *username* "FIRAUN" yang setelah dilakukan *profiling* merupakan akun milik Harry Togu Setiawan (berkas terpisah). Dalam grub tersebut, anggota grub saling bertukar pengalaman menjual data hasil *carding* maupun *spamming*/*phishing*. Harry togu setiawan memiliki peran sebagai pihak yang menjual data hasil *phishing* yang didapatnya dari terdakwa Rohmat Hidayat dan Renno Suryokusumo. Data yang didapat tersebut kemudian di kemas dalam berbagai bentuk, kemudian oleh Harry Togu dipasarkan dengan memposting adanya penjualan data berupa:

a. data *email result* yang berisikan data *credit card* (data kartu kredit) milik orang lain;
b. data akun *marketplace* (venmo, paxful, indodax); dan
c. *voucher* indodax untuk transaksi mata uang digital/kripto.

Senin tanggal 19 April 2021 Harry Togu Setiawan (berkas terpisah) selaku pemilik akun facebook “FIRAUN” berhasil ditangkap oleh petugas kepolisian pada saat berada di terminal 1 domestik keberangkatan Bandara Juanda Surabaya dan berdasarkan hasil pemeriksaan terhadap Harry Togu Setiawan (berkas terpisah) diperoleh petunjuk yang mengarah kepada terdakwa Rohmat Hidayat, sehingga petugas melakukan pengembangan dan berhasil melakukan penangkapan terhadap terdakwa Rohmat Hidayat di rumah Dsn. Sumber Rejo Kec. Winongan Kab. Pasuruan.

Berdasarkan putusan nomor: 1855/Pid.Sus/2021/PN.SBY, Hakim mengabulkan dakwaan subsidair penuntut umum sehingga terdakwa Rohmat Hidayat telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “secara bersama-sama ataupun sendiri-sendiri sebagai orang yang melakukan, yang menyuruh melakukan dan yang turut serta melakukan, dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik” sebagaimana diatur dan diancam pidana dalam Pasal 30 ayat (2) jo. Pasal 46 ayat (2) UU ITE.

Rangkaian pemeriksaan didapatkan fakta bahwa kejahatan ini dilakukan oleh mahasiswa asal Solo yang sama-sama tergabung dalam grub facebook yang beranggotakan para *hacker*. Terdakwa dan saksi Reno Suryokusumo memiliki tugas untuk mencari data kartu kredit atas perintah Harry Togu Setiawan. Dalam menjalankan tugas yang diberikan, terdakwa

melakukan *spamming* atau *phishing* untuk mendapatkan data kartu kredit. Namun dalam hal menjalankan aktifitas *phishing*, saksi Reno Kusumo merupakan yang berperan aktif.

Data kartu kredit (CC) yang biasa terdakwa dapatkan antara lain nomor kartu kredit, masa aktif kartu kredit, CVV kartu kredit, nama dan alamat pemilik kartu kredit, nomor telepon pemilik kartu kredit, tanggal lahir pemilik kartu kredit, SSN (*social security number*) dan *ip address*. Dalam hal ini teknik yang digunakan *phishers* adalah *script spampage* dan disebarkan melalui *email* dengan target nasabah Bank of Amerika (BOA). Kemudian data-data yang berhasil didapatkan tersebut dijual kepada saksi Harry Togu seharga Rp. 200.000, - Rp.300.000, per data. Selain menjual data kartu kredit, saksi Reno Suryokusumo juga memiliki peran untuk membuat akun *marketplace* paxful atas nama orang lain.

Hasil data akun paxful dan data kartu kredit yang diperoleh akan diserahkan kepada Alik Dakirin sebagai eksekutor untuk diolah menjadi *voucher* indodax (*platform* jual beli/*marketplace* aset kripto/mata uang digital ex: bitcoin, dll). Dari hasil penjualan data-data tersebutm Renno beserta kawanannya mendapatkan keuntungan sebesar rp.50.000.000 (lima puluh juta rupiah) per bulannya.

Proses pembuatan/verifikasi akun paxful dan juga pengolahan akun paxful dengan menggunakan data *credit card* (data CC) serta data akun venmo yang dilakukan tersebut dengan cara mengakses sistem elektronik secara tanpa hak dan melawan hukum karena terdakwa tidak memiliki hak

atas data milik orang lain yang saling dikirimkan dan selanjutnya mereka salah gunakan untuk mendapatkan keuntungan pribadi.

Setelah mengetahui posisi kasus kejahatan *phishing* dalam Putusan Nomor: 1855/Pid.Sus/PN.Sby, Putusan Nomor: 1837/Pid.Sus/ 2021/PN.Sby dan Putusan No: 1872/Pid.Sus/2021/PN.Sby, identifikasi modus operandinya yaitu:

a. *Phishers* menentukan target

   Penentuan target menjadi langkah pertama dikarenakan dalam pembuatan link *phishing* membutuhkan teknik untuk meniru website resmi agar seseorang terkecoh. Dalam hal ini Reno Suryokusumo atas anjuran dari Harry Togu Setiawan menjadikan nasabah *Bank of America* (BOA) untuk dijadikan target.

b. Menentukan tujuan *phishing*

   Phishers akan menentukan tentang data apakah yang ingin diambil dari target. Dalam hal ini Reno Suryokusmo menentukan bahwa tujuannya adalah untuk mendapatkan data finansial berupa data kartu kredit. Penentuan tujuan ini diperlukan agar *phishers* mengetahui langkah selanjutnya yang akan dilakukan, seperti: membuat *email* palsu, desain halaman *website*, atau mempersiapkan *malware*.

c. Membuat *website phishing*

   Phishers akan menyiapkan halaman web palsu dengan mendesain halaman web yang serupa dengan *website* aslinya dan

memilih nama *domain* yang mirip dengan *domain* aslinya. Bukan hanya itu, *phishers* juga akan meminimalisir kecurigaan dengan menyiapkan konten dan *caption* yang meyakinkan dan tentunya menarik target untuk mengakses web yang dibuat tersebut. Dalam hal ini pesan yang mengecoh adalah adanya perubahan regulasi pada kartu kredit dan hasil pembuatan halaman web serta *domain website* yang sulit dibedakan dengan *website* resminya.

d. Penyebaran *website phishing*

Reno Suryokusumo dengan keahliannya menyebarkan *web phishing yang* dikirimkan melalui *E-mail* dengan pesan berupa perubahan regulasi yang harus di konfirmasi oleh semua nasabah *Bank of America (BOA).*

e. Target mengakses *website phishing*

Ketika target mehakses *website phishing*, target akan digiring untuk mengikuti instruksi dalam halaman *website* tersebut. Pada halaman *website* yang telah dimanipulasi, target diminta melakukan *update* informasi. Dalam instruksi tersebut memuat laman yang memerintahkan untuk mengisi nomor kartu kredit, masa aktif kartu kredit, cvv kartu kredit, nama dan alamat pemilik kartu kredit, nomor telepon pemilik kartu kredit, tanggal lahir pemilik kartu kredit, SSN (*social security number*) beserta *ip address***.** Ketika seluruh instruksi dilakukan oleh target dan kemudian di *submit*, saat

itulah semua informasi target berhasil dimiliki oleh *phishers*. Dalam hal ini *phishers* berasil memainkan perannya.

f. Data korban akan dimanfaatkan

Data yang telah tersubmit tersebut akan otomatis terkirim ke *email phishers* yang nantinya akan dimanfaatkan dengan melawan hukum. Dalam hal ini data kartu kredit telah dimanfaatkan untuk belanja di *marketplace*, diolah menjadi *email result* untuk dijual ke komunitas *hacker*, dan dikonversikan dalam bentuk mata uang kripto atau mata uang digital.

Dari hasil penelitian, *phishing* dapat dikatakan sebagai *computer crime* karena pelaksanaan hingga penyelesaian kejahatan sebagian besar dilakukan mengunakan media komputer. *Computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih.[78] Disebut dengan *cybercrime* karena kejahatannya berada di *cyber space* yang merupakan karakteristik dari *cybercrime* itu sendiri.

Selain itu *cybercrime*, *phishing* juga masuk ke dalam bentuk kejahatan transnasional.[79] Hal tersebut karena *phishing* telah memenuhi karakteristik sebagai berikut:[80]

---

[78] M.E. Fuady, "Cybercrime: Fenomena Kejahatan melalui Internet di Indonesia", *MediaTor*: *Jurnal Komunikasi*, Edisi No.2, Vol.6, Fakultas Ilmu Ekonomi Universitas Islam Bandung, 2005, hlm.256.

[79] Humphrey Wangke, *Loc.Cit.*

[80] M.E. Fuady, "Cybercrime: Fenomena Kejahatan melalui Internet di Indonesia", *MediaTor*: *Jurnal Komunikasi*, Edisi No.2, Vol.6, Fakultas Ilmu Ekonomi Universitas Islam Bandung, 2005, hlm.258.

