BAB I

PENDAHULUAN

1.1. Latar Belakang

Indonesia merupakan negara dengan penduduk yang memiliki berbagai jenis suku ras dan Bahasa. Negara Indonesia merupakan negara hukum yang sebagaimana diterangkan di dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Kesatuan Republik Indonesia tahun 1945, yang berbunyi "*Negara Indonesia adalah negara hukum*", yang di mana artinya negara adalah pemegang kekuasaan hukum tertinggi untuk menegakan kebenaran dan keadilan, serta tidak ada kekuasaan yang tidak dipertanggungjawabkan. Pasal tersebut menjelaskan bahwa kekuasaan negara Indonesia dijalankan melalui hukum yang berlaku di segala aspek kehidupan dan telah diatur dalam peraturan yang sah sehingga akan mampu menegakkan hukum dan memecahkan konflik yang terjadi di masyarakat Indonesia khususnya. Tujuan dari penegakan hukum adalah memberikan jaminan terlaksananya keadilan dan perlindungan hukum terhadap harkat dan martabat manusia,ketertiban,ketentraman,dan kepastian hukum sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Dalam era modern seperti sekarang ini, internet merupakan suatu hal yang tidak dapat dipisahkan dalam kehidupan sehari-hari di masyarakat. Keberadaan internet tentu saja semakin memudahkan kehidupan. Banyak hal yang dapat dilakukan dengan internet. Misalnya sebagai sarana komunikasi, *e-money*, internet banking, dan masih banyak lagi. Internet sudah menjadi kebutuhan hidup di hampir sebagian besar masyarakat. Internet telah menghadirkan realitas kehidupan

baru kepada manusia. Internet telah mengubah jarak dan waktu menjadi tidak terbatas. Dengan internet, manusia dapat melakukan berbagai aktivitas yang dalam dunia nyata sulit dilakukan.

Disamping banyaknya manfaat serta kemudahan yang didapatkan dari penggunaan internet, tak jarang pula terdapat hal negatif yang ditimbulkan dari penggunaan internet ini sendiri. Untuk melindungi dan menghormati hak-hak masyarakat dibidang kebebasan serta memberikan keadilan yang merata bagi seluruh masyarakat dengan pertimbangan keamanan dan ketertiban umum terutama dalam bidang teknologi informasi, maka dibentuklah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kemudian di Tahun 2016 dilakukan perubahan terhadap undang-undang tersebut yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lalu di tahun 2024 saat ini dilakukan perubahan kembali agar terwujud keadilan, ketertiban umum, dan kepastian hukum yaitu dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Informasi dan Transaksi Elektronik bermaksud untuk melindungi hak dan kewajiban bagi para pengguna internet. Karena kejahatan tidak hanya ada pada dunia nyata tetapi juga di dunia maya. Kejahatan yang dilakukan dengan media internet ini dikenal pula dengan istilah *cyber crime*. *Cyber crime* sendiri adalah suatu bentuk kejahatan yang dilakukan menggunakan jaringan komputer sebagai unsur utamanya. “Hingga hari ini kasus kejahatan di

dunia maya (*cyber crime*) semakin bertambah, modusnya pun makin beragam, serta makin bervariasi karateristik pelaku kejahatannya, dan makin serius akibatnya".[1]

"Kehadiran teknologi informasi, ternyata masih belum diikuti dengan perkembangan hukum yang dapat mengikuti percepatan kemajuan teknologi komunikasi sehingga diperlukan adanya perangkat hukum yang dapat menyelesaikan suatu permasalahan yang terjadi di dunia maya (*cyber space*)".[2] Pada satu sisi, perkembangan dunia IPTEK (Ilmu Pengetahuan dan Teknologi) yang demikian mengagumkan itu memang telah membawa manfaat yang luar biasa bagi kemajuan peradaban umat manusia. Jenis-jenis pekerjaan yang sebelumnya menuntut kemampuan fisik yang cukup besar, kini relatif sudah bisa digantikan oleh perangkat mesin-mesin otomatis.

Demikian juga ditemukannya formulasi-formulasi baru kapasitas komputer, seolah sudah mampu menggeser posisi kemampuan otak manusia dalam berbagai bidang ilmu dan aktivitas manusia. Kemajuan teknologi informasi yang serba digital membawa orang ke dunia bisnis yang revolusioner (*digital revolution era*) karena dirasakan lebih mudah, murah, praktis dan dinamis berkomunikasi dan memperoleh informasi. Di sisi lain, berkembangnya teknologi informasi menimbulkan pula sisi rawan yang gelap sampai tahap mencemaskan dengan kekhawatiran pada perkembangan tindak pidana di bidang teknologi informasi yang berhubungan dengan kejahatan mayantara atau "*cyber crime*". Masalah

---

[1] Widodo, *Memerangi Cybercrime Karateristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi*, Asswaja Pressindo, Yogyakarta, 2013, h. 1.

[2] Ridwan (dkk), *Penilaian Alat Bukti Elektronik Dalam Perkara Perdata*, Jurnal Hukum dan Pembangunan, Vol.52, No.2, 2019, h. 35.

kejahatan mayantara dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama pada perkembangan teknologi informasi masa depan, karena kejahatan ini termasuk salah satu

"Kejahatan melalui teknologi informasi ataupun yang dikenal *cyber crime* ialah representasi dari kejahatan internasional yang memakai *hitech* sebab karakteristik serta kejahatan yang sangat menonjol merupakan *borderless* atau tidak mengenal batasan negara".[3] *Cyber crime* ialah tindak kejahatan ataupun aktivitas ilegal yang dijalankan lewat jaringan dunia elektronik. Kriminalitas dalam jaringan internet terus menjadi berisiko disebabkan ruang lingkup aksi tersebut sangat luas. Aksi kriminal dalam internet ialah kejahatan yang berhubungan dengan dunia maya yang bisa membahayakan privasi seorang. Kejahatan di dunia maya terus menjadi banyak totalnya serta terus menjadi banyak variasi yang dilakukan para pelaku. Para pelaku dengan mudah malakukan tindak kejahatan dengan menggunakan kemajuan teknologi informasi. " Contoh dari kejahatannya semacam pornografi, perjudian *online, terorisme, hacking, carding, phishing,* serta masih banyak tindak kejahatan yang lain".[4]

Pencurian informasi dalam dunia internet dapat disebuat sebagai *phising*, ialah aksi kejahatan memperoleh data privasi seorang secara ilegal. Dari tindakan tersebut butuh memperoleh nomor kartu kredit, PIN, User ID, nomor telepon, nomor rekening, serta data informasi pribadi yang lain. Dari aksi tersebut setelah

---

[3] Cemban Galuh Sambodo and Sri Endah Wahyuningsih, *The Criminal Law Enforcement Against Crime Of Carding In Electronic Transactions*, Law Development Journal, Vol.3, No.2, 2021, h. 240.

[4] Ni Putu Rai Yuliartini and Kadek Desy Pramita, *Analysis of Workload, Rest Rights, and the Rights to Enjoy Entertainment in Gender Differences*, Jurnal Komunikasi Hukum Vol.8, No.1, 2022, h. 480.

itu pelaku menggunakan untuk kejahatan yang bisa merugikan bagi korban yang dicuri informasinya serta korban yang lain yang hendak dijadikan sasaran dari pelaku untuk menipu. Tingkatan ancaman kejahatan eksploitasi data ataupun informasi pribadi di Indonesia telah sangat beresiko kala pemerintah menetapkan kebijakan Kartu Tanda Penduduk elektronik (e-KTP) yang merupakan tata cara pendataan data ataupun informasi pribadi masyarakat oleh pemerintah yang pertama kali dijalankan pada tahun 2011, ialah penerapan dari metode Nomor Induk Kependudukan (NIK). "Dalam kebijakan tersebut menginginkan identitas tiap penduduk berlaku seumur hidup, serta tiap orang memiliki 1 (satu) kartu yang dimana dalam kartu tersebut ada Nomor Induk Kependudukan (NIK). Segala data pribadi penduduk direkam yang di dalamnya tercantum identitas serta ciri-ciri fisik".[5]

> *Phising* merupakan salah satu upaya untuk mendapatkan informasi data seseorang dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/*legitimate organization* dan biasanya berkomunikasi secara elektronik. Data yang menjadi sasaran biasanya berupa data diri seperti nama, usia, alamat, kemudian data akun seperti *username* dan *password*, dan data finansial yang berkaitan dengan informasi kartu kredit atau nomor rekening. Istilah *phising* ini berasal dari kata *fishing* yang berarti memancing.[6]

Kegiatan *phising* ini memang bertujuan untuk memancing orang atau korban agar memberikan informasi pribadi secara tanpa ia sadari dan informasi tersebut nantinya akan digunakan untuk kejahatan. Modus kejahatan ini biasanya diawali dengan mengatasnamakan instansi resmi dengan menggunakan *website* atau *email* palsu untuk mengelabuhi korban.

---

[5] *Ibid,* h. 481.

[6] Efvy Zam, *Phising Trik Mudah Penyadapan Password Dan Pencegahannya,* Mediakita, Jakarta, 2014, h. 2.

