BAB I

PENDAHULUAN

1.1. Latar Belakang

Saat ini teknologi informasi maupun komunikasi merupakan sesuatu yang melekat dengan kehidupan manusia sehari-hari untuk menunjang aktivitas mereka. Teknologi informasi dan komunikasi sendiri memudahkan manusia dalam melakukan aktivitas menjadi semakin mudah dan efisien. Tidak dapat dipungkiri juga bahwa manusia serta teknologi saat ini adalah satu kesatuan yang tak bisa dipisahkan dari kehidupan masyarakat.

Beriringan dengan tingginya aktivitas manusia saat ini yang menggunakan teknologi informasi komunikasi, ternyata juga melahirkan beberapa tindak pidana kejahatan dalam dunia teknologi informasi dan komunikasi. Masih terbatasnya pengetahuan masyarakat tentang pemahaman teknologi informasi dan komunikasi saat ini meyebabkan lahirnya niat jahat dari orang – orang yang ingin mencari keuntungan dari ketidaktahuan orang lain. Tindak pidana dalam dunia teknologi informasi dan komunikasi sendiri biasa disebut dengan tindak pidana siber. Serangan siber di Indonesia pada Tahun 2020 berdasarkan laporan data anomali trafik BSSN 2021 ialah sebanyak 495,3 juta, di mana mengalami peningkatan sebesar 41% (empat puluh satu persen) yang pada tahun 2019 hanya sebesar 290,3 juta.[1]

[1] https://berkas.dpr.go.id/puskajianggaran/analisis-apbn/public-file/analisis-apbn-public-65.pdf, diakses pada 5 Juli 2022, pukul. 21.54.

Tindak pidana siber sendiri merupakan tindakan ilegal dalam menggunakan peralatan yang berkaitan dengan internet dan tindakan dapat menyebabkan rugi secara materiil maupun immateriil bagi siapa saja yang menjadi korban. Adapun berbagai macam istilah dala tindak pidana siber yaitu *Spamming*, *Phising*, *Hacking* dan *Carding*. Salat satu tindakan yang akhir-akhir meresahkan adalah tindak pidana siber *phising*.

Seperti hal nya tindak pidana siber *phising* yang dilakukan oleh Miqdad, S. Kom bin Abdul Azis sebagaimana Putusan No. 155/Pid.Sus/2018/PN.Cbn. yang tertuang bahwa terdakwa secara sengaja tanpa hak memanipulasi, menciptakan, merubah informasi dan dokumen elektronik untuk tujuan agar dianggap seakan-akan data otentik untuk mendapatkan nomor kartu kredit milik korbannya. Adapun cara dari terdakwa mendapatkannya tersebut adalah dengan mengirimkan pesan masal ke *Email List* yang di dapatkan melalui *SQL DUMPER* yang berisi notifikasi bahwa akun terkunci yang mana pada kenyataannya akun tidak terkunci dan dalam pesan tersebut disisipkan alamat web palsu yang telah dibuat untuk mendapat identitas detail kartu kredit korbannya.[2]

Kasus tindak pidana siber *phising* juga dilakukan oleh Riswanda N. S., yang berasal dari Kalimantan Selatan. Pelaku ditangkap pihak Direktorat Tindak Pidana Siber Bareskrim Polri yang melakukan kerjasama dengan pihak FBI dan Interpol pada 2021 lalu. Riswanda Noor Saputra sendiri telah

[2]https://putusan3.mahkamahagung.go.id/direktori/putusan/4bef366d5012e99dd2d55caa2c62f42a.html, diakses pada 15 Maret 2022, pukul. 15.33

ditetapkan terbukti melakukan tindakan *phising* sebagai pembuat alat untuk meretas guna data pribadi pemilik akun dapat di ambil, mulia data kartu kredit, email, sandi, kartu identitas, nomor telepon dan data lain yang menyebabkan kerugiaan bagi orang lain.[3]

Berdasarkan rangkuman perbandingan kasus diatas yang jadi urgensi penulis menangkat judul **"PENENTUAN *TEMPUS DELICTIE* PENCURIAN DATA DALAM TINDAK PIDANA SIBER (*PHISING*) MENURUT UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK"**

1.2. Rumusan Masalah

1. Bagaimana menentukan *tempus delictie* pencurian data dalam tindak pidana siber *phising*?
2. Bagaimana terjadinya pencurian data dalam tindak pidana siber *phising*?