1. Perbuatan tersebut dilakukan dengan melawan hukum, dan tanpa hak melalui dunia maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang diberlakukan terhadapnya.
2. Perbuatan dilakukan dengan perangkat komputer yang terhubung dengan internet.
3. Perbuatan tersebut menimbulkan kerugian materil dan nonmaterial yang biasanya lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelaku kejahatan adalah orang yang mengontrol penggunaan internet dan aplikasinya.
5. Kejahatan tersebut seringkali dilakukan dengan melintasi batas negara (transnasional).

Aktivitas *phishers* dalam memindahkan atau mentranfer informasi elektronik dapat dikatakan memiliki proses yang sudah diperinci sebelumnya. Proses tersebut yang dikatakan dengan modus operandi. Pada dasarnya kegiatan *phishing* bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari oleh target itu sendiri. Padahal informasi yang dibagikan tersebut akan digunakan untuk tujuan kejahatan. Dari hasil penelitian, dapat disimpulkan bahwa modus operandi diawali dengan penentuan target dan tujuan *phishing*,

pembuatan *website*, penyebaran *link*, target terkelabui, data dapat diambil alih.

Semua delik di atas mengatasnamakan sebagai pihak instansi kartu kredit (*spoofing*) dengan dalih apabila tidak dilakukan perubahan data maka *user account* akan dihapus sehingga tidak bisa digunakan lagi. Target yang tidak mengetahui modus penipuan ini tentu akan takut jika akun mereka dihapus oleh pihak bank sehingga tanpa pikir panjang langsung memberikan informasi rekening termasuk *username* dan *password-nya*.

Dari segala persiapan yang dilakukan *phishers*, tentu bukanlah hal yang sulit karena keahliannya di bidang teknologi. Siapapun dapat menjadi korban jika *phishers* menerapkan *random* target, sehingga kelalaian seseorang dalam sangat menguntungkan bagi *phishers*. Terdapat sebuah teori yang menyatakan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan (*crime is product of society its self)*.[81] Oleh karena itu, masyarakat memerlukan bekal berupa pengetahuan tentang pengoperasian suatu teknologi agar tidak berpotensi menjadi korban kejahatan siber berupa *phishing* ini.

Saat ini data pribadi menjadi harta yang rentan karena mudah untuk disalahgunakan, salah satunya adalah digunakan untuk pinjaman online yang hanya memerlukan KTP. Tanggungjawab pemilik data pribadi dalam

[81] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Cetakan pertama, PT. Refika Aditama, Bandung, 2010, hlm. 39.

Undang-Undang Perlindungan Data Pribadi juga telah ditegaskan bahwa data pribadi menjadi tanggung jawab pribadi, sehingga dalam hal kelalaian seseorang menjadi konsekuensi pribadi[82]. Sehinnga masyarakat juga harus lebih *aware* dan mawas diri terhadap pentingnya menjaga data pribadi agar terhindar dari hal-hal yang merugikan dirinya sendiri.

B. Pertanggungjawaban Pelaku Tindak Pidana *Phishing* yang Terjadi di Surabaya

Pertanggungjawaban pidana adalah pertanggungjawaban orang terhadap tindak pidana yang dilakukannya. Terjadinya pertangunggjawaban pidana karena telah ada tindak pidana yang dilakukan oleh seseorang. Pertanggungjawaban pidana pada hakikatnya merupakan suatu mekanisme yang dibangun oleh hukum pidana untuk bereaksi terhadap pelanggaran atas "kesepakatan menolak" suatu perbuatan tertentu.[83]

Chairul Huda mengatakan bahwa seseorang tidak dapat dimintai pertanggungjawaban pidana apabila dirinya tidak melakukan perbuatan pidana.[84] Seseorang dapat dikatakan telah melakukan kesalahan dan dapat dimintai dipertanggungjawabkan pidana apabila telah memenuhi unsur pertanggungjawaban pidana, yaitu:

1. Melakukan perbuatan pidana, perbuatan bersifat melawan hukum
2. Kemampuan bertanggungjawab

---

[82] Pasal 27 Peraturan Menteri Nomor 20 Tahun 2006 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

[83] Chairul Huda, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*, Cetakan kedua, Kencana, Jakarta, 2006, hlm.70.

[84] *Ibid*, hlm.19.

3. Melakukan perbuatan tersebut dengan sengaja atau karena kealpaan/kurang hati-hati
4. Tidak adanya alasan pemaaf

Ad.1. Melakukan perbuatan pidana, perbuatan bersifat melawan hukum

Tindak pidana (delik) adalah perbuatan seseorang yang telah memenuhi unsur-unsur suatu delik yang diatur dalam hukum pidana. Jika suatu perbuatan dilarang oleh undang-undang dan perbuatan yang dilakukan sesuai dengan hal yang dilarang, maka perbuatan itu bersifat melawan hukum. Unsur kesalahan dalam tindak pidana dianggap ada apabila dengan sengaja atau karena kelalaian telah melakukan perbuatan yang menimbulkan keadaan atau akibat yang dilarang oleh hukum pidana dan dilakukan dengan mempu bertanggung jawab.

Ad.2. Kemampuan bertanggungjawab

Menurut KUHP seseorang tidak dapat dimintai dipertanggungjawabkan atas perbuatan pidana yang dilakukannya sehubungan dengan:

a. Karena kurang sempurna akal atau karena sakit berupa akal (Pasal 44 KUHP);[85]
b. Karena belum dewasa (Pasal 45 KUHP).[86]

Mampu bertanggungjawab dalam hal ini adalah mampu menginsyafi sifat melawan hukumnya dan sesuai dengan keinsyafan itu mampu untuk

[85] Pasal 44 Kitab Undang-Undang Hukum Pidana.
[86] Pasal 45 Kitab Undang-Undang Hukum Pidana.

menentukan kehendaknya. Dalam hal kasus *phishing* yang terjadi maka kemampuan bertanggungjawab tersebut timbul disebabkan:

1) Seseorang melakukan pengelabuan atau menyesatkan masyarakat untuk mengikuti instruksi dalam bentuk apapun yang tujuannya adalah mendapatkan data pribadi, data akun finansial.
2) Seseorang memakai dan menggunakan data akun finansial orang lain dan dimanfaatkan secara ilegal.
3) Memperdagangkan data pribadi seseorang yang dikemas dalam bentuk email result tanpa sepengetahuan pemilik data pribadi tersebut.

Ad.3. Melakukan perbuatan tersebut dengan sengaja atau karena kealpaan/kurang hati-hati

Dalam hukum pidana, kesengajaan dan kealpaan itu dikenal sebagai bentuk dari kesalahan. Pelaku telah dianggap bersalah jika ia melakukan perbuatan pidana yang sifatnya melawan hukum itu dengan sengaja atau karena kealpaannya, yang dalam kejahatan *phishing* diatur dalam UU ITE pada Pasal 31 dam Pasal 45a.

Ad. 4. Tidak adanya alasan pemaaf

Tidak adanya alasan pemaaf berarti tidak adanya alasan yang menghapus kesalahan dari terdakwa. Alasan pemaaf ini menyangkut pertanggungjawaban seseorang terhadap perbuatan pidana yang telah dilakukannya atau *criminal responsibility*. Alasan ini menghapuskan kesalahan orang yang melakukan delik atas dasar beberapa hal, yaitu:[87]

[87] Kitab Undang-Undang Hukum Pidana.

a. Ketidakmampuan bertanggungjawab – Pasal 44 KUHP;
b. Pembelaan terpaksa yang melampaui batas – Pasal 49 ayat (2) KUHP;
c. Daya paksa (overmacht) – Pasal 48 KUHP; dan
d. Menjalankan perintah jabatan tanpa wewenang – Pasal 51 ayat (2) KUHP.

Pertanggungjawaban pidana sering kali memiliki kaitan dengan delik penyertaan. Berdasarkan ketentuan Pasal 55 dan 56 KUHP dapat ditarik kesimpulan bahwa penyertaan adalah apabila orang yang tersangkut untuk terjadinya suatu perbuatan pidana atau kejahatan itu tidak hanya satu orang saja, melainkan melibatkan lebih dari satu orang. Selain itu dalam ajaran penyertaan yang didasarkan pada Pasal 55 KUHP menyebutkan beberapa golongan yang dapat dipidana, yaitu:[88]

1. Pembuat (*daader*)

   Daader berasal dari kata daad yang di dalam bahasa belanda memiliki arti sebagai tindakan. Orang melakukan suatu daad disebut dengan *daader*, atau lazimnya dikenal dengan sebutan pelaku.

   a. Pelaku (*pleger*)

   Pleger adalah mereka yang memenuhi seluruh unsur yang ada dalam suatu perumusan karakteristik delik pidana dalam setiap pasal.[89] *Pleger* adalah orang yang secara materiil dan *persoonlijk* nyata-nyata melakukan perbuatan yang secara sempurna memenuhi semua unsur

[88] Pasal 55 Kitab Undang-Undang Hukum Pidana.
[89] A.F. Lamintang & Fraciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana di Indonesia*, Cetakan keenam, Sinar Grafika, Jakarta, 2014, hlm. 611.