Cara kerja *phising* bermula dari pelaku (*scammer*) akan menghubungi kepada korban dan berpura-pura berasal dari bisnis yang sah seperti bank, telepon atau penyedia layanan internet melalui *email*, media sosial, telepon, atau pesan SMS. Pesan *phising* dirancang agar terlihat asli, dan sering menyalin format yang digunakan oleh organisasi yang ditiru oleh *scammer*, termasuk merek dan logo mereka. Mereka akan membawa korban ke situs palsu yang terlihat seperti betulan, namun memiliki alamat yang sedikit berbeda. Misalnya, jika situs yang sah adalah "*www.realbank.com.au*", si penipu dapat menggunakan alamat seperti "*www.reallbank.com*". Jika korban memberikan *scammer* dengan rincian data secara *online* atau melalui telepon, mereka akan menyalahgunakannya untuk melakukan kegiatan penipuan, seperti menggunakan kartu kredit dan mencuri uang korban.

Tipe *phising* yakni *spear phising* adalah bentuk serangan siber yang ditargetkan, di mana pelaku menyamar sebagai individu atau entitas tepercaya untuk menipu target tertentu agar memberikan informasi sensitif, seperti data login, informasi keuangan, atau akses ke sistem internal. Berbeda dengan phishing umum yang menyasar banyak orang secara massal, spear phishing dirancang secara spesifik berdasarkan profil atau kebiasaan korban, sehingga terlihat lebih meyakinkan dan sulit dikenali. Yang berdampak pada Kebocoran data pribadi atau Perusahaan; Kerugian finansial; Kerusakan reputasi; Akses kejaringan internet; dan Ancam hukum dan kepatuhan.

Berdasarkan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan

Transaksi Elektronik, yaitu "*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik*". Dikenakan ancaman pidana Pasal 51 ayat (1) yang berbunyi "*Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00. (dua belas miliar rupiah)*".

Seperti halnya contoh kasus dalam Perkara Nomor 845/PID.SUS/2020/PT SBY, yang dilakukan oleh Kingditho Wulanesa Mahardika pada hari Selasa tanggal 28 Mei 2019 atau setidaknya pada waktu lain dalam bulan Mei 2019, bertempat Jln. Gedongsongo Timur No. 04 RT. 001 RW. 001 Kelurahan Manyaran Kecamatan Semarang Barat Kota Semarang, atau setidaknya di suatu tempat yang masih termasuk dalam daerah hukum Pengadilan Negeri Surabaya, berdasarkan Pasal 84 KUHAP membantu tindak pidana Informasi dan Transaksi Elektronik dengan sengaja dan tanpa hak atau melawan Hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada System Elektronik milik orang lain yang tidak berhak orang yang membantu melakukan perbuatan Pidana yang dilakukan. Dalam perkara tersebut majelis hakim hanya menjatuhkan hukuman kepada terdakwa dengan pidana penjara selama 1 (satu) tahun dan pidana denda sebesar Rp. 30.000.000,00 (tiga puluh juta rupiah), apabila denda tidak dibayar diganti dengan 2 (dua) bulan

kurungan. Sehingga menurut hemat penulis majelis hakim dalam memutus perkara tersebut belum mencerminkan rasa keadilan bagi pihak korban.

Mengenai perbuatan terdakwa dalam kasus *spear phising* tersebut tergolong bersekala besar dimana terdakwa menggunakan sosial media *facebook* untuk menipu banyak korbannya. Serangan *spear phishing* skala besar biasanya dilakukan dengan mengirimkan email atau pesan palsu secara massal menggunakan perangkat otomatis. Contohnya adalah email palsu yang mengaku berasal dari penyedia layanan global seperti *platform* media sosial *facebook*.

Sebagaimana contoh permasalahan diatas merupakan bentuk *cyber spear phising* yakni jenis *phishing* yang menargetkan individu tertentu menggunakan informasi personal mereka seperti di *Facebook*, pelaku biasanya menyamar sebagai teman korban atau membuat akun palsu, lalu mengirim pesan seolah-olah butuh pinjaman uang mendesak. Menyebarkan *link* palsu ke situs *web login* palsu (mirip *Facebook* atau dompet digital) dan menawarkan hadiah atau undian palsu dan meminta data kartu atau *One-Time Password* (OTP).

Beberapa permasalahan hukum normatif terkait penegakan hukum *cyber sper phishing* di Indonesia, antara lain adanya kekosongan hukum istilah dimana Undang-Undang Informasi dan Transaksi Elektronik belum secara eksplisit menyebutkan "*spear phishing*" sebagai tindak pidana tertentu, sehingga penegakan hukumnya bergantung pada interpretasi Pasal-Pasal umum. serta sulitnya mengumpulkan dan memverifikasi alat bukti elektronik secara forensik yang valid dan sah di pengadilan dikarenakan banyak pelaku menggunakan teknik anonimitas, seperti *Virtual Private Network* (VPN) dan *e-mail* palsu, yang

menyulitkan pelacakan. Dan banyak serangan *phishing* berasal dari luar negeri, sementara Undang-Undang Informasi dan Transaksi Elektronik masih terbatas yurisdiksinya seperti adanya keterbatasan kerja sama antar negara dalam ekstradisi dan *digital forensic* lintas batas.

Sehingga mengacu pada uraian latar belakang diatas, penulis tertarik membahas, mengkaji serta meneliti persoalan terkait kejahatan *cyber spear phising* dengan judul penelitian yakni terkait Pertanggungjawaban Tindak Pidana *Cyber Spear Phising* Dalam Perspektif Pencurian Data Pribadi.

1.2. Rumusan Masalah

Dari rangkaian latar belakang masalah yang telah di uraikan di atas dapat di rumuskan masalah yang hendak dikaji adalah :

1. Bagaimana pengaturan hukum terkait tindak pidana *cyber spear phising* dalam perspektif pencurian data pribadi ?
2. Bagaimana pertanggungjawaban hukum terhadap pelaku tindak pidana *cyber spear phising* menurut peraturan perundang-undangan ?

1.3. Tujuan Penelitian

Adapun dalam penelitian ini merupakan sebuah kegiatan yang bertujuan sebagai berikut :

1. Untuk mengetahui dan memahami, pengaturan hukum terkait tindak pidana *cyber spear phising* dalam perspektif pencurian data pribadi.
2. Untuk mengetahui dan memahami, pertanggungjawaban hukum terhadap pelaku tindak pidana *cyber spear phising* menurut peraturan perundang-undangan.

1.4. Manfaat Penelitian

Melalui penelitian ini diharapkan dapat memberikan manfaat dalam ilmu pengetahuan hukum, baik secara teoritis maupun secara prakti, yaitu:

1. Secara teoritis penelitian ini dapat memberikan kontribusi pemikiran dalam rangka pengembangan khasanah ilmu pengetahuan khususnya dibidang hukum pidana mengenai pertanggungjawaban tindak pidana *cyber spear phising* dalam perspektif pencurian data pribadi berdasarkan hukum di Indonesia.
2. Secara praktis penelitian ini dapat menjadi salah satu landasan hukum, rujukan dan/atau referensi sesuai ketentuan hukum mengenai pertanggungjawaban tindak pidana *cyber spear phising* dalam perspektif pencurian data pribadi berdasarkan hukum di Indonesia.

1.5. Tinjauan Pustaka

Dalam penelitian skripsi ini, peneliti menggali informasi dari pendapat para ahli hukum, teori-teori, asas-asas hukum dan beberapa peraturan yang menjadi konstruksi berfikir dalam menjawab pokok permasalahan.

1.5.1. Landasan Konseptual

Landasan konseptual merupakan suatu pengarah, atau pedoman yang lebih konkrit berisikan konsep-konsep umum atau tinjauan umum ketentuan dan pengertian serta hal hal yang berhubungan dengan pokok penelitian, adapun landasan konseptual dalam penelitian ini yaitu:

1.5.1.1. Tinjauan Umum Tindak Pidana

Pidana berasal dari kata *straf* (Belanda), yang adakalanya disebut dengan istilah hukuman. istilah pidana lebih tepat dari istilah hukuman, karena hukum sudah lazim merupakan terjemahan dari *recht*. "Pidana lebih tepat diartikan sebagai suatu penderitaan yang sengaja dijatuhkan atau diberikan oleh negara pada seseorang atau beberapa orang sebagai akibat hukum (sanksi) baginya atas perbuatan yang telah melanggar larangan hukum pidana".[7]

Tindak menunjuk pada hal kelakuan manusia dalam arti positif (*handelen*) semata, dan tidak termasuk kelakuan manusia yang pasif atau negatif (*nalaten*). Padahal pengertian yang sebenarnya dalam istilah *feit* itu adalah baik perbuatan aktif maupun pasif tersebut. "Simons merumuskan *strafbaar feit* adalah suatu tindakan melanggar hukum yang dengan sengaja telah dilakukan oleh seseorang yang dapat dipertanggungjawabkan atas tindakan yang dinyatakan sebagai dapat dihukum".[8]

Menurut Kanter dan Sianturi, memberikan pengertian tindak pidana sebagai berikut: "Tindak pidana ialah suatu tindakan pada tempat, waktu dan keadaan tertentu, yang dilarang (diharuskan) dan diancam dengan pidana oleh Undang-Undang, bersifat melawan hukum, serta dengan kesalahan dilakukan oleh seseorang mampu bertanggungjawab".[9]

---

[7] Adami Chazawi, *Pelajaran Hukum Pidana 1*, Rajawali Pers, Jakarta, 2019, h. 24.
[8] *Ibid*, h. 75.
[9] Erdianto Effendi, *Hukum Pidana Indonesia Suatu Pengantar*, PT Rafika Aditama, Bandung, 2011, h. 99.