1.3. Tujuan Penelitian

1. Mengetahui bagaimana menentukan *tempus delictie* pencurian data dalam tindakan siber *phising*.
2. Mengetahui bagaimana terjadinya pencurian data dalam tindak pidana siber *phising*.

[3] https://m.cyberthreat.id/read/13600/Polisi-FBI-dan-Interpol-Tangkap-Riswanda-Hacker-Indonesia-yang-Bikin-Alat-Peretas-16Shop, diakses pada 15 Maret 2022, pukul. 16.00.

1.4. Manfaat Penelitian

1. Sisi Teoritis
    a. Guna menggali secara dalam sekaligus mempraktekkan teori yang diperoleh penulis selama studi di Fakultas Hukum Universitas Pembagunan Nasional "Veteran" Jawa Timur.
    b. Guna sebagai wawasan dan pengetahuan terkait menentukan *tempus delictei* pencurian data dalam tindakan siber (*phising*) sebagaimana Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.
2. Sisi Praktis
    a. Sebagai referensi pembaca terkait menentukan *tempus delictie* pencurian data dalam tindakan siber (*phising*).
    b. Sebagai pemberi informasi sekaligus pemahaman tentang menentukan *tempus delictie* pencurian data pada tindakan siber (*phising*).

1.5. Kajian Pustaka

1.5.1. Tinjauan Umum *Tempus Delictie*

Tempus delictei merupakan waktu tindakan pidana terjadi. *Tempus delicti*e berkaitan dengan tempat tindak pidana teradi atau *locus delictie.* Maksudnya ialah tempat sekaligus waktu pada unsur tindak pidana telah sempurna, maka disitulah tindak pidana terjadi. Segala uraian yang kemudian diikuti terkait ilmu tempat tindak pidana terjadi,

maka waktu terjadinya tindak pidana dapat ditentukan sebagaimana teori *locus delicti*.[4]

Pentingnya mengetahui *tempus delictie* ialah guna menentukan:

a. Tindakan pada saat itu masuk dalam kategori dilarang sekaligus diancam pidana sebagaimana Pasal 1 ayat 1 Kitab Undang-Undang Hukum Pidana (KUHP) ataukah tidak;

b. Peraturan perundang-undangan apabila berubah, ketentuan yang diterapkan ialah yang baru atau lama sebagaimana Pasal 1 ayat 2 Kitab Undang-Undang Hukum Pidana (KUHP);

c. Apakah terdakwa pada waktu melakukan tindak pidana dapat dipertanggungjawabkan atau tidak (Pasal 44 Kitab Undang-Undang Hukum Pidana (KUHP);

d. Umur Terdakwa saat melakukan tindak pidana ialah telah berusia 12 (dua belas) tahun atukah belum, menyesuaikan dengan ketentuan Undang-Undang Republik Indonesia Nomor 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak;

e. Batas waktu mengajukan aduan, yang dimulai sejak adanya kejahatan sebagaimana Pasal 74 Kitab Undang-Undang Hukum Pidana (KUHP).[5]

---

[4] S.R. Sianturi, *Asas-Asas Hukum Pidana Dan Penerapannya*, Jakarta, Alumni Ahaem-Petehaem, 1986, Hlm. 115

[5] Sofjan Sastrawidjaja, *op.cit*, Hlm. 145

Bahasa latin mengartikan tempat terjadinya pidana ialah *locus delictie*. *Locus* dan *delictum* merupakan rangkaian kata yang terdapat di dalamnya. *Locus* artinya tempat, sedangkan arti *delictum* ialah sebagai tindakan melawan hukum, kejahatan, dan tindakan pidana".[6] Adagium hukum terkait hal tersebut kemudian muncul dengan bunyinya *locus regit actum.* Arti adagium tersebut ialah tempat untuk menentukan hukum yang berlaku atas tindakan tersebut.7

Locus delicti sebagaimana pandangan Van Hattum ialah di mana pelaku telah bertindak kejahatan dan telah memberikan dampak tersendiri. Van Bemmelen dalam pandangannya terkait *locus delicti* ialah tempat pelaku telah bertindak secara material.[8]