dari rumusan delik yang terjadi.[90] Oleh karena itu, pada dasarnya Ia adalah orang yang baik secara sendiri maupun terkait dengan orang lain, telah dapat dijatuhi sanksi pidana.

b. Yang menyuruh melakukan (*doenpleger*)

Doenpleger adalah orang yang menyuruh orang lain untuk melakukan suatu perbuatan pidana, dimana secara yuridis orang yang disuruh dan akhirnya secara nyata melakukan perbuatan pidana tersebut harus merupakan orang yang tidak dapat dipertanggungjawabkan secara pidana.[91]

c. Turut serta melakukan (*medepleger*)

Medepleger adalah orang yang melakukan kesepakatan dengan orang lain untuk melakukan suatu perbuatan pidana dan secara bersama-sama pula iaturut beraksi dalam pelaksanaan perbuatan pidana sesuai dengan yang telah disepakati.[92]

d. Penganjur (*uitlokker*)

Setiap orang yang menggerakkan atau membujuk orang lain (*pleger*) untuk melakukan suatu tindak pidana dengan menggunakan sarana-sarana yang telah ditentukan undang-undang secara limitatif, yaitu dengan memberikan atau menjanjikan sesuatu, menyalahgunakan kekuasaan atau martabat, kekerasan, ancaman, atau

---

[90] Chant S. R. Ponglabba, "Tinjauan Yuridis Penyertaan Dalam Tindak Pidana Menurut KUHP", Jurnal Hukum, Edisi No. 6, Vol. 6, Fakultas Hukum Universitas Sam Ratulangi, 2017, hlm. 34.

[91] *Ibid.*

[92] *Ibid.*

penyesatan dengan memberi sarana atau keterangan.[93] *Uitlokker* tidak mewujudkan tindak pidana secara materiil atau langsung tetapi melalui orang lain (*pleger*). Dalam hal ini pembuat mateiil dapat dimintai pertanggungjawaban.

Apabila keempat unsur di atas terpenuhi, maka pelaku kejahatan tersebut dinilai telah merugikan orang lain melalui perbuatan yang melanggar norma hukum yang berlaku dan harus mempertanggungjawabkan perbuatannya. Pertanggungjawaban pidana juga disesuaikan dengan penyertaannya dalam suatu tindak kejahatan. Teori pertanggungjawaban pidana apabila dikaitkan dengan kasus yang terjadi di Surabaya, pertanggungjawaban pidana kepada pihak yang terjaring dalam kegiatan ilegal akses berupa *phishing* adalah:

1. **Putusan Nomor: 1193/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1194/Pid.Sus/2021/PN.Sby.**

   Berdasarkan fakta-fakta dalam persidangan, terdakwa Michael Zeboth telah terbukti bersalah dengan melakukan perbuatan pidana *cybercrime* berupa *phishing* atau pengelabuan untuk mendapatkan data pribadi orang lain. Dalam putusan, terdapat unsur penyertaan yang dicerminkan dalam putusan yang di junctokan dengan Pasal 55 KUHP. Dalam hal melakukan perbuatannya, terdakwa dibantu dengan Shofiansyah Fahrur Rozi yang merupakan terdakwa dalam putusan nomor: 1194/Pid.Sus/2021/PN.SBY dengan peran dan persangkaan masing masing sebagai berikut:

[93] Pasal 55 ayat (1) angka 2e Kitab Undang-Undang Hukum Pidana.

a. Terdakwa Michael Zeboth Melki Sedek Boas Purnomo telah melakukan perbuatan pidana berupa *phishing* dengan cara membuat website *phishing.* Secara formil dan materiill Michael Zeboth merupakan orang yang pertama kali merencanakan, melakukan, dan menyelesaikan yang dari awal Ia mengetahui bahwa perbuatannya menimbulkan akibat yang di larang undang-undang. Dalam hal ini Terdakwa di kategorikan sebagai *pleger* karena telah memenuhi semua unsur delik, termasuk juga bila melalui orang lain atau bawahannya.
b. Terdakwa Shofiansyah Fahrur Rozi turut melakukan perbuatan pidana *phishing* dengan cara menyebarkan *link website phishing* yang telah dibuat oleh terdakwa lain, sebagai pengepul data, dan penyedia jasa rekber untuk menjual data orang lain. Dalam hal ini Terdakwa di kategorikan sebagai *medepleger* atau seseorang yang turut serta karena sebelumnya secara sadar Ia telah melakukan kesepakatan dengan orang lain (Michael Zeboth dan Sourav) untuk melakukan suatu perbuatan pidana dan secara bersama-sama Ia turut bersaksi dalam pelaksanaan perbuatan pidana sesuai dengan yang telah disepakati.
c. Tersangka Sourav (DPO/WN India) menganjurkan Michael Zeboth untuk membuat web *phishing* , dan juga menganjurkan Shofiansyah Fahrur Rozi untuk menyebarkan link *phishing* yang sudah ada. Para terdakwa dijanjikan dengan sebuah imbalan sebesar US 1$ untuk

setiap data akun yang diperoleh. Dalam hal ini para terdakwa berhasil memperoleh sebanyak 30.000 data pribadi, sehingga mendapatkan imbalan sebesar US $30.000 atau Rp. 420.000.000. Dalam hal ini penyertaanya dikategorikan sebagai *uitlokker* karena telah menganjurkan orang lain untuk melakukan sesuatu dengan sarana yang telah ditentukan undang-undang yaitu dijanjikan sesuatu berupa imbalan.

Berdasarkan hasil penyidikan dan penyelidikan, menurut perannya masing-masing bahwa terdakwa Michael Zeboth Melki dan Shofiansyah Fahrur Rozi (1194/Pid.Sus/2021/PN.SBY) oleh penuntut umum didakwa dengan dakwaan subsideritas. Keduanya didakwa dengan dakwaan primair yaitu Pasal 35 jo. Pasal 51 ayat (1) UU ITE jo. pasal 55 ayat (1) KUHP, dan dakwaan subsidair yaitu Pasal 32 atar (2) jo. Pasal 48 ayat (2) UU ITE jo. Pasal 55 ayat (1) KUHP.

Berdasarkan fakta dalam persidangan dan berdasarkan berita acara pemeriksaan yang menyatakan bahwa keduanya dalam persidangan masing-masing menyampaikan keterangannya dipengadilan maupun saat melakukan tindak pidana sebagaimana didakwakan oleh jaksa penuntut umum, para terdakwa melakukannya dalam keadaan sehat jasmani maupun rohani dan sadar akan dampak dari tindakannya, dimana berdasarkan asas *presumption iures de iure* bahwa semua orang dianggap tahu tentang hukum sehingga semua orang yang melakukan perbuatan

hukum harus sadar akan tindakannya, serta menginsyafi hakekat dari tindakannya tersebut.

Dilihat dari segi umurnya terdakwa Michael Zeboth dan Sofiansyah Fahrur Rozi tidak termasuk dalam kategori anak-anak, sesuai dengan Pasal 45 KUHP. Dengan fakta bahwa terdakwa Michael Zeboth yang telah berumur 20 Tahun dan terdakwa Shofiansyah telah berumur 25 Tahun, para terdakwa bukanlah lagi termasuk dalam golongan anak-anak dan sepatasnya mampu bertanggung jawab apabila dilihat dari segi umurnya. Sehingga berdasarkan hal tersebut Para Terdakwa tidak memiliki alasan pemaaf untuk menghapuskan kesalahan yang telah terdakwa lakukan.

Bawasannya terdakwa telah mempunyai bentuk kesalahan berupa kegiatan ilegal akses dan para terdakwa mengetahui bahwa perbuatan ilegal akses yang dilakukannya merupakan perbuaan pidana. Para terdakwa mengaku mengenal satu sama lain dan bekerja sama untuk menjalankan tugas yang diberikan Sdr. Sourav dan berinteraksi melalui WhatsApp. Kegiatan ilegal akses yang dilakukan adalah berupa pengelabuan dengan membuat website palsu agar diakses oleh target, yaitu warga negara amerika yang mendapatkan dana pengangguran.

Berdasarkan hasil pemeriksaan dan persidangan, menurut perannya masing-masing bahwa terdakwa Michael Zeboth Melki dan Shofiansyah Fahrur Rozi (1194/Pid.Sus/2021/PN.SBY) oleh hakim dinyatakan telah terbukti bersalah dengan melakukan perbuatan pidana yakni “bersama-

sama dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik" sebagaimana diatur dan diancam pidana dalam Pasal 35 jo. Pasal 51 ayat (1) UU ITE jo. pasal 55 ayat (1) KUHP.

Berkenaan dengan unsur kesalahan yakni harus melakukan perbuatan pidana, berdasarkan fakta – fakta dipersidangan terdakwa Michael Zeboth dan terdakwa Shofianyah Fahrur Rozi (1194/Pid.Sus/2021/PN.SBY) telah terbukti melakukan perbuatan pidana dimana telah terpenuhinya unsur–unsur dalam Pasal 35 jo. Pasal 51 ayat (1) UU ITE jo. pasal 55 ayat (1) KUHP, yakni:

1) *Unsur dengan sengaja dan tanpa hak atau melawan hukum*

   Terdakwa melakukan perbuatan ilegal tersebut dalam kondisi sadar.