Uraian di atas menjelaskan bahwa yang dimaksud dengan tindak pidana yaitu perbuatan yang dilakukan oleh manusia yang dilanggar ataupun perbuatan yang dilarang oleh hukum sehingga dapat dijatuhi sanksi pidana.

Unsur-unsur tindak pidana dapat dibedakan setidak-tidaknya dari 2 (dua) sudut pandang, yakni:

a. Sudut Teoritis
   Teoritis artinya berdasarkan pendapat para ahli hukum, yang tercermin pada bunyi rumusannya.
   Menurut Moeljatno, unsur tindak pidana adalah:
   1) Perbuatan;
   2) Yang dilarang (oleh aturan hukum); dan
   3) Ancaman pidana (bagi yang melanggar larangan).
   Menurut R. Tresna, unsur tindak pidana adalah:
   1) Perbuatan/rangkaian perbuatan (manusia);
   2) Yang bertentangan dengan peraturan perundang-undangan; dan
   3) Diadakan tindakan penghukuman.
b. Sudut Undang-Undang
   Sudut Undang-Undang adalah bagaimana kenyataan tindak pidana itu dirumuskan menjadi tindak pidana tertentu dalam Pasal-Pasal peraturan perundang-undangan. Rumusan-rumusan tindak pidana tertentu dalam KUHP dapat diketahui adanya 11 (Sebelas) unsur tindak pidana, yaitu:
   1) Unsur tingkah laku;
   2) Unsur melawan hukum;
   3) Unsur kesalahan;
   4) Unsur akibat konstitutif;
   5) Unsur keadaan yang menyertai;
   6) Unsur syarat tambahan untuk dapatnya dituntut pidana;
   7) Unsur syarat tambahan untuk memperberat pidana;
   8) Unsur syarat tambahan untuk dapatnya dipidana;
   9) Unsur objek hukum tindak pidana;
   10) Unsur kualitas subjek hukum tindak pidana; dan
   11) Unsur syarat tambahan untuk meringankan pidana.[10]

Diantara 11 (Sebelas) unsur yang telah disebutkan diatas terdapat unsur subjektif dan unsur objektif sebagaimana yang dijelaskan oleh Satochid Kartanegara.

[10] Adami Chazawi, *Op.Cit.*, h. 79.

> Menurut Satochid Kartanegara, menjelaskan bahwa unsur delik terdiri atas unsur objektif dan unsur subjektif. Unsur yang objektif adalah unsur yang terdapat di luar diri manusia yaitu, suatu tindakan, suatu akibat dan keadaan (*omstandigheid*). Kesemuanya itu dilarang dan diancam dengan hukuman oleh Undang-Undang. Sedangkan unsur subjektif adalah unsur-unsur dari perbuatan berupa kemampuan yang dapat dipertanggungjawabkan (*toerekeningsvatbaarheid*), dan kesalahan.[11]

1.5.1.2. Tinjauan Umum *Cyber Crime*

Cyber crime pada awalnya diartikan sebagai kejahatan komputer (*computer crime*). *The British Law Commission* mengartikan *computer crime* sebagai manipulasi komputer yang dilakukan dengan iktikad buruk agar bisa mendapatkan uang, barang, atau keuntungan yang lain atau dapat pula diartikan sebagai timbulnya kerugian bagi pihak lain. Mandell membagi *computer crime* atas 2 (dua) kegiatan, yaitu:[12]

a) Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian untuk bisa mendapatkan keuangan, keuntungan, bisnis, kekayaan atau pelayanan; dan
b) Ancaman bagi komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.

Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri serta sistem informasi yang sebagai sarana untuk menyampaikan atau melakukan pertukaran informasi kepada pihak lainnya. "*Computer crime* merupakan tindak kejahatan yang tidak melibatkan jaringan dan internet tetapi hubungan antara tindak kejahatan dengan komputer sebagai sarana kejahatannya, sedangkan *cyber*

---

[11] Leden Marpaung, *Asas Teori dan Praktik Hukum Pidana*, Sinar Gratika, Jakarta, 2005, h. 10.

[12] Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, Rajawali Pers, Jakarta, 2012, h. 10.

crime merupakan tindak kejahatan dengan menggunakan koneksi internet bahkan bisa menembus negara lain".[13]

Di bidang teknologi informasi kejahatan dapat digolongkan dalam *white colour crime* karena pelaku *cyber crime* adalah mereka yang mengerti dan menguasai penggunaan internet serta aplikasi yang ada atau biasa disebut sebagai orang yang ahli dalam bidangnya. *Cyber crime* memiliki beberapa karakteristik yaitu:[14]

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang atau wilayah, siber atau *cyber*, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya;
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet;
c. Perbuatan tersebut mengakibatkan kerugian berupa materil dan inmateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya; dan
e. Perbuatan tersebut saring dilakukan secara transnasional atau melintas batas negara.

1.5.1.3. Karakteristik dan Bentuk Tindak Pidana *Cyber Crime*

Cyber crime merupakan kejahatan yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, khususnya melalui jaringan internet. Karakteristik utama dari *cyber crime* adalah sifatnya yang tanpa batas wilayah (*borderless*), sehingga pelaku dapat beroperasi dari mana saja di dunia. Selain itu, kejahatan ini bersifat anonim karena pelaku sering menyembunyikan identitasnya dengan teknik enkripsi atau

[13] Maskun dan Wiwik Meilarati, *Aspek Hukum Penipuan Berbasis Internet*, Keni Media, Bandung, 2017, h. 20.
[14] Budi Sahariyanto, *Op.Cit.*, h. 11.

menggunakan identitas palsu. *Cyber crime* juga bersifat cepat dan merusak, di mana dalam hitungan detik data dapat dicuri, dimanipulasi, atau dihancurkan. Kejahatan ini mencakup berbagai bentuk, seperti pencurian data pribadi, peretasan, penyebaran malware, dan penipuan online. Karena bersifat digital, *cyber crime* sering kali sulit dilacak dan dibuktikan secara hukum, menjadikannya tantangan besar bagi penegak hukum di era modern. *Cyber crime* memiliki beberapa karakteristik, yaitu:[15]

a. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber* (*cyber space*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya;
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet;
c. Perbuatan tersebut mengakibatkan kerugian materill maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasian informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya; dan
e. Perbuatan tersebut sering transnasional atau melintas batas negara.

Karakteristik tindak pidana *cyber crime* berbeda dengan tindak pidana yang lain, karakteristik bentuk tindak pidana *cyber crime* antara yang satu dengan yang lain pun berbeda hal ini dikarenakan modus operandi yang digunakan berbeda. Sehingga dengan demikian dalam penegakan hukum dan dalam proses beracaranya dari tahap penyelidikan dan penyidikan memerlukan ketentuan khusus. Ketentuan khusus yang berkaitan dengan acara pidana yang terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah dirubah oleh

[15] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) : Urgensi Pengaturan dan Celah Hukumnya*, PT Raja Grafindo Persada, Jakarta, 2013, h. 13.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah sebagai berikut:

1. Diakuinya alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cyber crime*;
2. Adanya wewenang khusus yang diberiakan kepada Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan transaksi elektronik sebagai penyidik;
3. Adanya kewenangan penyidik, penuntut umum, dan hakim untuk meminta keterangan kepada penyedia jasa dan penyelenggara sistem elektronik mengenai data-data yang berhubungan dengan tindak pidana, dengan tetap terikat terhadap privasi, kerahasian, dan kelancaran layanan publik, integritas data dan keutuhan data; dan
4. Adanya wewenang terhadap penyidik untuk melakukan penggeledahan, penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat, hal ini menghindari agar sistem elektronik tersebut tidak bias hapus oleh pelaku dan menghindari agar pelacakan pelaku berjalan cepat, sehingga jejak pelaku mudah untuk ditemukan.

Cyber crime mempunyai bentuk beragam, karena setiap negara tidak selalu sama dalam melakukan kriminalisasi. Begitu pula, dalam setiap negara dalam menyebut apakah suatu perbuatan tergolong kejahatan *cyber crime* atau bukan kejahatan *cyber crime* juga belum tentu sama. Secara teoritik, berkaitan dengan konsepsi kejahatan. "Muladi mengemukakan bahwa asas *mala in se* mengajarkan bahwa suatu perbuatan dikategorikan sebagai kejahatan karena masyarakat dengan sendirinya menganggap perbuatan tersebut jahat. Sedangkan berdasarkan asas *mala prohibita*, suatau perbuatan dianggap jahat karena melanggar peraturan perundang-undangan".[16] Asas *mala prohibita* menghasilkan konsep si kejahatan dalam arti yuridis (yaitu sebagaimana diatur dalam peraturan perundang-undangan tertulis).

Jonathan Rosenoer menjelaskan tentang bentuk-bentuk *cyber crime* sebagai berikut, yaitu:[17]

1) *Copright, include exclutive right, subject matter of copyright, formalities, infringement, source of risk, word wide web sites, hypertext link, graphical element, e-mail, criminal liability, fair use, first amandment, and softwere rental*;
2) *Trademark*;
3) *Defamation*;
4) *Privacy, include common law privacy, constitutinal law, anonymity, and technology expanding privacy right*;
5) *Duty of care*;

a. *Negligence*;
b. *Negligent misstatement*;
c. *Equipment malfunctions*;
d. *Economic loss may not be recoverable*;
e. *Contractural limitations of liability.*

---

[16] Muladi, *Demokratisasi , Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, Habibie Center, Jakarta, 2002, h. 196.

