

BAB I

PENDAHULUAN

A. Latar Belakang

Globalisasi menjadi pendorong lahirnya era perkembangan teknologi informasi, sehingga kebutuhan akan teknologi jaringan komputer semakin meningkat. Perkembangan teknologi yang begitu pesatnya seperti, telekomunikasi, informasi dan komputer yang didukung oleh jaringan yang luas berupa internet dan juga memiliki kecepatan yang terus berkembang memudahkan manusia dalam melaksanakan kehidupan. Manusia antar benua bahkan belahan dunia dapat berkomunikasi hanya menggunakan alat telekomunikasi berupa komputer dan juga telepon genggam tanpa bertatap muka secara langsung. Berbagai macam informasi bisa mudah disajikan dengan kecanggihannya dan begitu mudah diperoleh. Hal ini memberi isyarat bahwa era *cyber* dalam dunia bisnis dimulai.¹

Kemajuan teknologi begitu pesat dapat kita rasakan, teknologi yang berkembang pesat ini selain memiliki dampak yang positif juga memiliki suatu dampak negatif yang juga ikut hadir dengan teknologi tersebut. Adanya dampak negatif yang hadir dengan perkembangan teknologi maka muncul pula kejahatan-kejahatan baru yang sangat kompleks dalam bentuk modus operasi baru yang belum pernah terjadi.² Kejahatan-kejahatan seperti ini

¹ Suparni, Niniek, *Cyberspace Problematika dan Aplikasi Pengaturannya*, Jakarta: Sinar Grafika, 2009, hal. 1.

² Wahid, Abdul & Latib, Mohamad, *Kejahatan Mayantara*, Bandung: Refika Aditama, 2005, hal. 33.

disebut sebagai kejahatan mayantara (*cybercrime*) yang merupakan suatu aspek negatif yang melekat pada perkembangan teknologi.

Semakin canggihnya suatu teknologi, pelaku *cybercrime* berevolusi menjadi berbagai jenis kejahatan baru dengan modus operandi yang baru juga. Berbagai bentuk *cybercrime* terus berkembang dengan pesat seperti *hacking*, *cracking*, *carding* hingga yang lebih spesifik lagi yaitu: *probe* (usaha untuk memperoleh akses ke dalam suatu sistem), *scan* (*probe* dalam jumlah besar), *account compromise* (penggunaan *account* secara ilegal), *root compromise* (*account compromise* dengan *privilege* bagi si penyusup), *denial of service* atau *dos* (membuat jaringan tidak berfungsi karena kebanjiran *traffic*), penyalahgunaan *domain name* dan lain-lain.³

Cybercrime sendiri merupakan kejahatan yang dilakukan menggunakan jaringan sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual menggunakan jaringan internet dan menjadikan pengguna internet lainnya sebagai korban atau sasarannya. Beberapa bentuk kejahatan *cyber* adalah seperti memanipulasi data, *spionase*, *hacking*, penipuan kartu kredit orang (*carding*), merusak sistem (*cracking*), penyalinan data dari kartu ATM (Anjungan Tunai Mandiri) (*skimming ATM*), dan berbagai macam kejahatan lainnya. Kejahatan ini merupakan kejahatan yang sulit dibasmi mengingat para pelaku adalah para ahli di bidangnya.⁴

³ Ekawati, Dian, "Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan", *UNES Law Review*, Vol 1, Issue 2, 2018, hal. 158.

⁴ Suhariyanto, Budi, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: Rajawali Pers, 2013, hal. 17.

Cybercrime di Indonesia terjadi sejak tahun 1983, terutama di bidang perbankan. Setiap tahunnya sampai saat ini di Indonesia banyak terjadi *cybercrime*, seperti pembajakan program komputer, *cracking*, penipuan penggunaan kartu kredit pihak lain secara tidak sah (*carding*), pembobolan bank (*banking fround*), pornografi, menduplikasi dan merekam data kartu ATM (*skimming ATM*), termasuk kejahatan terhadap nama domain (*domain name*).⁵ Dari berbagai macam kejahatan *cyber* tersebut, penelitian ini hanya akan mefokuskan pada kejahatan *skimming ATM*.