2) *Unsur melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan informasi elektronik dan/atau Dokumen elektronik tersebut dianggap seolah-olah data yang otentik*

   Terdakwa melakukan perbuatan ilegal akses dalam kondisi sadar dan dengan niat melakukan pembuatan website tiruan dari website pemerintah untuk mendapatkan informasi orang lain. Terdakwa menerangkan dan memastikan bila website website

tersebut diatas bukan website asli atau resmi milik pemerintahan Negara bagian Amerika atau bisa dikatakan website palsu atau scampage. Perbedaan antara website palsu atau scampage dengan website asli atau resmi milik pemerintahan Negara bagian Amerika adalah pada bagian domain link URL, adapun website resmi/asli milik pemerintahan Negara bagian Amerika mengunakan domain .gov (goverment) sedangkan pada website palsu atau scampage tersebut diatas menggunakan bermacam macam domain seperti, .link, .com, .info dan .net.

3) *Unsur dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak*"

Terdakwa melakukan pemindahan secara ilegal dan tanpa hak milik orang lain kepada orang lain yang juga tidak berhak atas informasi tersebut.

Sesuai dengan penelitian yang telah diuraikan, maka unsur pertanggungjawaban pidana pada orang yang dengan sengaja melakukan tindak pidana berupa *phishing* berdasarkan (Putusan Nomor : 1193/Pid.Sus/2021/PN.SBY telah terbukti secara sah dan meyakinkan, dan Michael Zeboth Melki Sedek Boas Purnomo dapat dimintai pertanggungjawaban pidana sebagaimana perbuatan terdakwa diatur dalam Pasal 35 jo. Pasal 51 ayat (1) UU ITE jo. pasal 55 ayat (1) ke KUHP. Majelis Hakim dalam Putusan Nomor: 1194/Pid.Sus/2019/PN.SBY

menjatuhkan pidana kepada terdakwa SHOFIANSYAH FAHRUR ROZI dengan mengabulkan dakwaan subsidair penuntut umum, yang mana terdakwa terbukti secara sah dan meyakinkan melanggar Pasal 35 jo. Pasal 51 ayat (1) UU ITE jo. pasal 55 ayat (1) ke KUHP.

Dalam putusannya, terdakwa dijatuhi hukuman pidana penjara selama 2 (dua) tahun ; dan pidana denda sebesar Rp.5.000.000,- (lima juta rupiah) subsidair 1 (satu) bulan kurungan sebagaimana perbuatannya yang telah melanggar pasal 35 ayat (1) Jo. pasal 51 ayat (1) UU R.I No.19 Tahun 2016 tentang Perubahan atas Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) jo. pasal 55 ayat (1) ke 1 KUHP.

2. **Putusan Nomor: 2205/Pid.Sus/2021/PN.SBY, Putusan Nomor: 2182/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 2206/ Pid.Sus/2021/PN.SBY**

Berdasarkan fakta-fakta dalam persidangan, terdakwa Rico Aprianza Bin Totok Markistian telah terbukti bersalah dengan melakukan perbuatan pidana *cybercrime* berupa *phishing* atau pengelabuan untuk mendapatkan data pribadi orang lain. Dalam putusan, terdapat unsur penyertaan yang dicerminkan dalam putusan yang di junctokan dengan Pasal 55 KUHP. Dalam hal melakukan perbuatannya, terdakwa dibantu dengan Gabriel Fransisco yang merupakan terdakwa dalam putusan nomor 2182/Pid.Sus/2021/PN.SBY, dan Thofan Permana yang merupakan

terdakwa dalam putusan nomor 2206/Pid.Sus/2021/PN.SBY dengan peran dan persangkaan masing masing sebagai berikut:

a. Terdakwa Rico Aprianza telah melakukan perbuatan pidana berupa *phishing* dengan cara membuat website *phishing*. Perbuatannya dimulai dari niat mencuri data orang lain, yang direalisasikan dengan membuat link *phishing*, kemudian menyebarkannya secara mandiri. Dalam hal ini perbuatannya telah mencerminkan tindakan *pleger* sebagai seseorang yang melakukan perbuatannya sendiri, yang mana perbuatan tersebut memenuhi unsur delik.
b. Terdakwa Thofan Permana turut melakukan perbuatan pidana *phishing* dan perannya dikategorikan sebagai *medepleger* atau seseorang yang turut serta melakukan perbuatan pidana, karena Thofan Permana telah bersepakat dengan terdakwa lain (Rico Aprianza) untuk secara bersama-sama melakukan tindak pidana. Kesepakatan dilakukannya secara sadar dan mengetahui bahwa perbuatannya merupakan hal yang dilarang oleh undang-undang. Terdakwa memiliki peran sebagai penampung data *phishing* kemudian mengememasnya menjadi *email result*, dan menjual atau menyetorkan *email result* tersebut kepada Gabriel Fransisco.
c. Terdakwa Gabriel Fransisco Gerard Tangdiombo turut melakukan perbuatan *phishing*. Dirinya memiliki peran sebagai penyedia jasa rekber pada *grub* facebook SIG, untuk menjual *email result* yang berisi data kartu kredit warga Amerika yang Ia dapatkan dari Rico

Aprianza dan Thofan Permana. Dalam hal ini Terdakwa dikategorikan sebagai *medepleger* karena sebelumnya telah membuat kesepakatan untuk menjual *email result* yang didapatkan dari terdakwa lain (Rico Aprianza & Thofan Permana) sebagai bentuk tindak lanjut dari kegiatan *phishing* yang dilakukan.

Berdasarkan hasil penyidikan dan penyelidikan, menurut perannya masing-masing bahwa terdakwa Rico Aprianza, Thofan Permana, dan Gabriel Fransisco oleh penuntut umum didakwa dengan dakwaan alternatif. Para terdakwa diancam pidana dengan dakwaan pertama Pasal 48 ayat (2) jo Pasal 32 ayat (2) UU ITE jo Pasal 55 ayat (1) ke-1 KUHP, dan/atau dakwaan kedua Pasal 46 ayat (2) jo Pasal 30 ayat (2) UU ITE Jo. Pasal 55 ayat (1) ke-1 KUHP.

Berdasarkan fakta dalam persidangan dan berdasarkan berita acara pemeriksaan yang menyatakan bahwa para terdakwa dalam persidangan masing-masing menyampaikan keterangannya dipengadilan maupun saat melakukan tindak pidana sebagaimana didakwakan oleh jaksa penuntut umum, para terdakwa melakukannya dalam keadaan sehat jasmani maupun rohani dan sadar akan dampak dari tindakannya, dimana berdasarkan asas *presumption iures de iure* bahwa semua orang dianggap tahu tentang hukum sehingga semua orang yang melakukan perbuatan hukum harus sadar akan tindakannya, serta menginsyafi hakekat dari tindakannya tersebut.

Dilihat dari segi umurnya Para terdakwa tidak termasuk dalam kategori anak-anak, sesuai dengan Pasal 45 KUHP. Dengan fakta bahwa terdakwa Rico Aprianza yang telah berumur 21 Tahun, terdakwa Thofan Permana 21 Tahun dan terdakwa Gabriel Fransisco telah berumur 23 Tahun, para terdakwa bukanlah lagi termasuk dalam golongan anak-anak dan sepatasnya mampu bertanggung jawab apabila dilihat dari segi umurnya. Sehingga berdasarkan hal tersebut Para Terdakwa tidak memiliki alasan pemaaf untuk menghapuskan kesalahan yang telah terdakwa lakukan.

Bawasannya terdakwa telah mempunyai bentuk kesalahan berupa kegiatan ilegal akses dan para terdakwa mengetahui bahwa perbuatan ilegal akses yang dilakukannya merupakan perbuaan pidana. Para terdakwa mengaku mengenal satu sama lain dan sama-sama tergabung dalam *grub* facebook SIG. Kegiatan ilegal akses yang dilakukan adalah berupa pengelabuan dengan membuat website palsu agar diakses oleh target yang merupakan warga negara amerika, memperjualbelikan data pribadi orang lain, serta carding.

Berdasarkan hasil pemeriksaan dan persidangan, menurut perannya masing-masing bahwa para terdakwa oleh Hakim dinyatakan telah terbukti bersalah dengan melakukan perbuatan pidana yakni secara sah dan meyakinkan bersalah melakukan tindak pidana setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan transmisi, memindahkan atau mentransfer suatu informasi elektronik dan/atau dokumen elektronik milik orang lain dan melanggar Pasal 48 ayat (2)

Undang-Undang RI No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang ITE jo. Pasal 32 ayat (2) Undang-Undang RI Nomor 11 tahun 2008 tentang ITE jo Pasal 55 ayat (1) ke-1 KUHP.