[17] Jonathan Rosenoer, *Cyberlaw: The Law of The Internet,* Spring Verlag, New York, 1997, h. 45.

6) *Criminal liability; such as; computer fraud and abuse act, wire fraund. Electronic communication privacy act, extortion and threats, expose, sexual exploitation of children, obscene and indent telephone call, copyright stalking*;
7) *Procedural issues, include jurisdiction, venue and conflict of law*; *and*
8) *Electronic contract and digital signature, include electronic agreement enforceable, public key encryption and digital signature.*

Jika diterjemahan dalam bahasa Indonesia yang berarti : 1) *Copright*, termasuk hak eksklusif, materi hak cipta, formalitas, pelanggaran, sumber risiko, situs *web* di seluruh kata, tautan *hypertext,* elemen grafis, *email*, tanggung jawab pidana, penggunaan wajar, amandemen pertama, dan penyewaan *softwere*; 2) Merek dagang; 3) Pencemaran nama baik; 4) Privasi, termasuk privasi hukum umum, hukum konstituensial, anonimitas, dan teknologi yang memperluas hak privasi; 5) Kewajiban perawatan; a. Kelalaian; b. Kesalahan penyajian yang lalai; c. Kerusakan peralatan; d. Kerugian ekonomi mungkin tidak dapat dipulihkan; dan e. Batasan tanggung jawab kontraktual; 6) Tanggung jawab pidana; misalnya; Undang-Undang Penipuan dan Penyalahgunaan Komputer, *Wire Fraund*. Undang-Undang privasi komunikasi elektronik, pemerasan dan ancaman, eksposisi, eksploitasi seksual anak-anak, panggilan telepon cabul dan indentasi, penguntitan hak cipta; 7) Masalah prosedural, termasuk yurisdiksi, tempat dan konflik hukum; dan 8) Kontrak elektronik dan tanda tangan digital, termasuk perjanjian elektronik yang dapat dilaksanakan, enkripsi kunci publik dan tanda tangan digital.

Cyber crime meliputi pelanggaran hak kekayaan intelektual, fitnah atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi

(*privacy*), ancaman dan pemerasan, ekploitasi seksual anak-anak dan pencabulan, perusakan sistem komputer, pembobolan kode akses, dan pemalsuan tanda tangan digital. Semua perbuatan tersebut dapat dipertanggungjawabkan secara pidana sesuai dengan yurisdiksinya. *Cyber crime* juga dapat berbentuk pemalsuan data, penyebaran virus komputer ke jaringan komputer atau sistem komputer, penambahan atau pengurangan sistem instruksi dalam jaringan komputer, pembulatan angka, perusakan data, dan pembocoran data rahasia

The International Hendbook on Computer mengklasifikasikan bentuk-bentuk *cyber crime* sebagai berikut:[18]

1) *Computer-related Economic Crimes*
   a. Fraund by Computer Manipulation;
   b. Computer Espionage and Software Piracy;
   c. Computer Sabotage;
   d. Theft of Services;
   e. Unauthorized Access to DP Systems and Hacking; *and*
   f. Crime The Computer as a Tool for Traditional Business Offences.
2) *Computer-related Infrigements of Privacy*
   a. Use of Incorrect Data;
   b. Illegal Collection and Storage of Correct Data;
   c. Illegal Disclosure and Misuse of data;
   d. Infrigments of Formalities of Privancy Laws.
3) *Further Abuses*
   a. Offences Against State and Political Interests;
   b. The Extension to Offences Against Personal Intergity.

Jika diterjemahan dalam bahasa Indonesia yang berarti : 1) Kejahatan Ekonomi Terkait Komputer; a. *Fraund* dengan Manipulasi Komputer; b. *Spionase* Komputer dan Pembajakan Perangkat Lunak; c. Sabotase Komputer; d. Pencurian Layanan; e. Akses Tidak Sah ke Sistem DP dan

[18] *Ibid.*

Peretasan; f. Kejahatan Komputer sebagai Alat untuk Pelanggaran Bisnis Tradisional; 2) *Infrigations* Privasi Terkait Komputer; a. Penggunaan Data yang Salah; b. Pengumpulan dan Penyimpanan Data yang Benar Secara *Ilegal*; c. Keterbukaan *Ilegal* dan Penyalahgunaan Data; d. Ketentuan Formalitas Undang-Undang *Privancy*; dan 3) Penyalahgunaan Lebih Lanjut; a. Pelanggaran terhadap kepentingan negara dan politik; b. Perpanjangan pelanggaran terhadap gangguan pribadi.

Berdasarkan uraian *Handbook on Computer Crime, cyber crime* dikategorikan menjadi 3 (tiga). Yakni kategori yang pertama, *cyber crime* adalah kejahatan ekonomi yang terkait dengan komputer, meliputi penipuan dengan manipulasi komputer, pembajakan perangkat lunak komputer, spionase komputer, sabotase, pencurian jasa, akses tidak sah ke dalam sistem atau jaringan komputer, komputer sebagai alat untuk menyerang bisnis tradisional. Kategori kedua, adalah pelanggaran terhadap keleluasaan pribadi, yaitu penggunaan data yang tidak benar, pengumpulan data secara tidak sah, penyalahgunaan data, pelanggaran rahasia perusahaan. Sedangkan kategori ketiga, misalnya melakukan penyerangan terhadap dan kepentingan politik, dan penyerangan terhadap kebebasan pribadi orang per orang.

Selain penggolongan *cyber crime* sebagaimana terjabar di atas, Donn Parker mengklasifikasikan bentuk-bentuk *cyber crime* ke dalam 4 (empat) klasifikasi sebagai berikut, yaitu:[19]

1. Komputer sebagai Objek;

[19] Widodo, *Aspek Hukum Kejahatan Mayantara*, Aswindo, Yogyakarta, 2011, h. 199.

Dalam kategori ini, bentuk-bentuk *cyber crime* termasuk kasus kasus perusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusakan terhadap sarana-sarana komputer seperti *Air Condutouring* (AC) dan peralatan yang menunjang pengoprasian komputer.

2. Komputer sebagai Subjek;
   Komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya pencurian, penipuan, dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh (*intangible*), misalnya pulsa elektronis dan guratan-guratan magnetis.
3. Komputer sebagai Alat; dan
   Komputer digunakan sebagai alat melakukan kejahatan sehingga sifat peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh adalah seseorang pelaku kejahatan yang mengambil warkat-warkat setoran darai suatu bank dan menulis nomor rekening pelaku dengan tinta magnetis pada warkat-warkat tersebut kemudian melaetakkan kembali ke tempat semula. Nasabah yang akan memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomor rekening pelaku kejahatan memproses warkat-warkat nasabah, komputer secara otomatis akan mengkredit sejumlah uang pada rekening pelaku kejahatan. Salah satu pelaku kejahatan menarik uang dengan cek dari rekeningnya sebelum peran nasabah yang menyetor mengajukan komplain ke bank.
4. Komputer sebagai Simbol.
   Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman, dalam kategori ini termasuk penipuan "Biro Jodoh" yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu si koraban mencari jodoh, akan tetapi ternyata biro jodoh tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.

Ari Juliano Gema menyatakan bahwa kejahatan siber dapat dikelompokkan menjadi beberapa bentuk, yaitu:[20]

1. *Unauthorized Acces to Computer System and Service*;
   Kejahatan ini dilakukan dengan cara memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau dengan melawan hukum. Contoh bentuk kejahatan siber ini yaitu *cracking, hacking*.
2. *Iilegal Content*;

[20] Wahid, Abdul dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* Refika Aditama, Bandung, 2005, h. 72.

Kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh bentuk kejahatan ini yaitu konten pornografi, berita bohong/*hoax.*

3. *Data Forgery*;
   Merupakan kejahatan dengan memalsukan data pada dokumen dokumen penting yang tersimpan sebagai *scriptless documen* melalui internet.
4. *Cyber Espionage*;
   Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata dengan memasuki sistem jaringan komputer pihak sasaran.
5. *Cyber Sabotage and Extortion*;
   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Contoh bentuk kejahatan ini yaitu penanaman *malware*/virus.
6. *Offence Againts Intellectual Property*; dan
   Kejahatan ini berupa pelanggaran Hak Kekayaan Intelektual (HKI) yang dimilki pihak lain di Internet. Contoh bentuk kejahatan ini misalnya *cloning, phising web*.
7. *Infringement of Privacy*.
   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Informasi yang dimaksud seperti PIN ATM, Nomor Kartu Kredit, NIK dan sebagainya. Contoh bentuk kejahatan ini yaitu pencurian data pribadi.

Bentuk-bentuk *cyber crime* sangat beragam, antara lain *hacking*, yaitu upaya untuk membobol sistem keamanan komputer tanpa izin, *phishing* yaitu penipuan melalui *email* atau situs palsu untuk mencuri data pribadi seperti kata sandi dan informasi keuangan; serta *malware*, yaitu penyebaran perangkat lunak berbahaya yang dapat merusak sistem atau mencuri data. Selain itu, terdapat pula *cyber bullying* yang berupa pelecehan atau penghinaan melalui media sosial, serta penipuan online seperti jual beli fiktif yang merugikan konsumen. Perkembangan teknologi yang pesat membuat pelaku c*yber crime* semakin canggih, sehingga penting bagi

masyarakat untuk waspada dan memahami cara melindungi diri di dunia digital.