Skimming sendiri merupakan modus kejahatan yang berupa pengganda data kartu ATM nasabah yang menggunakan alat yang ditempatkan pada *card reader*, dengan cara menempatkan alat yang dibentuk sedemikian rupa menyerupai sebuah *card reader*. Kemudian menggunakan modus ini kemudian ketika nasabah memasukkan kartu ATM kemesin secara otomatis alat tersebut dapat menggandakan data dan menyalin pin nasabah, dan kemudian pelaku menggunakan kartu palsu yang sudah disiapkan untuk mengambil uang nasabah dengan cepat dan pada umumnya para nasabah tidak menyadari bahwa mereka telah menjadi korban *skimming*.⁶

Awal tahun 2021, diberitakan suaramerdeka.com sebanyak 35 nasabah BRI yang berada di Kota dan Kabupaten Tegal mengalami kehilangan uang yang ada di saldo rekening. Setelah melakukan pengecekan rekaman CCTV di

⁵ Widodo, *Sistem Pidana dalam Cyber Crime*, Yogyakarta: Laksbang Mediatama, 2009, hal. 29.

⁶ Ramdhan, Jovin Ganda & Sumiyati, "Perlindungan Hukum Terhadap Nasabah Korban Skimming Ditinjau Dari Undang Undang Nomor 8 Tahun 1999", *Vol. 12. No. 1, (Surabaya: 2019, Edisi Februari-Juli)*, hal. 89.

mesin ATM BRI yang berlokasi di pinggir jalan raya dekat Batalyon Yonif 407 Slawi, diketahui tanggal 15 Januari 2021 ada pemasangan alat *skimming* dan tanggal 16 Januari 2021 ada pelepasan alat tersebut yang dilakukan dua orang yang tidak dikenal menggunakan helm, jaket, memakai masker. Penggunaan uang dari 35 nasabah tersebut digunakan untuk transaksi perbankan di daerah Malang Jawa Timur dan mengarah ke rekening BRI atas nama Ari Indra Samudra. Akibat adanya kejahatan *skimming* kartu ATM BRI tersebut, total kerugian sebesar Rp. 202.850.000.⁷

Di Amerika pada tahun 2011 perbuatan *skimming* ATM telah diatur dalam peraturan perundang-undangan ATM, dengan merumuskan perbuatan *skimming* ATM sebagai tindak pidana penipuan atau tindak pidana pencurian, maka dapat diharapkan dapat menekankan atau menanggulangi kejahatan ini. Alat *skimming* sangat mudah didapatkan pada pasar gelap dengan harga yang cukup murah di Amerika, Indonesia sendiri belum mengatur tentang kejahatan *skimming* ATM sedangkan hukum harus berkembang sesuai dengan perkembangan masyarakat untuk itulah perlu dilakukan kriminalisasi terhadap perbuatan *skimming* ATM sebagai sebuah tindak pidana.⁸

Sementara itu di Indonesia *cybercrime* telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 yang kemudian telah diperbarui dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi

⁷ Cun Cahaya, 35 Nasabah BRI Kota dan Kabupaten Tegal Kena *Skimming*, Kerugian Rp. 202.850.000, Online: <https://www.suamerdeka.com/nasional/pr-041505953/>, diakses tanggal 12 Maret 2022, pukul 18.33 Wib.

⁸ Ubwarin, Erwin, "Kebijakan Formulasi Hukum Pidana dalam Melanggulangi Kejahatan *Skimming* ATM, *Jurnal Sasi*, Vol. 21, No. 2, 2015, hal. 18.

Elektronik (ITE). Kepolisian melalui peraturan Kepala Kepolisian Nomor 22 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Organisasi membentuk Ditreskrimsus di masing-masing kepolisian daerah untuk memaksimalkan penegakan peraturan hukum yang diberlakukan di *cyberspace*. Peran penting adanya suatu hukum untuk menyelesaikan persoalan-persoalan yang ada, selain menjadi ketentuan yang menjadi dasar manusia untuk melakukan sesuatu dalam norma dan dalam statusnya.⁹

Skimming merupakan teknik mengumpulkan informasi sebuah kartu kredit atau kartu ATM dengan cara menempatkan alat yang biasa disebut *skimmer*. Alat ini bertugas merekam jejak penggunaan sebuah kartu kredit atau kartu ATM. Jika alat ini dipasang dalam sebuah mesin ATM, otomatis semua kartu yang keluar masuk di mesin tersebut akan terekam data dan aktifitasnya. Kejahatan *skimming* termasuk dalam tindak pidana informasi dan transaksi elektronik yang sebagaimana diatur Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Jika mengikuti kasus-kasus kejahatan komputer dan siber yang terjadi, hal tersebut dikaji dengan menggunakan kriteria peraturan hukum pidana konvensional, maka dari segi hukum kejahatan komputer dan siber tersebut bukanlah merupakan suatu kejahatan yang sederhana. Pembuatan pidana agar dapat digunakan di bidang komputer dan siber adalah penipuan, kecurangan, pencurian, dan perusakan yang ada pokoknya

⁹ Wahid, Abdul & Labib, Mohammad, *Op Cit*, hal. 47.

dilakukan secara langsung (dengan menggunakan bagian tubuh secara fisik dan pikiran) oleh si pelaku.¹⁰ Setiap tindak pidana *skimming* tersebut berkaitan dengan tindakan penipuan maupun pencurian melalui *skimming* ATM diatur dalam KUH Pidana yaitu pencurian *skimming* diatur dalam Pasal 363 ayat (1) ke-4 dan ke-5. Sedangkan penipuan *skimming* ini diatur dalam Pasal 378 KUH Pidana.