Berkenaan dengan unsur kesalahan yakni harus melakukan perbuatan pidana, berdasarkan fakta – fakta dipersidangan terdakwa Michael Zeboth dan terdakwa Shofianyah Fahrur Rozi (1194/Pid.Sus/2021/PN.SBY) telah terbukti melakukan perbuatan pidana dimana telah terpenuhinya unsur–unsur dalam Pasal 35 jo. Pasal 51 ayat (1) UU ITE jo. pasal 55 ayat (1) KUHP, yakni:

1) *Unsur setiap orang*

   Menunjuk kepada orang perorangan sebagai subyek hukum (*natuurlijke persoon*) yang mampu bertanggung jawab secara hukum, yang dihadapkan ke muka persidangan karena didakwa melakukan tindak pidana. Orang yang dihadapkan tersebut yaitu Terdakwa adalah orang yang cakap dan mampu bertanggung jawab menurut hukum dan dalam perkara ini tidak terdapat atau tidak terjadi tentang kesalahan tentang orang (*error in persona*), maka berdasarkan uraian fakta dan pertimbangan tersebut diatas Majelis berpendapat bahwa unsur setiap orang dalam hal ini telah terpenuhi dan terbukti menurut hukum.

2) *Unsur dengan sengaja dan tanpa hak atau melawan hukum*

Terdakwa melakukan perbuatan ilegal tersebut. secara sadar dan tanpa paksaan dalam menjalankan kegiatannya yang bertentangan dengan peraturan yang berlaku. artinya seseorang yang melakukan suatu tindakan dengan sengaja harus menghendaki serta menginsyafi tindakan tersebut dan/atau akibatnya. Sengaja berarti menghendaki dan mengetahui apa yang dilakukan, orang yang melakukan perbuatan dengan sengaja menghendaki perbuatan itu dan disamping itu mengetahui atau menyadari tentang apa yang dilakukan itu serta akibat yang akan timbul dari perbuatan tersebut

3) *Unsur melakukan transmisi, memindahkan atau mentransfer suatu informasi elektronik dan/atau dokumen elektronik milik orang lain*

Bahwa unsur perbuatan yang disebutkan diatas yaitu perbuatan yang dilarang berupa menyebarluaskan atau bahkan diperdagangkan tanpa seizin pemilik data pribadi dan yang tidak berhak atau ditentukan lain oleh Peraturan Perundang-undangan adalah bersifat alternatif dimana salah satu dari tindak pidana tersebut terbukti dilakukan oleh terdakwa maka unsur ini dapat dinyatakan telah terpenuhi dan terbukti menurut hukum dalam perbuatan terdakwa;

Sesuai dengan penelitian yang telah diuraikan, maka unsur pertanggungjawaban pidana pada orang yang dengan sengaja melakukan tindak pidana berupa *phishing* berdasarkan Putusan Nomor:

2205/Pid.Sus/2021/PN.SBY telah terbukti secara sah dan meyakinkan, dan Rico Aprianza dapat dimintai pertanggungjawaban pidana sebagaimana perbuatan terdakwa diatur dalam Pasal 48 ayat (2) jo Pasal 32 ayat (2) UU ITE jo Pasal 55 ayat (1) ke-1 KUHP. Dalam putusannya, Hakim menjatuhkan pidana kepada terdakwa oleh karena itu dengan pidana penjara selama 1 tahun 4 bulan dan denda sebesar Rp.5.000.000,- (lima juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 1 bulan.

Gabriel Fransisco yang merupakan terdakwa dalam putusan nomor 2182/Pid.Sus/2021/PN.SBY, dan Thofan Permana yang merupakan terdakwa dalam putusan nomor 2206/Pid.Sus/2021/PN.SBY menjatuhkan pidana kepada terdakwa kepada masing-masing terdakwa dengan mengabulkan dakwaan alternative pertama, yang mana terdakwa terbukti secara sah dan meyakinkan melanggar Pasal 48 ayat (2) jo Pasal 32 ayat (2) UU ITE jo Pasal 55 ayat (1) ke-1 KUHP.

Dalam putusannya, Hakim menjatuhkan pidana kepada Terdakwa oleh karena itu dengan pidana penjara selama 10 (sepuluh) bulan dan denda sejumlah Rp2.500.000,- (dua juta lima ratus ribu rupiah) dengan ketentuan apabila denda tersebut tidak dibayar diganti dengan pidana kurungan selama 1 (satu) bulan sebagaimana perbuatannya yang telah melanggar Pasal 48 ayat (2) Undang-Undang RI No. 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 tahun 2008 tentang ITE jo.

Pasal 32 ayat (2) Undang-Undang RI Nomor 11 tahun 2008 tentang ITE jo Pasal 55 ayat (1) ke-1 KUHP.

3. Putusan Nomor: 1855/Pid.Sus/2021/PN.SBY, , Putusan Nomor: 1837/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1872/ Pid.Sus/2021/PN.SBY.

Berdasarkan fakta-fakta dalam persidangan, terdakwa Rohmat Hidayat telah terbukti bersalah dengan melakukan perbuatan pidana *cybercrime* berupa *phishing* atau pengelabuan untuk mendapatkan data pribadi orang lain. Dalam putusan, terdapat unsur penyertaan yang dicerminkan dalam putusan yang di junctokan dengan Pasal 55 KUHP. Dalam hal melakukan perbuatannya, terdakwa dibantu dengan Harry Togu Setiawan yang merupakan terdakwa dalam putusan nomor 1837/Pid.Sus/2021/PN.SBY, Alik Dakirin yang merupakan terdakwa dalam putusan nomor: 1872/Pid.Sus/2021/PN.SBY, dan Reno Suryokusumo dengan peran dan persangkaan masing masing sebagai berikut:

a. Reno Suryokusumo memiliki peran untuk mencari data akun pribadi orang lain melalui *phishing*. Reno bertugas mencari data dari bank di Amerika. Reno berkedudukan sebagai seseorang yang melakukan dan menyelesaikan kegiatan *phishing* yang diawali dengan pembuatan link *phishing* hingga berakhirnya delik berupa data pribadi orang lain telah didapatkan. Meskipun berbuatanya atas anjuran orang lain, namun menjadi tidak berlaku karena dirinya tidak memenuhi pasal 44

dan 48 KUHP. Dalam hal ini, Ia telah memenuhi seluruh unsur delik dan penyertaannya dikategorikan sebagai pleger.

b. Terdakwa Rohmat Hidayat telah melakukan perbuatan pidana berupa penyedia jasa rekber dan sebagai pencari data akun kartu kredit tetapi tidak dengan *phishing* yang dilakukannya sendiri, melainkan membeli dari orang lain. Dalam hal ini terdakwa dikategorikan sebagai *medepleger* karena telah membantu kegiatan jual beli data pribadi secara ilegal dengan membelinya dari orang lain. Sehingga dalam hal ini, penyertaannya dikategorikan sebagai *medepleger* atau turut serta melakukan tindak pidana. Sebelumnya, terdakwa dengan sadar melakukan kesepakatan dengan teman 1 (satu) grup facebook untuk bekerjasama melakukan serangkaian kegiatan pencurian data meskipun mengetahui bahwa kegiatannya melanggar undang-undang.
c. Terdakwa Harry Togu Setiawan menganjurkan orang lain untuk melakukan perbuatan pidana *phishing.* Togu meminta anggota grup Facebook (Reno, Rohmat Hidayat, Alik Dakirin) untuk mencari data kartu kredit. Anjuran tersebut disertai dengan pemberian imbalan per/ 1 (satu) data kartu kredit. Data itu kemudian diolah untuk dijadikan kripto. Setelah Togu mendapatkan data kartu kredit, dia menyerahkannya ke Alik untuk diproses menjadi mata uang kripto. Dalam hal ini penyertaannya dikategorikan sebagai *uitlokker* karena dirinya menganjurkan orang lain untuk melakukan tindak pidana dengan kesepakatan. Terdakwa memberikan imbalan berupa

pembagian hasil penjualan data pribadi orang lain yang telah dikemas menjadi *email result.*

d. Terdakwa Alik Dakirin turut melakukan perbuatan *phishing*. Dirinya memiliki peran sebagai pengolah data. Alik berperan mengolah data kartu kredit untuk dijadikan kripto seperti bitcoin dan sebagainya. Dalam hal ini terdakwa dalam peryertaannya dikategorikan sebagai *medeplege*r atau turut serta melakukan. Ia secara sadar telah menyepakati dan melakukan kerjasama melakukan pencurian data yang di lakukan secara bersama-sama hingga berakhir dengan terselesainya delik berupa pembagian hasil.