1.5.1.4. Bentuk dan Modus Operadi *Cyber Spear Phising*

Bahwa dalam "Kamus hukum mengartikan pencurian sebagai bentuk mengambil kepunyaan orang lain tanpa izin yang biasanya dilaksanakan secara sembunyi-sembunyi".[21] Unsur mengambil bermakna sebagai setiap perbuatan untuk membawa atau mengalihkan suatu barang ketempat lain. Awalnya perbuatan mengambil merujuk pada perbuatan yang menggunakan sentuhan tangan, namun seiring perkembangan zaman. "Pengertian mengambil mengalami perluasan. Termasuk dalam perbuatan mengambil yaitu perbuatan untuk mengalihkan atau memindahkan suatu barang dengan berbagai cara. Perbuatan dapat disebut sebagai mengambil, manakala perpindahan barang telah terjadi".[22]

> *Cyber phishing* merupakan tindakan penipuan dalam pembuatan *website* palsu yang menyerupai *website* asli untuk memperdayai korbannya agar memperoleh informasi rahasia berupa nama, kata sandi, nomor rekening bank, nomor jaminan sosial, atau nomor kartu kredit. Informasi rahasia yang berhasil didapatkan oleh pelaku ini yang kemudian dimanfaatkan untuk mengakses akun pribadi yang dampaknya sangat merugikan korban yaitu pencurian identitas dan kerugian finansial.[23]

Phishing merupakan perilaku dalam menjebak seseorang untuk memberikan informasi rahasia yang dilakukan melalui pesan penting

---

[21] Adami Chazawi, *Pelajaran Hukum Pidana Bagian* 1, Cet. VII, Rajawali Pers, Jakarta, 2013, h. 112.

[22] Ki Jagad Tomara, *Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs Phishing*, Skripsi, Fakultas Hukum Universitas Brawijaya, 2011, h. 84.

[23] Routhu Srinivasa Rao and Syed Taqi Ali, *A Computer Vision Technique to Detect Phishing Attacks, 2015 5th International Conference on Communication Systems and Network Technologies*, CSNT, Jakarta, 2015, h. 596.

bohongan berupa *website, e-mail*, atau komunikasi elektronik lainnya. "Pesan bohongan yang terlihat seperti orisinal yang memaksudkan target untuk memberikan data penting yang dilakukan secara cepat dan terkadang dalam pesan tersebut menyertakan suatu ancaman apabila tidak memberikan informasi tersebut, maka akan berakibat buruk".[24]

Dalam penelitian yang dilakukan oleh Mia Haryawati Wibowo, bentuk-bentuk *cyber phising* terbagi menjadi 3 (tiga), yaitu:[25]

1. *E-mail Phishing*, yakni pelaku akan bertindak sebagai orang yang bekerja di suatu organisasi yang berhubungan dengan korban lalu mengirimkan *e-mail* palsu yang memaksudkan target untuk memperbarui informasi pribadi melalui tautan URL yang telah disematkan pada *e-mail* tersebut;
2. *Website Phishing*, yakni seseorang menciptakan sebuah situs *web* tiruan yang menyerupai dengan situs *web* yang orisinal dari suatu perusahaan atau organisasi yang tujuannya akan memperdayai target agar memasukkan data pribadi seperti kata sandi dan nomor rekening bank; dan
3. *Malware Phishing*, yakni *malware* yang merupakan sebuah program komputer yang dibentuk agar mengganggu suatu sistem pada komputer tanpa diketahui pengguna komputer tersebut. Metodenya berupa mengirimkan suatu file tertentu kepada target agar terkena virus yang dapat merusak sistem komputer apabila mengunduh file tersebut yang mengakibatkan pelaku bisa mengakses sistem komputer sang target sesuai keinginannya.

Sedangkan penelitian yang dilakukan oleh Dian Rachmawati, bentuk-bentuk *cyber phising* terbagi menjadi menjadi 6 (enam), yaitu:[26]

1. *E-mail Spoofing* yaitu di mana pelaku akan mengirimkan *e-mail* ke beberapa pengguna dengan mengatasnamakan dari suatu lembaga resmi. *E-mail* ini meminta nomor kredit, kata sandi atau mengarahkan untuk mengunduh *form* tertentu;

---

[24] Otoritas Jasa Keuangan, *Bijak Ber-eBANKING*, OJK, Jakarta, 2015, h. 47.

[25] Mia Haryawati Wibowo, *Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime*, Jurnal STKIP PGRI Tulungagung, Vol. 1, No. 1, Tulungagung, 2017, h. 3.

[26] Dian Rachmawati, *Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber,* Jurnal Universitas Sumatera Utara, Vol.13, No.3, Medan, 2014, h. 212.

2. Pengiriman Berbasis *Web* yaitu pelaku akan mengirimkan *web* palsu kepada korbannya;
3. Pesan Instan yaitu korban menerima sebuah pesan yang berisi *link* yang terarahkan ke situs *web* palsu yang menyerupai dengan situs *web* orisinalnya;
4. *Trojan Hosts* yaitu di mana hacker melakukan *login* ke akun salah satu pengguna untuk mengumpulkan surat rahasia atau surat penting yang akan dikirimkan ke pelaku *phishing*;
5. Manipulasi tautan yaitu di mana pelaku mengirimkan tautan ke sebuah *web* dan apabila korban menekan tautan tersebut, maka akan terbukalah *web* palsu; dan
6. *Malware Phishing* adalah penipuan *phishing* yang melibatkan *malware* yang akan dipergunakan dalam komputer korbannya. *Malware* ini melekat pada *e-mail* targetnya dan setelah korban menekan link tersebut, maka secara bersamaan *malware* akan berfungsi.

Adapun mengenai cara kerja *cyber phishing* biasanya dilakukan dengan cara sebagai berikut, yaitu:[27]

1) Mengirimkan pesan melalui sms atau surat masa singkat, *e-mail* atau surat elektronik, *web*, atau media komunikasi elektronik lainnya kepada sasarannya;
2) Meminta untuk diberikan data pribadi yang bersifat rahasia, seperti nama, kata sandi, nomor kartu kredit, dan lainnya; dan
3) Memberikan batasan dengan durasi yang singkat. Pelaku memfokuskan korban untuk berbuat tanpa berpikir panjang, sehingga terciptalah suasana yang tegang dan memberitahukan adanya akibat buruk jika tidak ditindaklanjuti.

Phishing merupakan kegiatan seseorang dalam memperoleh data yang bersifat rahasia melalui *e-mail* dan situs palsu yang tampilannya mirip dengan situs resminya. “Informasi yang diperoleh oleh pelaku berupa kata sandi suatu akun atau nomor kartu kredit korban. Pelaku memakai *e-mail* untuk memperdayai korbannya ke situs tiruan (*fake webpage*), di mana target diminta mengenai data kerahasiannya. Berkat kelalaian atau kelengahan korban, maka informasi pribadi tersebut bisa didapatkan oleh

[27] Otoritas Jasa Keuangan, *Op.Cit*., h. 48.

pelaku".[28] Pengguna *online banking* merupakan salah satu sasaran oleh pelaku, sebab memakai Isian Data (ID) pengguna dan kata sandi serta tidak menutup peluang hal ini bisa terjadi pada pengguna lainnya. "Proses yang dilakukan oleh pelaku adalah memberikan *fake form login* yang meminta data berupa nama, kata sandi serta hal yang bersifat pribadi kepada korban dan apabila sudah terisi, maka pelaku berhasil memperoleh data tersebut".[29]

Sedangkan mengenai *spear phishing* adalah bentuk serangan *phishing* yang lebih spesifik dan ditargetkan. Berbeda dengan *phishing* yang bersifat massal, *spear phishing* dirancang untuk menyerang individu atau organisasi tertentu. Penyerang melakukan riset mendalam tentang korban untuk membuat pesan yang tampak lebih personal dan meyakinkan.

Adapun mengenai ciri-ciri *cyber spear phishing* yaitu:[30]

1. Pesan yang Dipersonalisasi: Menggunakan informasi spesifik tentang korban, seperti nama, jabatan, atau organisasi;
2. Berpura-Pura Menjadi Orang yang Dikenal: Penyerang sering menyamar sebagai kolega, atasan, atau mitra bisnis;
3. Target Terbatas: Biasanya menyerang individu yang memiliki akses ke informasi penting atau sistem sensitif.

Sedangkan mengenai cara kerja *cyber spear phishing* yaitu:[31]

1. Riset Korban: Penyerang mengumpulkan informasi tentang korban dari media sosial, situs web perusahaan, atau sumber lain;
2. Pembuatan Pesan yang Dipersonalisasi: Berdasarkan informasi tersebut, penyerang membuat pesan yang tampak sangat kredibel;

---

[28] Dian Rachmawati, *Op.Cit.*, h. 211.

[29] Ardi Saputra Gulo, et al., *Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik,* Jurnal Universitas Jambi, Vol.1, No.2, Jambi, 2020, h. 71.

[30] Widya Scurity, *Spear Phishing vs Phishing: Ungkap Perbedaan dan Cara Kerjanya*, diakses melalui: https://widyasecurity.com/2024/12/27/spear-phishing-vs-phishing-ungkap-perbedaan-cara-kerjanya/, diakses pada tanggal 25 Mei 2025.