Permasalahan terkait tempat dan waktu terjadinya tindakan pidana secara umum ialah penting dan memiliki hubungan dengan ketentuan hukum acara pidana atau secara formil. Ketentuan hukum pidana formil tersebut salah satunya ialah ditemukan pada Pasal 143 Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Hukum Acara Pidana atau Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Pasa tersebut mengatur bahwa penuntut umum dalam surat dakwaanya harus dicantumkan terkait tempat sekaligus waktu

[6] S. Adiwinoto, *Istilah Hukum*, Jakarta, Intermasa, 1977, Hlm. 34
[7] *Ibid*, Hlm. 63
[8] Lamintang, P.A.F, *KUHAP dengan Pembahasan Secara Yuridis Menurut Yurisprodensi dan Ilmu Pengetahuan Hukum Pidana*, Bandung, Sinar Baru, 1984, Hlm. 86

terjadinya tindakan pidana. Hal tersebut apabila tidak dicantumkan, maka surat dakwaan tersebut menjadi batal.[9]

1.5.2. Tinjauan Umum Tindak Pidana

1.5.2.1. Pengertian Tindak Pidana

Tindakan pidana pada Istilah Bahasa Indonesia ialah asalnya dari bahasa Belanda "*strafbar feit*". Pihak yang membentuk undang-undang menggunakan kata "*strafbar feit*" guna menyebut "tindak pidana". Hukum pidana sendiri sejatinya tak menjelaskan maksud dari "*strafbar feit*".[10]

Bahasa Belanda mengartikan "*feit*" sebagai bagian atas kenyataan (*een gedelte van de werkelijkeid*". Arti "*strafbaar*" sendiri ialah "dapat dihukum". Harfiah dari "*strafbar feit*" ialah sebagai bagian dari kenyataan yang dapat di hukum. Suatu yang dapat dihukum ialah manusia sebagai pribadi, bukan kenyataan maupun tindakan.[11]

Strafbar feit menurut Simons ialah dimana seseorang berbuat melanggar hukum secara sengaja. Seseorang tersebut dapat mempertanggungjawabkan tindakannya. Hal tersebut kemudian dinyatakan dapat di hukum".[12]

---

[9] Tongat, *Dasar-dasar Hukum Pidana Indonesia dalam perspektif pembaharuan*, Malang, UMM Pres, 2012, Hlm. 131

[10] Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Bandung, Citra Adit ya Bakri, 1997, Hlm.181

[11] *Ibid.*

[12] Adami Chazawi, *Pelajaran Hukum Pidana Bagian 1*, Cetakan Pertama, Jakarta, Raja Grafindo Persada, 2002. Hlm.72

Menjelaskan hukum positif dengan beberapa pendapat secara teori ialah sangat bahaya. Pendapat Simons terkait *strafbar feit* ialah sifatnya khusus, karena hanya spesifik bahwa tindakan hanya bisa dipertanggungjawabkan apabila melakukannya secara sengaja.[13] Pandangan Simons bertolakbelakang dengan pandangan Pompe, di mana "*strafbar feit*" secara teori merupakan norma yang dilanggar pelaku secara sengaja maupun tidak. Pelaku perlu dijatuhi hukuman agar tertib hukum dapat terpelihara sekaligus kepentingan umum dapat terjamin.[14]

Strafbar feit menurut pandangan Moeljatno ialah tindakan pidana yang dibatasi sebagai tindakan yang dilarang sekaligus diancam secara pidana. Pelanggaran tersebut kemudian harus berdampak terhadap masyarakat sebagai tindakan yang tidak wajar sekaligus menghambat tata pergaulan masyarakat yang di cita-citakan dapat tercapai dengan baik.

1.5.2.2. Jenis Tindak Pidana

Tindakan pidana atau delik menurut doktrin terdiri dari beberapa jenis sebagai berikut:

a. Delik Formil dan Materil

Delik formil ialah terjadi dengan dilakukannya tindakan dilarang sekaligus diancam pidana oleh undang-undang. Delik

[13] Andi Sofyan, Nur Azisa, *Hukum Pidana*, Makassar, Pustaka Pena Press, 2016, Hlm. 98
[14] Lamintang, *Op. Cit.*, Hlm.182

materil sendiri ialah baru dianggap terjadi ketika melahirkan dampak yang dilarang sekaligus diancam pidana oleh undang-undang.

b. Delik Komisi dan Omisi

Delik komisi berupa larangan undang-undang yang dilanggar. Delik omisi sendiri berupa pelanggaran atas kewajiban yang di atur dalam undang-undang.