Berdasarkan hasil penyidikan dan penyelidikan, menurut perannya masing-masing bahwa terdakwa Rohmat Hidayat, Harry Togu Setiawan, Alik dakirin, dan Reno Suryokusumo oleh penuntut umum didakwa dengan dakwaan alternatif. Para terdakwa didakwa dengan:

1) Rohmat Hidayat
    a) alternatif pertama : Pasal 30 ayat (2) Jo Pasal 46 ayat (2) UU ITE jo Pasal 55 ayat (1) ke-1 KUHP, dan/atau;
    b) Alternatif kedua : Pasal 46 ayat (2) jo Pasal 30 ayat (2) UU ITE Jo. Pasal 55 ayat (1) ke-1 KUHP.
2) Harry Togu Setiawan
    a) alternatif pertama : Pasal 30 ayat (2) Jo Pasal 46 ayat (2) UU ITE jo Pasal 55 ayat (1) ke-1 KUHP, dan

b) alternatif kedua : Pasal 32 ayat 2 jo. Pasal 48 ayat 1 UU ITE jo. Pasal 55 ayat 1 ke-1 KUHP

3) Alik Dakirin dan Reno Suryokusumo

a) alternatif pertama : Pasal 30 ayat (2) Jo Pasal 46 ayat (2) UU ITE jo Pasal 55 ayat (1) ke-1 KUHP, dan

b) alternatif kedua : Pasal 32 ayat 2 jo. Pasal 48 ayat 2 UU ITE jo. Pasal 55 ayat 1 ke-1 KUHP

Berdasarkan fakta dalam persidangan dan berdasarkan berita acara pemeriksaan yang menyatakan bahwa para terdakwa dalam persidangan masing-masing menyampaikan keterangannya dipengadilan maupun saat melakukan tindak pidana sebagaimana didakwakan oleh jaksa penuntut umum, para terdakwa melakukannya dalam keadaan sehat jasmani maupun rohani dan sadar akan dampak dari tindakannya, dimana berdasarkan asas *presumption iures de iure* bahwa semua orang dianggap tahu tentang hukum sehingga semua orang yang melakukan perbuatan hukum harus sadar akan tindakannya, serta menginsyafi hakekat dari tindakannya tersebut.

Dilihat dari segi umurnya Para terdakwa tidak termasuk dalam kategori anak-anak, sesuai dengan Pasal 45 KUHP. Dengan fakta bahwa terdakwa Rohmat Hidayat berumur 37 Tahun, Harry Togu Setiawan 23 Tahun, Alik dakirin berusia 21 Tahun, dan Reno Suryokusumo berumur 21 Tahun, para terdakwa bukanlah lagi termasuk dalam golongan anak-anak dan sepatasnya mampu bertanggung jawab apabila dilihat dari segi umurnya.

Sehingga berdasarkan hal tersebut Para Terdakwa tidak memiliki alasan pemaaf untuk menghapuskan kesalahan yang telah terdakwa lakukan.

Bawasannya terdakwa telah mempunyai bentuk kesalahan berupa kegiatan ilegal akses dan para terdakwa mengetahui bahwa perbuatan ilegal akses yang dilakukannya merupakan perbuaan pidana. Para terdakwa mengaku mengenal satu sama lain dan sama-sama tergabung dalam grup facebook SIG. Perbuatan para terdakwa dimulai dengan adanya pertunjuk dari terdakwa Harry Togu Setiawan. Karena tidak semua dapat melakukan *phishing*, Rohmat Hidayat dan kawan-kawannya membagi tugas berdasarkan keahlian masing-masing. Setiap data pribadi yang didapatkan oleh Rohmat Hidayat dan Reno Suryo Kusumo hasil dari *phishing* dengan target utama nasabah Bank USA dan akun Paxful akan di serahkan kepada Alik Dakirin untuk diolah menjadi mata uang digital, antara lain berupa:

a. Data *E-Mail Result* yang berisikan data *Credit Card (*Data Kartu Kredit) milik orang lain.
b. Data akun *marketplace* (Venmo, Paxful, Indodax).
c. Voucher Indodax untuk transaksi mata uang Digital/Kripto.

Setiap data yang didapatkan, akan dijual kepada Harry togu dengan harga Rp 200 ribu hingga Rp 300 ribu per data. Atas kegiatan ilegal yang dilakukannya tersebut, Rohmat hidayat dan kawan-kawannya

mendapatkan keuntungan masing-masing Rp. 50.000.000 (lima puluh juta rupiah) setiap bulannya.

Berkenaan dengan unsur kesalahan yakni harus melakukan perbuatan pidana, berdasarkan fakta – fakta dipersidangan Para terdakwa telah terbukti melakukan perbuatan pidana dimana telah terpenuhinya unsur–unsur dalam pasal. Sesuai dengan penelitian yang telah diuraikan, maka unsur pertanggungjawaban pidana pada orang yang dengan sengaja melakukan tindak pidana berupa *phishing* yang telah terbukti secara sah dan meyakinkan, dan Para terdakwa dapat dimintai pertanggungjawaban pidana sebagaimana perbuatan terdakwa. Berdasarkan hasil pemeriksaan dan persidangan, menurut perannya masing-masing bahwa Para terdakwa oleh hakim dinyatakan telah terbukti bersalah dengan melakukan perbuatan pidana yakni:

a. Rohmat Hidayat atas perbuatannya telah dinyatakan memenuhi unsur "secara bersama-sama ataupun sendiri-sendiri sebagai orang yang melakukan, yang menyuruh melakukan dan yang turut serta melakukan, dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik" dan melanggar Pasal 30 ayat (2) Jo Pasal 46 ayat (2) Undang-Undang RI No. 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 tahun 2008 tentang ITE jo Pasal 55 ayat (1) ke-1 KUHP. Hakim menjatuhkan pidana kepada terdakwa Rohmat

Hidayat oleh karena itu dengan pidana penjara selama 1 (satu) Tahun dan 8 (delapan) Bulan dan denda sebesar Rp.25.000.000,00 (dua puluh lima juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 1 (satu) Bulan;

b. Harry Togu Setiawan atas perbuatannya telah dinyatakan memenuhi unsur "dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik", dan melanggar Pasal 30 ayat (2) Jo Pasal 46 ayat (2) UU.RI.Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik Jo UU.RI.Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik Jo Pasal 55 ayat (1) ke-1 KUHP. Oleh karena itu, Hakim menjatuhkan sanksi dengan pidana penjara selama 1 (Satu) tahun dan 8 (Delapan) bulan serta denda sebesar Rp. 25.000.000,- (Dua puluh lima juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 1 (Satu) bulan.

c. Alik Dakirin atas perbuatannya telah dinyatakan memenuhi unsur "secara bersama-sama dengan sengaja dan tanpa hak mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik" dan melanggar Pasal 30 ayat (2) Jo Pasal 46 ayat (2) UU.RI Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik

Jo UU.RI.Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik Jo Pasal 55 ayat (1) ke-1 KUHP. Hakim menjatuhkan pidana kepada terdakwa Alik Dakirin oleh karena itu dengan Pidana Penjara selama 1 (satu) tahun dan 3 (tiga) bulan dan denda sebesar Rp.25.000.000,- (dua puluh lima juta rupiah) dengan ketentuan apabila pidana denda tersebut tidak dibayar, maka akan diganti dengan pidana penjara selama 1 (satu) bulan.

d. Reno Suryokusumo atas perbuatannya telah dinyatakan memenuhi unsur "turut serta melakukan dengan sengaja dan tanpa hak atau melawan hukum melakukan transmisi, memindahkan atau mentransfer suatu informasi elektronik dan/atau dokumen elektronik milik orang lain", dan melanggar Pasal 32 ayat 2 jo. Pasal 48 ayat 2 UU ITE jo. Pasal 55 ayat 1 ke-1 KUHP. Hakim menjatuhkan pidana kepada terdakwa Reno Suryokusumo dengan pidana penjara selama 1 (Satu) tahun dan 8 (Delapan) bulan serta denda sebesar Rp.25.000.000 (Dua puluh lima juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 1 (Satu) bulan.

Terdapat ketidak sesuaian amar putusan dengan teori penyertaan yang ditegaskan dalam Pasal 55 ayat (1) KUHP bahwa kedudukan *pleger*, *medepleger*, dan *uitlokker* dianggap sebagai pembuat (*daader*) sehingga hukuman atau sanksi yang diberikan adalah sama. Dalam hal

ini Alik dakirin sebagai medepleger memiliki selisih pidana penjara selama 5 (lima) bulan lebih ringan dibandingkan dengan sanksi terdakwa lainnya, yaitu pidana penjara selama 1 (satu) tahun dan 8 (delapan) bulan.

BAB IV

PENUTUP

A. Kesimpulan

1. Modus operandi tindak pidana *phishing* melalui putusan pengadilan pada Pengadilan Negeri Surabaya

Dari riset terhadap putusan di Pengadilan Negeri Surabaya dari tahun 2019 sampai 2021 ditemukan bahwa modus operandinya, sebagai berikut:

a. Putusan Nomor: 1193/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1194/Pid.Sus/2021/PN.SBY.