[31] *Ibid.*

3. Komunikasi Langsung: Penyerang sering kali menggunakan alamat email yang mirip dengan orang atau organisasi yang dikenal korban;
4. Manipulasi Psikologis: Pesan dirancang untuk memanfaatkan kepercayaan atau rasa urgensi korban;
5. Eksekusi: Korban terjebak dan memberikan informasi atau melakukan tindakan yang diinginkan penyerang.

Cyber spear phishing adalah pelaku kejahatan siber yang menggunakan teknik *phishing* yang sangat terarah dan personal untuk menipu korbannya. Berbeda dengan phishing biasa yang menyasar banyak orang secara acak, spear phishing menargetkan individu atau organisasi tertentu dengan memanfaatkan informasi pribadi korban agar pesan yang dikirim terlihat meyakinkan dan autentik. Pelaku biasanya menyamar sebagai orang yang dikenal atau institusi resmi, kemudian mengirimkan pesan yang berisi permintaan data sensitif, akses akun, atau transfer uang. Karena tingkat personalisasi dan kecanggihan penyamaran tersebut, *spear phishing* sering berhasil mengecoh korban dan menyebabkan kerugian besar baik secara finansial maupun reputasi.

1.5.1.5. Pengertian Pencurian Data Pribadi

Data Pribadi menurut Pasal 1 angka 1 Rancangan Undang-Undang Perlindungan Data Pribadi dijelaskan bahwa Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Data pribadi adalah informasi tentang seseorang yang bersifat penting dan privasi. Data pribadi berisi berbagai macam data penting yang seharusnya dirahasiakan dan dijaga penggunaannya.

Data pribadi menurut Rancangan Undang-Undang Perlindungan Data Pribadi terbagi menjadi 2 (dua) yaitu data pribadi bersifat umum dan data pribadi bersifat spesifik. Data pribadi umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, dan atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Data pribadi spesifik meliputi, data dan informasi kesehatan , data biometrik, data genetika, kehidupan/orientasi kehidupan.

Data pribadi umum berisi tentang informasi yang secara umum melekat pada diri seseorang yang keberadaannya sangat mudah untuk diberitahu. Contohnya pada saat kita menuliskan biodata diri kita, ini merupakan hal sepele tapi yang harus kita perhatikan dikarenakan barangkali bisa disalahgunakan. Dan data pribadi spresifik memiliki arti informasi tentang diri kita secara lebih mendalam meliputi data-data yang sangat privasi, contohnya seperti data informasi kesehatan kita yang diketahui oleh seorang dokter rumah sakit. Data ini sangat dijaga kerahasiaannya.

Pencurian data pribadi adalah mentransfer atau mengirimkan data pribadi orang lain dan menggunakannya tanpa ada nya suatu hak yang dimiliki oleh orang tersebut. Pencurian data pribadi adalah pengambilan tanpa hak oleh seseorang terhadap data pribadi seseorang yang seharusnya menjadi privasi dengan dirawat, di simpan, dan dijaga kerahasiaannya.

Mengenai subjek dari pencurian data pribadi tidak lepas dari subjek ilmu hukum itu sendiri. Dalam dunia hukum, perkataan orang berarti

pembawa hak yaitu sesuatu yang mempunyai hak dan kewajiban dan disebut sebagai subjek hukum. “Subjek hukum terdiri dari: 1) Manusia; dan 2) Badan Hukum”.[32]

1.5.2. Landasan Yuridis

Landasan yuridis merupakan dasar hukum yang mengatur dan berhubungan dengan objek penelitian. Landasan yuridis dalam penelitian ini berkaitan dengan tindak pidana *phising*. *Phishing* sendiri merupakan salah satu bentuk kejahatan siber (*cyber crime*) yang dilakukan dengan cara menipu korban untuk memperoleh informasi pribadi, seperti kata sandi, data kartu kredit, atau informasi sensitif lainnya. Dalam konteks hukum di Indonesia, tindak pidana *phishing* diatur dalam beberapa peraturan perundang-undangan.

1.5.2.1. *Cyber Crime* Dalam Kitab Undang-Undang Hukum Pidana

Tindak pidana *phishing* juga dapat dikaitkan dengan delik penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana, yang menyebutkan bahwa setiap orang yang dengan tipu muslihat atau kebohongan untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dapat dijatuhi hukuman penjara hingga 4 tahun.

1.5.2.2. *Cyber Crime* Dalam Undang-Undang Perlindungan Konsumen

Dalam kasus *phishing* yang melibatkan konsumen, sebagaiman penjelasan Pasal 4 huruf c Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang berbunyi “*Hak atas informasi yang benar,*

[32] C.S.T Kansil dan Christine S.T. Kansil., *Pengantar Ilmu Hukum Indonesia,* Rineka Cipta, Jakarta, 2011, h. 72.

jelas, dan jujur mengenai konsidi dan jaminan barang dan/atau jasa". Tindakan *phishing* melanggar hak ini karena memberikan informasi palsu atau menipu konsumen. *Phishing* yang mengakibatkan kerugian finansial bagi konsumen dapat dianggap sebagai pelanggaran terhadap hak-hak konsumen untuk mendapatkan keamanan dan kenyamanan. Penyedia layanan internet dan platform digital juga memiliki tanggung jawab untuk memastikan bahwa layanan mereka tidak digunakan untuk *phishing*, sebagaimana diatur dalam Pasal 3 ayat (1) dan ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana penjelasan dalam Pasal 3 ayat (1) yang berbunyi "*Penyelenggaraan Sistem Elektronik wajib dilakukan secara andal, aman, terpercaya, dan bertanggung jawab untuk memastikan keberlangsungan operasional Sistem Elektronik*". Dan Pasal 3 ayat (2) yang berbunyi "*Penyelenggaraan Sistem Elektronik harus menjamin kerahasiaan, keutuhan, dan ketersediaan Informasi Elektronik dan/atau Dokumen Elektronik yang dikelolanya*". *Phishing* melibatkan penyalahgunaan sistem elektronik untuk mencuri informasi pribadi atau dokumen elektronik secara tidak sah. Sehingga penyelenggara yang gagal mencegah praktik ini dapat dianggap melanggar kewajiban keamanan data.

1.5.2.3. *Cyber Crime* Dalam Undang-Undang ITE

Phishing dikategorikan sebagai tindak pidana yang melanggar Pasal 30 dan Pasal 32 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang

Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, yang merupakan Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008. Dalam Pasal 30 ayat (1) berbunyi "*Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik milik orang lain*". Dan ayat (3) berbunyi "*Jika akses tersebut dilakukan dengan tujuan mendapatkan informasi elektronik atau dokumen elektronik milik orang lain, maka dapat dijerat dengan ancaman pidana*". Sedangkan dalam Pasal 32 ayat (1) berbunyi "*Melarang perbuatan dengan sengaja dan tanpa hak atau melawan hukum memindahkan, mentransfer, atau mengakses data elektronik milik orang lain. Pelanggaran Pasal ini diancam pidana penjara hingga 8 (delapan) tahun dan/atau denda hingga Rp.800.000.000,- (delapan ratus juta rupiah)*".

1.5.3. Landasan Teori

Landasan teori merupakan teori-teori yang digunakan oleh penulis sebagai dasar atau pedoman berpikir dalam penelitian. Adapun landasan teori dalam penelitian ini yaitu : a) Teori Perlindungan Hukum; dan b) Teori Pertanggungjawaban Hukum.

1.5.3.1. Teori Perlindungan Hukum

Teori perlindungan hukum merupakan konsep dalam ilmu hukum yang menjelaskan bagaimana hukum memberikan jaminan terhadap hak-hak individu agar terlindungi dari tindakan sewenang-wenang, baik oleh sesama warga negara maupun oleh penguasa. Teori ini menekankan pentingnya adanya peraturan perundang-undangan yang adil, aparat penegak hukum

yang profesional, serta mekanisme peradilan yang independen untuk menjamin kepastian dan keadilan hukum. Perlindungan hukum dapat bersifat preventif, yaitu upaya pencegahan sebelum terjadi pelanggaran hak, dan represif, yaitu upaya penegakan dan pemulihan hak setelah terjadi pelanggaran. Tujuan akhir dari teori perlindungan hukum adalah terciptanya rasa aman, keadilan, dan penghormatan terhadap hak asasi manusia dalam kehidupan bermasyarakat dan bernegara.