c. Delik Berdiri Sendiri dan Berlanjut

Delik berdiri sendiri meliputi 1 (satu) tindakan tertentu. Delik berlanjut sendiri meliputi tindakan-tindakan yang masing-masing berdiri sendiri, tetapi antara tindakan tersebut berkaitan erat dan dianggap sebagai tindakan berlanjut.

d. Delik Rampung dan Berlanjut

Delik rampung meliputi 1 (satu) tindakan atau beberapa tindakan tertentu dalam suatu waktu singkat tertentu. Delik berlanjut sendiri meliputi 1 (satu) atau beberapa tindakan yang melanjutkan keadaan yang dilarang undang-undang.

e. Delik Tunggal dan Bersusun

Delik tunggal ialah hanya 1 (satu) kali tindakan telah cukup untuk dijerat pidana. Delik bersusun sendiri ketika dijerat pidana haruslah beberapa kali dilakukan.

f. Delik Sederhana, Pemberatan atau Berkualifikasi, dan Delik Berprevilise

Delik sederhana merupakan dasar atau pokok. Delik dengan pemberatan atau berkualifikasi sendiri memiliki beberapa unsur yang sama dengan delik dasar atau pokok dengan terdapat beberapa unsur lain, sehingga ancaman pidananya lebih berat daripada delik dasar atau pokok. Delik prevellise mengandung beberapa unsur yang sama dengan delik dasar atau pokok dengan terdapat unsur lain, sehingga ancaman pidananya lebih ringan dari delik dasar atau pokok.

g. Delik Sengaja dan Kealpaan

Delik sengaja ialah dilakukan secara sengaja. Delik kealpaan sendiri ialah dilakukan atas kesalahan atau kealpaannya.

h. Delik Politik dan Umum

Delik politik ialah ditujukan dalam hal keamanan negara maupun kepala negara. Delik umum sendiri tak ditujukan terhadap keamanan negara maupun kepala negara.

i. Delik Khusus dan Umum

Delik khusus ialah hanya dapat dilakukan orang tertentu atas suatu kualitas. Delik umum sendiri dapat dilakukan oleh semua orang.

j. Delik Aduan dan Biasa

Delik aduan ialah hanya dapat dilakukan penuntutan ketika diadukan oleh pihak yang mengalami rugi atas tindakan

pelaku tersebut. Delik biasa sendiri tak perlu adanya aduan untuk dapat melakukan penuntutaan.[15]

1.5.2.3. Unsur Tindakan Pidana

Tindakan pidana merupakan tindakan kejahatan dengan melanggar peraturan perundang-undangan. Tindakan pidana sendiri terdapat beberapa unsur di dalamnya sebagai berikut:

a. Tindakan tersebut ialah aktif atau pasif dengan melahirkan dampak yang dilarang secara hukum;
b. Sifat tindakannya ialah melawan hukum secara formil maupun materil;
c. Adanya beberapa hal atau keadaan tertentu yang menyertai terjadinya akibat atas tindakan yang dilarang hukum.[16]

Unsur tindak pidana menurut Simon ialah sebagai berikut:

a. Tindakan manusia, baik yang bersifat negatif maupun positif;
b. Diancam pidana (*statbar gedteld*);
c. Bertentangan dengan hukum (*onrechtmatig*).
d. Tindakan dengan kesalahan (*met schuld in verband stand*).
e. Pelaku mampu bertanggung jawab (*toerekeningsvatoar person*).[17]

---

[15] Sofjan Sastrawidjaja, *Hukum Pidana I*, Bandung, ARMICO, 1990, Hlm. 135

[16] http://kuliahnyata.blogspot.com/2013/10/pengertian-arti-istilah-tindak-pidana.html, diakses tanggal 14 Maret 2022 Pukul. 12.05

[17] http://www.tenagasosial.com/2013/08/unsur-unsur-tindak-pidana.html, diakses tanggal 14 Maret 2022 Pukul. 13.00

1.5.3. Tinjauan Umum Tindak Pidana Siber

1.5.3.1. Pengertian Tindak Pidana Siber

Permasalahan yang muncul sebagai dampak dari perkembangan tekologi informasi salah satunya ialah lahirnya kejahatan bersifat baru dengan menggunakan internet sebagai alat bantu. Kejahatan tersebut disebut sebagai *cybercrime* atau kejahatan dalam dunia maya. Kejahatan tersebut contohnya seperti *hacker*, *cracker*, *cybersquting*, dan sebagainya.[18] Pihak yang menguasai sekaligus mampu mengoperasikan komputer seperti operator, *programer*, analis, *consumer*, *manager*, maupun kasir dapat melakukan tindakan kejahatan siber. Beberapa cara yang dapat dilakukan ialah berkaitan dengan data yang dirusak, dicuri, dan digunakan secara ilegal.[19]