Identifikasi modus operandi dalam putusan terkait antara lain adalah *phishers* telah memilih target terlebih dahulu yaitu warga Amerika Serikat yang diberikan dana pengangguran oleh pemerintah. Sesuai dengan tujuan awalnya, pembuatan *website phishing* difokuskan untuk mendapatkan data kartu kredit. Pembuatan *website* yang dilakukan oleh Michael Zeboth adalah dengan menggunakan teknik *script spampage* atau lamannya dibuat serupa dengan web instansi resmi pemerintahan AS. *Link website* tersebut kemudian disebarkan melalui SMS dengan pesan yang berisi tentang perubahan regulasi pada kartu kredit. Tahap lanjutan adalah diharapkannya target untuk mengakses link, mengikuti, dan mengisi berdasarkan seluruh isntruksi didalamnnya. Jika target terkelabui, informasi data yang diketikkan dalam web akan secara otomatis terkirim ke email *phishers* yang nantinya akan dimanfaatkan dengan melawan hukum

b. Putusan Nomor: 2205/Pid.Sus/2021/PN.SBY, Putusan Nomor: 2182/Pid. Sus/2021/PN.SBY dan Putusan Nomor: 2206/Pid.Sus/2021/PN.SBY

Identifikasi modus operandi dalam putusan terkait adalah bahwa *phishers* telah memilih target terlebih dahulu yaitu warga Negara Amerika (USA). Sesuai dengan tujuan awalnya, pembuatan *website* difokuskan untuk mendapatkan identitas diri target dan nomor kartu kredit dan kode exp. Pembuatan *website* dilakukan dengan teknik *script spampage*, kemudian disebarkan melalui *e-mail* secara random ke warga Negara Amerika. Kelalaian dan ketidak telitian target akan menjadi keuntungan *phishers* ketika target mengakses *website phishing*. Ketika target mengakses *website phishing*, target akan digiring untuk mengikuti instruksi dalam halaman *website* tersebut. Setelah target mengisi seluruh instruksi, data yang diketikkan tersebut akan otomatis terkirim ke *email phishers* yang nantinya akan dimanfaatkan dengan melawan hukum.

c. Putusan Nomor: 1855/Pid.Sus/2021/PN.SBY, Putusan Nomor: 1837/Pid. Sus/2021/PN.SBY, dan Putusan Nomor: 1872/Pid.Sus/2021/PN.SBY.

Identifikasi modus operandinya adalah bahwa *phishers* telah memilih target terlebih dahulu yaitu nasabah *Bank of America* (BOA). Sesuai dengan tujuannya, pembuatan *website phishing* difokuskan untuk mendapatkan data finansial berupa kartu kredit. Pembuatan *website* dilakukan dengan teknik *script spampage. Website* tersebut kemudian disebarkan melalui *e-mail* dalam bentuk *link*. Ketika target mengakses link tersebut, Ia akan digiring untuk mengisi nomor kartu kredit, masa aktif

kartu kredit, cvv kartu kredit, nama dan alamat pemilik kartu kredit, nomor telepon pemilik kartu kredit, tanggal lahir pemilik kartu kredit, SSN (*social security number*) dan *ip address*. Target yang mempercayai dan mengsubmit isi web tersebut akan otomatis terkirim ke email *phishers* yang nantinya akan dimanfaatkan dengan melawan hukum.

2. Pertanggungjawaban pidana tindak pidana *phishing* melalui putusan pengadilan pada Pengadilan Negeri Surabaya

Dari riset terhadap putusan di Pengadilan Negeri Surabaya dari tahun 2019 sampai 2021, terkait dengan aspek pertanggungjawaban pidana ditemukan ulasan sebagai berikut:

a. Putusan Nomor: 1193/Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1194/Pid.Sus/2021/PN.SBY.

Pertanggungjawaban pidana adalah pertanggungjawaban atas kejahatan yang dilakukan. Dapat dipidananya seseorang ditentukan bahwa apabila telah memenuhi 4 unsur pertanggungjawaban pidana, dan hasil penelitian menunjukkan bahwa seluruh terdakwa telah memenuhi 4 unsur pertanggungjawaban pidana, sehingga atas perbuatannya dapat dimintai pertanggungjawaban. Bentuk pertanggungjawaban pidana yang harus ditanggung oleh para terdakwa adalah berupa pidana penjara selama 2 (dua) tahun dikurangkan masa penahanan dan pidana denda sebesar Rp.5.000.000 (lima juta rupiah). Sebab perbuatan yang dilakukannya secara terang-terangan telah dilarang oleh perundang-undangan sesuai dengan kejahatan dan perbuatan yang dilakukan diancam dengan Pasal 35

ayat (1) jo. Pasal 51 ayat (1) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP. Dalam putusan terkait di temukan beberapa cara turut serta melakukan tindak pidana, yaitu: Michael Zeboth sebagai pleger, dan Shofiansyah Fahrurrozi sebagai medepleger, dianggap sebagai pelaku atau pembuat tindak pidana sehingga ancaman hukumannya sama.

b. Putusan Nomor: 2205/Pid.Sus/2021/PN.SBY, Putusan Nomor: 2182/Pid.Sus /2021/PN.SBY, Putusan No: 2206/Pid.Sus/2021/PN.SBY

Hasil penelitian menunjukkan bahwa seluruh terdakwa telah memenuhi 4 unsur pertanggungjawaban pidana, sehingga atas perbuatannya dapat dimintai pertanggungjawaban. Bentuk pertanggungjawaban pidana yang harus ditanggung oleh para terdakwa adalah berupa pidana penjara selama 10 (sepuluh) bulan dan pidana denda sebesar Rp. 2.500.000 (dua juta lima ratus ribu upiah). Sebab perbuatan yang dilakukannya secara terang-terangan telah dilarang oleh perundang-undangan sesuai dengan kejahatan dan perbuatan yang dilakukan diancam dengan Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP. Dalam putusan terkait di temukan beberapa cara turut serta melakukan tindak pidana, yaitu: Rico Aprianza sebagai pleger, Thofan Permana dan Gabriel Fransisco sebagai medepleger, dianggap sebagai pelaku atau pembuat tindak pidana sehingga ancaman hukumannya sama.

c. Putusan nomor: 1855/Pid.Sus/2021/PN.SBY, Putusan Nomor: 1837/ Pid.Sus/2021/PN.SBY, dan Putusan Nomor: 1872/Pid.Sus/2021/PN.SBY.

Hasil penelitian menunjukkan bahwa seluruh terdakwa telah memenuhi 4 unsur pertanggungjawaban pidana, sehingga atas perbuatannya dapat dimintai pertanggungjawaban. Bentuk pertanggungjawaban pidana yang harus ditanggung oleh para terdakwa adalah berupa pidana penjara selama 1 tahun 8 bulan dan pidana denda sebesar Rp. 25.000.000. Sebab perbuatan yang dilakukannya secara terang-terangan telah dilarang oleh perundang-undangan sesuai dengan kejahatan dan perbuatan yang dilakukan diancam dengan Pasal 30 ayat (2) jo. Pasal 46 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP. Dalam putusan terkait di temukan beberapa cara turut serta melakukan tindak pidana, yaitu: Reno Suryokusumo sebagai *pleger*, Rohmat Hidayat dan Alik Dakirin sebagai *medepleger*, dan Harry Togu sebagai *uitlokker* dianggap sebagai pelaku atau pembuat tindak pidana sehingga ancaman hukumannya sama. Namun terdapat ketidaksesuaian teori dengan putusan yaitu berupa hukuman penjara yang ditanggungjawabkan kepada Alik Dakirin selama 1 tahun 3 bulan dengan perbuatan yang diancam dengan Pasal 30 ayat (2) jo. Pasal 46 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP.

B. Saran

Berdasarkan hasil analisis serta kesimpulan yang telah saya jabarkan diatas, maka saya membagi saran saya untuk pihak pemerintah, lembaga penegak hukum, dan warga sipil. Dalam hal ini, supaya saran dapat digunakan dan ditujukan kepada setiap pihak dengan sesuai dan jelas.

1. Pemerintah

   Perlunya untuk merancang regulasi khusus yang berkaitan dengan kejahatan *cybercrime*. Regulasi khusus yang dimaksud adalah berupa peraturan secara spesifik mengatur mengenai kejahatan mayantara yang melibatkan media elektronik dan internet khususnya pada kejahatan *phishing*. Pemerintah juga diharapkan untuk meningkatkan perlindungan data pribadi mengingat kemampuan *hacker* yang reliabel hingga dapat melintasi batas negara.

2. Lembaga Penegak Hukum

   Pentingnya untuk menelusuri atau *monitoring* secara berkala dengan melakukan patroli siber untuk menjaring pelaku kejahatan siber. Kemudian bagi lembaga peradilan diharapkan lebih tegas dalam hal penjatuhan hukuman atau sanksi. Diharapkan untuk memberikan sanksi maksimal berdasarkan hukum yang menjeratnya.

3. Masyarakat

   Pentingnya untuk mengetahui modus operandi pengelabuan agar dapat mengetahui bagaimana modus yang digunakan dalam kegiatan *phishing*. Kurangnya kesadaran masyarakat sekarang bahwa jenis kejahatan baru telah muncul yang lebih berbahaya daripada yang lain. Kita harus saling melindungi agar tidak terpengaruh oleh kejahatan dunia maya.