> Menurut Fitzgerald sebagaimana dikutip Satjipto Raharjo awal mula dari munculnya teori perlindungan hukum ini bersumber dari teori hukum alam atau aliran hukum alam. Aliran ini dipelopori oleh Plato, Aristoteles (murid Plato), dan Zeno (pendiri aliran Stoic). Menurut aliran hukum alam menyebutkan bahwa hukum itu bersumber dari Tuhan yang bersifat universal dan abadi, serta antara hukum dan moral tidak boleh dipisahkan. Para penganut aliran ini memandang bahwa hukum dan moral adalah cerminan dan aturan secara internal dan eksternal dari kehidupan manusia yang diwujudkan melalui hukum dan moral.[33]

> Fitzgerald menjelaskan teori pelindungan hukum Salmond bahwa hukum bertujuan mengintegrasikan dan mengkoordinasikan berbagai kepentingan dalam masyarakat karena dalam suatu lalu lintas kepentingan, perlindungan terhadap kepentingan tertentu hanya dapat dilakukan dengan cara membatasi berbagai kepentingan di lain pihak. Kepentingan hukum adalah mengurusi hak dan kepentingan manusia, sehingga hukum memiliki otoritas tertinggi untuk menentukan kepentingan manusia yang perlu diatur dan dilindungi. Perlindungan hukum harus melihat tahapan yakni perlindungan hukum lahir dari suatu ketentuan hukum dan segala peraturan hukum yang diberikan oleh masyarakat yang pada dasarnya merupakan kesepakatan masyarakat tersebut untuk mengatur hubungan prilaku antara anggota-anggota masyarakat dan antara perseorangan dengan pemerintah yang dianggap mewakili kepentingan masyarakat.[34]

Dalam Kamus Besar Bahasa Indonesia (KBBI) Perlindungan berasal dari kata lindung yang memiliki arti mengayomi, mencegah,

---

[33] Satjipto Raharjo,*Ilmu Hukum*, PT Citra Aditya Bakti, Bandung, 2000, h. 53.
[34] Ibid, h. 54.

mempertahankan, dan membentengi. Sedangkan Perlindungan berarti konservasi, pemeliharaan, penjagaan, asilun, dan bunker. Secara umum, perlindungan berarti mengayomi sesuatu dari hal-hal yang berbahaya, sesuatu itu bisa saja berupa kepentingan maupun benda atau barang. Selain itu perlindungan juga mengandung makna pengayoman yang diberikan oleh seseorang terhadap orang yang lebih lemah. Dengan demikian, perlindungan hukum dapat diartikan Perlidungan oleh hukum atau perlindungan dengan menggunakan pranata dan sarana hukum.

Adapun pendapat yang dikutip dari beberapa ahli mengenai perlindungan hukum sebagai berikut, yaitu:[35]

1. Menurut Satjito Rahardjo perlindungan hukum adalah adanya upaya melindungi kepentingan seseorang dengan cara mengalokasikan suatu Hak Asasi Manusia kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya tersebut;
2. Menurut Setiono perlindungan hukum adalah tindakan atau upaya untuk Melindungi masyarakat dari perbuatan sewenang-wenang oleh penguasa yang tidak sesuai dengan aturan hukum, untuk mewujudkan ketertiban dan ketentraman sehingga memungkinkan manusia untuk menikmat martabatnya sebagai manusia;
3. Menurut Muchsin perlindungan hukum adalah kegiatan untuk melindungi individu dengan menyerasikan hubungan nilai-nilai atau kaidah-kaidah yang menjelma dalam sikap dan tindakan dalam menciptakan adanya ketertiban dalam pergaulan hidup antara sesama manusia; dan
4. Menurut Philipus M. Hadjon Selalu berkaitan dengan kekuasaan. Ada dua kekuasaan pemerintah dan kekuasaan ekonomi. Dalam hubungan dengan kekuasaan pemerintah, masalah perlindungan hukum bagi rakyat (yang diperintah), terhadap pemerintah (yang memerintah). Dalam hubungan dengan kekuasaan ekonomi, permasalahan perlindungan hukum adalah perlindungan bagi si lemah (ekonomi) terhadap si kuat (ekonomi), misalnya perlindungan bagi pekerja terhadap pengusaha.

[35] Asri Wijayanti, *Strategi Penulisan Hukum*, Lubuk Agung, Bandung, 2011, h. 10.

Pada dasarnya perlindungan hukum tidak membedakan terhadap kaum pria maupun wanita. Indonesia sebagai negara hukum berdasarkan pancasila haruslah memberikan perlindungan hukum terhadap warga masyarakatnya karena itu perlindungan hukum tersebut akan melahirkan pengakuan dan perlindungan hak asasi manusia dalam wujudnya sebagai makhluk individu dan makhluk sosial dalam wadah negara kesatuan yang menjunjung tinggi semangat kekeluargaan demi mencapai kesejahteraan bersama.

1.5.3.2. Teori Pertanggungjawaban Hukum

Dalam hukum pidana konsep *liability* atau "pertanggungjawaban" itu merupakan konsep sentral yang dikenal dengan ajaran kesalahan. Dalam bahasa Latin ajaran kesalahan ini dikenal dengan sebutan *mens rea.* Suatu perbuatan tidak mengakibatkan seseorang bersalah kecuali jika pikiran orang itu jahat. Doktrin *mens rea* dilandaskan pada *maxim actus non facit reum nisi mens sit rea,* yang berarti "suatu perbutan tidak mengakibatkan seseorang bersalah kecuali jika pikiran orang itu jahat".

Menurut padangan tradisional, disamping syarat-syarat objektif melakukan perbuatan pidana, harus dipenuhi pula syarat-syarat subjektif atau syarat-syarat mental untuk dapat dipertanggungjawabakan dijatuhkan pidana kepadanya. Syarat subjektif ini disebut "kesalahan".

Menurut sistem hukum Kontinental, syarat-syarat subjektif ini dibagii dua, yaitu bentuk kesalahan (Kesengajaan dan Kealpaan) dan mampu bertanggung jawab. "Dalam sistem hukum *common law* syarat-syarat ini disatukan dalam *mens rea*. Dengan demikian, maka yang dimaksud dengan

pertanggungjawaban pidana adalah penilaian apakah tersangka atau terdakwa dapat dipertanggungjawabkan atas suatu tindak pidana yang terjadi".[36]

Kesalahan, Pertanggungjawaban dan Pidana adalah ungkapan-ungkapan yang terdengar dan digunakan dalam percakapan sehari-hari, dalam moral, agama, dan hukum. Tiga unsur ini berkaitan satu dengan yang lain, dan berakar dalam satu keadaan yang sama yaitu adanya pelanggaran terhadap suatu sistem aturan-aturan. Sistem aturan-aturan ini dapat bersifat luas dan aneka macam (hukum perdata, hukum pidana, aturan moral dan sebagainya). "Kesamaan dari ketiga tiganya adalah bahwa mereka meliputi suatu rangkaian aturan tentang tingkah laku yang diikuti oleh suatu kelompok tertentu. Jadi sistem yang melahirkan konsepsi kesalahan, pertanggungjawab dan pemidanaan itu adalah sistem normatif".[37]

Menurut Pompe kemampuan bertanggungjawab pidana harus mempunyai unsur-unsur sebagai berikut :[38]

1. Kemampuan berfikir (*psychisch*) pembuat (*dader*) yang memungkinkan ia menguasai pikirannya, yang memungkinkan ia menentukan perbuatannya;
2. Oleh sebab itu, ia dapat menentukan akibat perbuatannya; dan
3. Sehingga ia dapat menentukan kehendaknya sesuai pendapatnya.

1.6. Penelitian Terdahulu

Dalam penelitian yang dilakukan penulis, terdapat beberapa penelitian yang terdahulu sebagai bahan rujukan dan masukan dalam penelitian ini yaitu:

---

[36] SR. Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*, Alumi, Jakarta, 1982, h. 250.

[37] *Ibid*, h. 33.

[38] Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana Indonesia*, PT Erseko, Bandung, 1986, h. 55.

1. Lutfiyatul Hanifah. Skripsi Fakultas Hukum Universitas Islam Sultan Agung Semarang 2023. Dengan judul Pengaturan Tindak Pidana *Cyber Crime* Dalam Bentuk *Cyber Phising* Menurut Hukum Pidana Indonesia. Bahwa dalam penelitian ini lebih memfokuskan kepada perlindungan kepada korban berupa pemberian Restitusi atau ganti kerugian bagi korban tindak pidana oleh pelaku/pihak ketiga dengan memperhatikan syarat agar permohonan dapat diterima ataupun ditolak. Sedangkan perbedaan dalam penelitian yang akan dikaji oleh penulis lebih berfokus terhadap pertanggungjawaban secara hukum positif di Indonesia.
2. Hasna Kholivia. Skripsi Fakultas Hukum Universitas Islam Sultan Agung (Unissula) Semarang 2021. Dengan judul Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Dalam Kasus Tindak Pidana Mayantara (*Cyber Crime*). Hasil dari penelitian ini ini membahas tentang tindak pidana mayantara yang mana fokus kajiannya dititik beratkan dalam RUU KUHP 2019 mengatur pula mengenai tindak pidana pencurian data pribadi dalam kasus tindak pidana mayantara diatur dalam hukum pidana yang akan datang. Sedangkan perbedaan dalam penelitian penulis nantinya akan diulas secara menyeluruh baik dari Undang-Undang Hukum Pidana dan juga Undang-Undang Informasi Elektronik

Adapun perbedaan penelitian ini dengan penelitian sebelumnya bahwa dalam penelitian sebelumnya mengkaji mengenai tindak pidana *cyber crime* secara umum, namun dalam penelitian yang dilakukan oleh penulis lebih memfokuskan mengeni *cyber sper phising*. Oleh karena itu penelitian ini lebih

memfokuskan pada pertanggungjawaban tindak pidana *cyber spear phising* dalam perspektif pencurian data pribadi.

Sedanggkan persamaan antara penelitian ini dengan penelitian terdahulu yakni sama-sama meneliti tentang *cyber crime* serta kejahatan terkait *phising*. Serta sama-sama menelatah permasalahan tersebut dengan menggunakan hukum positif di Indonesia.

1.7. Metode Penelitian

Metode penelitian ini merupakan cara yang digunakan untuk mendapatkan data serta memperoleh jawaban yang akurat atas rumusan masalah diatas dengan mencari dan mengelola data dalam suatu penelitian.