Komputer memiliki definisi sebagaimana Kamus Besar Bahasa Indonesia (KBBI) ialah alat elektronik otomatis sebagai penghitung atau pengolah data dengan cermat menurut instruksi, memberi hasil olahan, serta dapat menjalankan sistem multimedia. Komputer di dalamnya meliputi unit pemasukan, pengeluaran, penyimpanan, serta sebagai pengontrol.[20]

---

[18] Didik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law-Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, Hlm 22

[19] H. Sutarman, 2007, *Cyber Crime-Modus Operandi dan Penanggulangannya*, Yogyakarta Laksbang Pressindo, Hlm 4

[20] http://kbbi.web.id/komputer, diunduh pada tanggal 14 Maret 2022, pukul 13.35

Semakin canggihnya teknologi komputer kemudian dimanfaatkan oleh beberapa oknum tak bertanggung jawab dalam bertindak secara melawan hukum seperti:

a. *Unauthorized Aces to Computer System & Service*

Kejahatan ini dilakukan dengan menyusup ke dalam sistem jaringan komputer secara tidak wajar tanpa sepengetahuan pemilik sistem tersebut.

b. *Infrengment of Privacy*

Kejahatan ini bertujuan mengetahui informasi seseorang yang bersifat rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan formulir data pribadi seseorang yang telah tersimpan secara *computerize*. Hal tersebut apabila diketahui oleh orang lain, tentu akan menimbulkan korban secara materiil atau imateriil.

c. *Ilegal content*

Kejahatan ini dilakukan dengan memasukkan hal tidak wajar mengenai data atau informasi ke internet.

d. *Data Forgey*

Kejahatan ini ialah melakuan pemalsuan data dokumen yang tersimpan pada internet.

e. *Cyber Esponage*

Kejahatan ini ialah dengan memata-matai dalam jaringan internet dengan memasuki sistem jaringan komputer sasaran.

f. *Cyber Sabotage & Extortin*

Kejahatan ini ialah dengan mengganggu, merusak atau menghancurkan data, program atau sistem jaringan komputer yang terhubung internet.

g. *Ofense Against Intelectual Property*

Kejahatan ini berkaitan denga hak kekayaan intelektual milik pihak lain pada internet, seperti meniru tampilan *web page* situs milik pihak lain secara illegal.[21]

Kejahatan komputer atau kejahatan siber secara umum merupakan upaya masuk atau menggunakan komputer tanpa izin dan bertentangan dengan hukum. Hal tersebut kemudian dapat atau tak menyebabkan perubahan maupun kerusakan pada fasilitas komputer tersebut. Pihak yang menggunakan komputer tanpa izin tentu tindakannya tersebut tergolong kejahatan komputer. Aktivitas kejahatan komputer ialah beragam dan sangat besar, hingga telah melahirkan banyak kata baru dalam penyebutannya seperti *hacking*, *cracking*, *virus*, *time boomb*, *woorm*, *trooyan horsee*, *logicall bomb*, *spaming*, *hoax*, dan sebagainya.[22]

1.5.3.2. Bentuk Tindak Pidana Siber

Tindak pidana siber didalamnya terdapat bentuk-bentuk sebagaimana ketentuan Pasal 27 hingga Pasal 35 Undang-Undang

[21] Budi Suhariyanto, 2012 *Tindak Pidana Teknologi Informasi (Cybercrime)-Urgensi Pengaturan dan Celah Hukumnya*, Jakarta, Rajawali Pers, Hlm 15-16

[22] Didik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law-Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, Hlm 8

Republik Indonesia Nomor 11 Tahun 2018 tentag Informasi dan Transaksi elektronik. Bentuknya tersebut ialah sebagai berikut:

1) Kejahatan siber dengan menggunakan komputer sebagai alat kejahatan, seperti pornografi, judi, nama baik yang dicemarkan, penipuan, pemalsuan, pemerasan, pengancaman, penyebaran informasi bohong, melanggar hak cipta, aksi teror, yang kesemuanya dilakukan melalui *online*.
2) Kejahatan siber yang berkaitan dengan computer, di mana jaringan dimanfaatkan sebagai sasaran dengan melakukan akses secara *ilegal.* Sistem dan data komputer dirusak, disadap atau diintersepsi secara tidak sah. Data pada computer tersebut dicuri dan disalahgunakan.