DAFTAR PUSTAKA

Buku

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Cetakan pertama, PT. Refika Aditama, Bandung, 2010.

A.F. Lamintang & Fraciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana di Indonesia*, Cetakan keenam, Sinar Grafika, Jakarta, 2014.

Agus Rusianto, *Tindak Pidana dan Pertanggungjawaban Pidana*, Cetakan pertama, Prenadamedia Group, Jakarta, 2016.

Bachtiar, *Metode Penelitian Hukum*, Cetakan pertama, UNPAM PRESS, Tangerang Selatan, 2018.

Chairul Huda, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*, Cetakan kedua, Kencana, Jakarta, 2006.

E. Y. Kanter & S.R. Sianturi, *Asas -Asas Hukum Pidana di Indonesia dan Penerapannya*, Cetakan ketiga, Storia Grafika, Jakarta, 2012.

H. Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam*, Cetakan pertama, Sinar Grafika, Jakarta, 2004.

Jan Remmelink, *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting KUHP Belanda dan padanannya Dalam KUHP Indonesia*, Cetakan pertama, PT. Gramedia Pustaka Utama, Jakarta, 2003.

J.M.van Bemmelen, *Hukum Pidana 1: Hukum Pidana Material Bagian Umum*, Binacipta, Bandung, 1984.

Moeljatno, *Asas-Asas Hukum Pidana*, Cetakan ketiga, PT.Bina Aksara, Jakarta, 1995.

Muhaimin, *Metode Penelitian Hukum*, Cetakan. pertama, Mataram University Press, NTB, 2020.

Muladi Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Cetakan kedua, Alumni, Bandung, 1992.

Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime*, Edisi kedua, Abingdon, Routledge, 2015.

Satjipto Rahardjo, *Ilmu Hukum*. Cetakan keenam, Citra Aditya Bakti, Bandung, 2006.

Humphrey Wangke, *Kejahatan Transnasional Di Indonesia Dan Upaya Penanganannya, Cetakan pertama*, P3DI Sekertariat Jendral DPR RI, Jakarta Pusat, 2011.

Jurnal

Chant S. R. Ponglabba, "Tinjauan Yuridis Penyertaan Dalam Tindak Pidana Menurut KUHP", *Jurnal Hukum*, No. 6, Vol. 6, 2017.

Destya Fidela Pratiwi, "Pertanggungjawaban Tindak Pidana Skimming", *Jurnal Hukum*, No.4, Vol. 2, 2019.

Dewi Bunga, "Politik Hukum Pidana Terhadap Penanggulangan", *Jurnal Legislasi Indonesia*, No. 1, Vol. 16, 2019.

Erika Magdalena Chandra, "Victimless Crime in Indonesia: Should We Punished Them?", *Padjadjaran Journal of Law*, No.2, Vol. 6, 2019.

Fahrurrozi, "Sistem Pemidanaan Dalam Penyertaan Tindak Pidana Menurut KUHP", *Jurnal Ilmu Hukum*, No.1, Vol. 10, 2019.

Ike Indra, "Pembantuan Dan Penyertaan (*Deelmening*) Dalam Kasus Perkosaan Anak", *Jurnal Hukum Media Iuris*, No. 2, Vol. 1, 2018.

I.Radiansyah, Candiwan and Y. Priyadi, "Analisis Ancaman *Phishing* Dalam Layanan Online Banking", *Jurnal Pengabdian dan Pemberdayaan Masyarakat*, No. 1 Vol. 7, 2019.

Kurniawan & Pujiyono, "Modus Operandi Korupsi Pengadaan Barang Dan Jasa Pemerintah Oleh PNS", *Jurnal Law Reform*, No. 1, Vol. 14, 2018.

Made Sugi Hartono, "Korupsi Kebijakan Oleh Pejabat Publik (Suatu Analisis Perspektif Kriminologi)", *Jurnal Komunikasi Hukum*, No.2, Vol. 2, 2016.

M.E. Fuady, "Cybercrime: Fenomena Kejahatan melalui Internet di Indonesia", *MediaTor*: *Jurnal Komunikasi*, No.2, Vol.6, 2005.

Muhammad Maulana Zaki, "Aspek Pidana Cyberstalking Sebagai Salah Satu Bentuk Cybercrime", *Jurist-Diction*, No.3, Vol. 5, 2022.

Massulthan Rafi Wijaya, Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?, *Indonesian Journal Of Criminal Law Studies*, No.1, Vol. 5, 2020.

Rodliyah, "Konsep Pertanggungjawaban Pidana Korporasi *(Corporate Crime)* dalam Sistem Hukum Pidana Indonesia", *Jurnal Kompilasi Hukum*, No. 1, Vol. 5, 2020.

Vikran Fasyadhiyaksa Putra Y. "Modus Operandi Tindak Pidana *Phishing* Menurut UU ITE", *Jurnal Hukum*, No. 6 Vol. 4, 2021.

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 j.o Undang-Undang Nomor 19 Tahun 2016 tentang Informasi Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP).

Putusan Pengadilan

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 1193/Pid.Sus/2021/PN.SBY.

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 1194/Pid.Sus/2021/PN.SBY.

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 2205/Pid.Sus/2021/PN.SBY.

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 2182/Pid.Sus/2021/PN.SBY.

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 2206/Pid.Sus/2021/PN.SBY.

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 1855/Pid.Sus/2021/PN.SBY.

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 1837/Pid.Sus/2021/PN.SBY.

Putusan Pengadilan Negeri pada Pengadilan Negeri Surabaya Nomor 1872/Pid.Sus/2021/PN.SBY.

Artikel Elektronik

https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/.

https://www.acronis.com/id-id/blog/posts/acronis-cyberthreats-report2022-unveils-cyberthreat-predictions/.

https://www.cips-indonesia.org/publications/perlindungan-keamanansiber-di-indonesia?lang=id.

https://jurnalsecurity.com/jenis-modus-operandi-cybercrime/.

http://myprojectfamous.blogspot.com/2017/08/perbedaanpenyertaandeelneming-pleger.html.

https://kbbi.lektur.id/data-pribadi

https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114522-4891.pdf

https://www.ekrut.com/media/*phishing*-adalah

https://berkas.dpr.go.id/puslit/files/infografis/infografis-public-72.pdf

https://www.cnnindonesia.com/teknologi/20220325194851-192-776315/3180-serangan-*phishing*-awal-2022-lembaga-keuangan-jadi-sasaran-utama

https://finance.detik.com/moneter/d-2817485/bayar-parkir-elektronik-bisa-pakai-kartu-apa-saja

https://www.niagahoster.co.id/blog/mengatasi*phishing*/#Bagaimana_Sebuah_Aksi_ *Phishing*_Dijalankan

https://www.antaranews.com/berita/2783013/lebih-dari-3000-*phishing*-terjadi-di-indonesia-kuartal-pertama-2022

https://www.cnbcindonesia.com/tech/20210306162132-37-228322/kasus-*phishing*-email-yang-serang-indonesia-makin-merajalela

https://www.niagahoster.co.id/blog/mengatasi*phishing*/#Bagaimana_Sebuah_Aksi_ *Phishing*_Dijalankan

http://myprojectfamous.blogspot.com/2017/08/perbedaanpenyertaandeelneming-pleger.html

https://rumaysho.com/3727-taat-pada-pemimpin-pada-selain-perkara-maksiat.html

https://islam.nu.or.id/tafsir/tafsir-surat-al-baqarah-ayat-42-Tcchv

https://www.referensimakalah.com/2013/04/pengertian-jarimah-qishas-dan-diyat.html

https://www.zenius.net/blog/pengertian-jenis-kriminalitas

LAMPIRAN

FAKULTAS HUKUM
Gedung Fakultas Hukum
Universitas Islam Indonesia
Jl.Kaliurangkm 14,5 Yogyakarta55584
T. (0274)7070222
E. fh@uii.ac.id
W law.uii.ac.id

SURAT KETERANGAN BEBAS PLAGIASI

No. : 378/Perpus/20/H/XI/2022

Bismillaahhirrahmaanirrahaim

Yang bertanda tangan di bawah ini:

Nama	: **Joko Santosa, A.Md.**
NIK	: **961002136**
Jabatan	: **Staf Perpustakaan Referensi Fakultas Hukum UII**

Dengan ini menerangkan bahwa :

Nama	: Maulida Diah Laurentina
No Mahasiswa	: 18410617
Fakultas/Prodi	: Hukum
Judul karya ilmiah	: MODUS OPERANDI TINDAK PIDANA PHISHING DAN PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PHISHING DI SURABAYA (STUDI PUTUSAN PENGADILAN)

Karya ilmiah yang bersangkutan di atas telah melalui proses uji deteksi plagiasi dengan hasil **13**.%

Demikian surat keterangan ini dibuat agar dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 30 November 2022 M
06 Jumadil Awwal 1444 H

Perpustakaan Referensi FH UII

Joko Santosa, A.Md.