1.7.1. Jenis Penelitian

Jenis penelitian ini adalah penelitian hukum normatif, penelitian hukum untuk menemukan aturan hukum, prinsip-prinsip hukum maupun doktrin-doktrin hukum. "Penelitian hukum normatif adalah proses penelitian untuk meneliti dan mengkaji tentang hukum sebagai norma, aturan, asas hukum, prinsip hukum, doktrin hukum, teori hukum dan kepustakaan lainnya untuk menjawab permasalahan hukum yang diteliti".[39]

Hasil dari penelitian ini memberikan diskripsi mengenai rumusan masalah yang diajukan, penelitian normatif hanya meneliti norma hukum, tanpa melihat praktek hukum di lapangan (*law in action*) mengenai penelitian terkait pertanggungjawaban tindak pidana *cyber spear phising* dalam perspektif pencurian data pribadi.

---

[39] Suyanto, *Penelitian Hukum Pengantar Penelitian Normatif Empiris dan Gabungan*, Cetakan Pertama, Unigres Press, Gresik, 2022, h. 88.

1.7.2. Metode Pendekatan

Metode pendekatan merupakan salah satu tahapan penelitian yang dimaksudkan untuk mengumpulkan bahan-bahan hukum dalam berbagai aspek untuk mencari jawaban atas permasalahan yang telah dirumuskan dalam penelitian ini. Adapaun dalam penelitian ini penulis menggunakan tiga metode pendekatan antara lain pendekatan konseptual (*conceptual approach*), pendekatan perundang-undangan (*statute approach*), dan pendekatan kasus (*case approach*).

a. Pendekatan Konseptual (*Conceptual Approach*).

   Pendekatan konseptual beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum. Dengan mempelajari pandangan-pandangan dan doktrin-doktrin di dalam ilmu hukum, peneliti akan menemukan ide-ide yang melahirkan pengertian-pengertian hukum. Pendekatan konseptual dilakukan guna dijadikan sebagai acuan untuk membangun argumentasi hukum yang berkaitan dengan pokok permasalahan dalam penelitian ini yakni mengenai Pertanggungjawaban Tindak Pidana *Cyber Spear Phising* di Indonesia. Adapun konsep dalam penelitian ini diantaranya : a) Tinjauan Umum Tindak Pidana; b) Tinjauan Umum *Cyber Crime*; c) Pengertian Data Pribadi; dan d) Pencurian Data Pribadi.

b. Pendekatan Perundang-Undangan (*Statute Approach*).

   Pendekatan perundang-undangan dilakukan dengan menelaah semua Undang-Undang dan regulasi yang bersangkut paut dengan isu karena

yang akan diteliti adalah berbagai aturan hukum yang menjadi fokus sekaligus tema sentral suatu penelitian. Dilakukan dengan cara menelaah dan mengkaji semua peraturan perundang-undangan yang berkaitan dengan pokok permasalahan yang dirumuskan dalam penelitian ini. Pendekatan perundang-undangan ini digunakan untuk mendapatkan ketentuan-ketentuan hukum guna untuk mempelajari konsistensi dan kesesuaian antara Undang-Undang yang satu dengan Undang-Undang lainnya. Adapun pendekatan perundang-undangan dalam penelitian ini yakni Undang Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; dan Kitab Undang-Undang Hukum Pidana (KUHP).

c. Pendekatan Kasus (*Case Approach*).

Pendekatan kasus dalam hukum normatif adalah metode pendekatan yang digunakan untuk mengkaji hukum dengan cara menelaah dan menganalisis putusan-putusan pengadilan yang relevan terhadap isu hukum yang sedang dibahas. Melalui pendekatan ini, peneliti dapat memahami bagaimana norma hukum diterapkan dalam praktik, termasuk bagaimana hakim menafsirkan Undang-Undang dalam menyelesaikan suatu perkara. Pendekatan ini penting dalam penelitian hukum normatif karena dapat menunjukkan konsistensi, perkembangan, dan dinamika dalam penerapan hukum, serta menjadi

dasar dalam menyusun argumentasi hukum atau usulan perbaikan terhadap peraturan yang berlaku. Adapun pendekatan kasus yang digunakan dalam penelitian ini yakni Putusan Perkara Nomor 845/PID.SUS/2020/PT SBY.

1.7.3. Sumber Bahan Hukum (*Legal Sources*)

Bahan hukum yang dikumpulkan dalam penulisan untuk menjawab isu hukum penulisan ini yaitu: bahan hukum primer; bahan hukum sekunder; dan bahan hukum tersier.

1. Bahan Hukum Primer

   Bahan Hukum Primer adalah bahan-bahan hukum yang mengikat seperti Norma dan Kaidah Dasar, Peraturan Dasar, Peraturan Perundang-Undangan. Bahan hukum primer yang digunakan adalah :

   a) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
   b) Kitab Undang-Undang Hukum Pidana (KUHP);
   c) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
   d) Undang-Undang Nomor 13 Tahun 2016 tentang Perlindungan Saksi dan Korban;
   e) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

f) Undang-undang (UU) Nomor 1 Tahun 2024 Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

g) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana;

h) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; dan

i) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

2. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan mengenai bahan hukum primer seperti : buku-buku hukum, hasil-hasil penelitian, pendapat pakar hukum. Dalam penelitian ini penulis menggunakan buku, makalah, hasil penelitian dalam bidang hukum, internet yang berkaitan dengan penelitian yang penulis lakukan.

3. Bahan Hukum Tersier

Bahan-bahan yang memberikan informasi tentang bahan hukum primer dan bahan hukum sekunder seperti : Ensiklopedia hukum, kamus bahasa Indonesia, kamus hukum, internet, hal ini dilakukan untuk mendukung dan menunjang penelitian penulis.

1.7.4. Teknik Pengumpulan dan Pengolahan Bahan Hukum

Berisi uraian logis prosedur pengumpulan bahan-bahan hukum primer, skunder, serta bahan hukum tersebut diinventarisasi dan diklarifikasi dengan menyesuaikan masalah yang dibahas. Dalam penelitian hukum normatif, teknik pengumpulan bahan hukum sebagai berikut:

Bahan hukum primer berupa perundang-undangan dikumpulkan dengan metode inventarisasi dan kategorisasi. Bahan hukum sekunder dikumpulkan dengan sistem kartu catatan (*card system*), baik dengan kartu ikhtiar (memuat ringkasan tulisan sesuai aslinya, secara garis besar dan pokok gagasan yang memuat pendapat asli penulis), maupun kartu ulasan (berupa analisis dan catatan khusus penulis).

Dalam penelitian hukum normatif yuridis, teknik pengumpulan bahan hukum sebagai berikut:

1) Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif artinya mempunyai otoritas. Bahan-bahan hukum primer terdiri dari perundang-undangan;
2) Bahan hukum sekunder berupa publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi. Publikasi tentang hukum meliputi buku-buku teks, kamus-kamus hukum, jurnal-jurnal hukum, dan media daring.

1.7.5. Teknik Analisa Bahan Hukum

Analisis bahan hukum dalam penelitian ini berdasarkan data yang ada dilakukan secara yuridis kualitatif, yaitu tidak hanya mengungkapkan

kebenaran belaka tetapi juga memahami kebenaran tersebut menurut aturan perundang-undangan. Dengan memberikan gambaran permasalahan tentang pertanggungjawaban tindak pidana *cyber spear phising* dalam perspektif pencurian data pribadi dianalisis berdasarkan aturan hukum yang berlaku di Indonesia dan fakta di lapangan untuk kemudian diperoleh kesimpulan sebagai jawaban atas permasalahan yang diajukan.

1.8. Sistematika Penulisan

Untuk lebih mengetahui dan mempermudah dalam melakukan pembahasan, penganalisaan, dan penjabaran isi dari penelitian ini, maka dalam penulisan skripsi ini penulis menyusun sistematika penulisan sebagai berikut :

Bab I menerangkan Pendahuluan yang berisikan tentang Latar Belakang Permasalahan, Rumusan Masalah, Kajian Pustaka, Tujuan Penelitian, Manfaat Penelitian, Orisinalitas Penelitian, Kajian Pustaka yang terdiri dari Landasan Teori dan Penjelasan Konsep, Metode Penelitian terdiri atas Jenis Penelitian, Pendekatan Masalah, Sumber Bahan Hukum, Teknik Pengumpulan dan Pengolahan Bahan Hukum, Analisis Bahan Hukum, dan diakhiri dengan Pertanggung Jawaban Sistematika.

Bab II membahas tentang Pengaturan Hukum Terkait Tindak Pidana *Cyber Spear Phising* Dalam Perspektif Pencurian Data Pribadi. Dengn sub bab diantaranya: Tindak Pidana *Cyber Spear Phising* di Indonesia; dan Pengaturan Hukum Terkait Tindak Pidana *Cyber Spear Phising* Dalam Perspektif Pencurian Data Pribadi.

Bab III membahas tentang Pertanggungjawaban Hukum Terhadap Pelaku Tindak Pidana *Cyber Spear Phising* Menurut Peraturan Perundang-Undangan. Dengan sub bab diantaranya: Bentuk Pertanggungjawaban Hukum Terhadap Pelaku Tindak Pidana *Cyber Spear Phising* Menurut Peraturan Perundang-Undangan; dan Perlindungan Hukum Terhadap Korban Tindak Pidana *Cyber Spear Phising*.

Bab IV sebagai penutup, memuat beberapa kesimpulan dari jawaban permasalahan-permasalahan yang dibahas, serta sebagai saran bagi pihak yang berkaitan dalam penulisan skripsi ini.