1.5.4. Tinjauan Umum Tindak Pidana *Siber Phising*

Salah 1 (satu) bentuk kejahatan internet ialah *Phising*, yang disebut dengan *identity theft. Phising* ialah mengirim *e-mail* palsu terhadap pihak dengan mengaku bahwa pengirim tersebut merupakan pihak yang sah. Tujuan mengirim *e-mail* palsu tersebut ialah untuk menipu penerima. Penerima *email* ketika mengira bahwa *email* yang diterimanya tersebut bukan merupakan *e-mail* palsu tentu akan terpancing untuk mengunjungi *website* pengirim *e-mail* sekaligus mengungkapkan informasi diri penerima. Informasi tersebut dapat meliputi *pasword,* identitas *credit card*,

bahkan rekening bank. *Website* tersebut ialah dipalsukan dengan sengaja untuk mencuri informasi pribadi korban.[23]

Phishing pada umumnya dilakukan via *email*. *Phising* juga dapat dilakukan melalui pesan singkat. *E-mail* palsu dalam tindakan *phising* memang tampak seperti asli dengan logo sekaigus link *website* yang asli, namun banyak juga ditemukan bahwa pelakunya tidak profesional dengan menampilkan format yang berantakan maupun menampakkan beberapa kesalahan lain pada penulisan kalimatnya.[24]

1.6. Metode Penelitian

1.6.1. Jenis Penelitian

Penelitian yang digunakan penulis dalam penelitian ini ialah jenisnya yuridis normatif. Bahasan penelitian ini ialah terkait doktrin atau asas pada ilmu hukum.[25] Penelitian terhadap asas hukum memiliki tujuan sebagai penentu asas hukum positif. Penelitian jenis ini disebut juga sebagai penelitian doktrinal.[26]

Penulis pada penelitian ini ialah mengedepankan sifat analitis induktif. Dalam prosesnya ialah bertentangan dari norma hukum positif dan berakhir pada penemuan asas hukum Pangkal tolak pencarian asas ialah norma hukum positif. Pendekatan penelitian ini ialah undang-

---

[23] Syahdeini, Sutan Remy. 2009. *Kejahatan & Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafita, Hlm 64.

[24]http://www.bristol.ac.uk/is/computing/advice/security/protectyou/idtheft/phish.html,diakses pada 14 Maret 2022, Pukul 14.05

[25] Zainuddin Ali, *Metode Penelitian Hukum*, Jakarta: Sinar Grafika, 2016, Hlm. 25

[26] Bambang Sunggono, *Metode Penelitian Hukum*, Jakarta: Raja Grafindo Persada, 2003, Hlm. 89

undang dengan menelaah secara keseluruhan yang berkaitan dengan permasalahan yang diangkat.[27]

1.6.2. Sumber Data

Penelitian ini hanya mengenal data sekunder sebagai sumber datanya, di mana terdiri dari bahan hukum primer, sekunder, maupun tersier. Data yang diperoleh ialah bersumber dari beberapa dokumen, buku terkait objek penelitian ini, hasil penelitian berupa skripsi, tesis dan peraturan perundang-undangan. Data sekunder terbagi menjadi:

1. Bahan Hukum Primer

   Bahan hukum ini meliputi peraturan perundang-undangan, yurisprudensi, dan perjanjian internasional.[28] Bahan hukum primer yang digunakan pada penelitian ini antara lain:

   a. Undang-Undang Republik Indonesia nomor 73 tahun 1958 tentang Menyatakan Berlakunya Undang-Undang nomor 1 tahun 1946 Republik Indonesia tentang Peraturan Hukum Pidana untuk Seluruh Wilayah Republik Indonesia dan Mengubah Kitab Undang-Undang Hukum Pidana (KUHP);
   b. Undang-Undang Republik Indonesia nomor 8 tahun 1981 tentang Hukum Acara Pidana atau Kitab Undang-Undang Hukum Acara Pidana (KUHAP);

[27] Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta: Kencana, 2006, Hlm. 93

28 MuktiFajar, *Dualisme Penelitian Hukum Normatif dan Empiris*, Yogyakarta: Pustaka Belajar, 2010, Hlm. 157

c. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentag Perubahan atas Undang-Undang Nomor 8 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Bahan Hukum Sekunder

Bahan hukum ini sebagai pemberi kejelasan atas bahan hukum primer. Bahan hukum sekunder yang digunakan pada penelitian ini ialah:

a. Buku, termasuk skripsi, tesis dan disertasi hukum.
b. Kamus Hukum.
c. Jurnal Hukum.

3. Bahan Hukum Tersier

Bahan hukum ini sebagai petunjuk dari bahan hukum primer maupun sekunder. Bahasn hukum tersier pada penelitian ini berasal dari:

a. Kamus Besar Bahasa Indonesia;
b. Kamus Lengkap Bahas Inggris-Bahasa Indonesia;
c. Ensiklopedia.

1.6.3. Metode Mengumpulkan dan Olah Data

Perolehan bahan hukum yang diperlukan dalam penelitian ini ialah dengan cara sebagai berikut:

a. Studi Kepustakaan

Studi kepustakaan ialah studi terkait segala sumber yang digunakan dalam penelitian untuk mencari segala data terkait hal

dengan berupa catatan, transkip, buku, majalah, dan hal lain yang menunjang penelitian.[29]

b. Wawancara

Wawancara dalam hal ini digunakan sebagai bahan tambahan untuk melakukan analisa sekaligus menambah akurasi data sekunder hasil studi pustaka.

1.6.4. Metode Analisa Data

Data yang diperoleh kemudian di olah dan di analisa guna mendapat jawaban atas permasalahan yang ada. Data yang di olah dalam penelitian normatif lebih menekankan pada langkah spekulatif teoritis dan analisa normatif kualitatif. Metode deskriptif analisa digunakan Penulis dalam hal ini, dengan memaparkan data sekunder, yang diperoleh melalui studi kepustakaan maupun wawancara. Hal tersebut kemudian di susun, di jabarkan dan diinterprestasi untuk memperoleh jawaban sekaigus kesimpulan atas permasalahan dalam penelitian ini.

1.6.5. Lokasi Penelitian

Dalam hal memperoleh data yang diperlukan dalam penelitian ini, Penulis melakukan penelitian di perpustakaan pada lingkup fakultas, kampus, maupun luar kampus.

1.6.6. Waktu Penelitian

[29] Suharsimi Arikunto, *Prosedur Penelitian Suatu Pendekatan Praktek*, Jakarta: Rhineka Cipta, 1998, Hlm. 19

Penelitian ini dilakukan dalam waktu 4 (empat) bulan, terhitung sejak Maret 2022 hingga Juni 2022. Penelitian ini dilakukan pada minggu pertama bulan Maret 2022.

1.6.7. Sistematika Penulisan

Penelitian ini terbagi menjadi beberapa bab dengan beberapa sub bab. Penelitian ini mengangkat judul **"PENENTUAN *TEMPUS DELICTI* PENCURIAN DATA DALAM TINDAK PIDANA SIBER (*PHISING*) MENURUT UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK",** dengan pembahasannya terbagi menjadi 4 (empat) bab.

Bab Pertama merupakan pendahuluan dengan terbagi menjadi 4 (empat) sub bab. Pertama mengenai latar belakang dengan menguraikan alasan dari masalah penelitian yang diangkat penulis. Sub bab kedua mengenai rumusan masalah yang berisi tentang permasalahan dari uraian latar belakang. Sub bab ketiga mengenai tujuan penelitian. Sub bab keempat ialah mengenai manfaat penelitian.

Bab Kedua membahas tentang penentuan *tempus delicti* pencurian data dalam tindak pidana siber *phising*

Bab Ketiga membahas tentang terjadinya pencurian data dalam tindak pidana siber *phising*. Bab ini terbagi menjadi 2 (dua) sub bab. Pertama membahas tentang kronologi terjadinya pencurian data dalam

tindak pidana siber *phising*. Sub bab kedua membahas tentang analisis terjadinya pencurian data dalam tindak pidana siber *phising*.

Bab Keempat merupakan penutup yang sekaligus sebagai bagian terakhir. Bab ini berisi kesimpulan atas pembahasan yang telah diuraikan dalam bab sebelumnya sekaligus terdapat saran dari penulis.