Berdasarkan uraian di atas, perkembangan teknologi dan transaksi elektronik yang berkembang sangat pesat sehingga semakin banyak kejahatan yang berbasis teknologi terjadi, salah satunya perbuatan *skimming* pada sistem elektronik melalui mesin ATM. Maka penulis tertarik untuk meneliti lebih mendalam terkait permasalahan tersebut dengan mengangkat judul “Tindak Pidana *Skimming* pada Sistem Elektronik Melalui Mesin ATM dalam Hukum Positif di Indonesia.”

B. Rumusan Masalah

Berdasarkan uraian latar belakang yang telah uraikan di atas, maka penulis merumuskan permasalahan penelitian sebagai berikut:

1. Bagaimana pengaturan hukum tindak pidana *skimming* pada sistem elektronika melalui mesin ATM dalam hukum positif di Indonesia?
2. Bagaimana penerapan hukum pidana terhadap tindak pidana *skimming* pada sistem elektronika melalui mesin ATM pada putusan nomor 106/Pid.B/2021/PN Slw?

¹⁰ Suparni, Niniek, *Op Cit*, hal. 4.

C. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Untuk mendeskripsikan hukum tindak pidana *skimming* pada sistem elektronika melalui mesin ATM dalam hukum positif di Indonesia.
2. Untuk mengkaji penerapan hukum pidana terhadap tindak pidana *skimming* pada sistem elektronika melalui mesin ATM pada putusan nomor 106/Pid.B/2021/PN Slw.

D. Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat bagi para pembaca dan kontribusi di bidang ilmu hukum baik secara teoritis maupun praktis. Adapun manfaat dari penelitian ini, antara lain:

1. Secara teoritis, diharapkan hasil penelitian ini dapat menambah wawasan dan pengetahuan ilmu hukum khususnya hukum tindak pidana *skimming* pada sistem elektronika melalui mesin ATM. Hasil penelitian juga dapat dijadikan sumber referensi baru dalam bidang keilmuan hukum pidana untuk kajian studi dalam perkembangan ilmu hukum.
2. Secara praktis, hasil penelitian diharapkan dapat memberikan jawaban rumusan penelitian dan diharapkan dapat memberikan pengetahuan lebih tentang hukum di Indonesia, karena selama ini masyarakat cenderung tidak peduli selama dirinya tidak dirugikan. Sebenarnya, secara tidak langsung masyarakat awam juga ikut dirugikan, dengan adanya kerugian yang dialami oleh negara baik secara materiil maupun moril.

E. Tinjauan Pustaka

Tinjauan pustaka merupakan hasil penelitian terdahulu tentang tindak pidana pelaku tindak pidana *skimming*. Meskipun penelitian terdahulu dengan penelitian ini sejenis dan mempunyai persamaan, namun penelitian ini berbeda dengan penelitian-penelitian sebelumnya baik dalam kajiannya maupun objek yang dikaji. Berikut penelitian terdahulu yang menjadi referensi dalam penelitian ini.

1. Saskara dan Arthani (2021), Tinjauan Kriminologi terhadap Kejahatan *Skimming* melalui ATM di Polda Bali.¹¹ Permasalahan dalam penelitian ini yaitu apa faktor penyebab terjadinya kejahatan *skimming* dan upaya apa yang dilakukan kepolisian dalam menanggulangi kejahatan *skimming*. Pada penelitian ini, memuat penelitian hukum empiris, dengan menggunakan penelitian yang bersifat deskriptif dan menggunakan analisis data kualitatif. Hasil penelitian ini terkait dengan faktor penyebab terjadinya kejahatan *skimming* di Polda Bali terdapat 2 (dua) faktor penyebab yakni faktor internal pelaku dan faktor eksternal pelaku. Terdapat berbagai upaya yang telah dilakukan kepolisian seperti diantaranya upaya pre-emptif, upaya preventif dan upaya represif. Upaya pre-emptif dimaksud dengan memberikan sosialisasi kepada masyarakat agar lebih waspada. Selanjutnya upaya preventif dilakukan dengan bersurat dan bertemu langsung kepada setiap pimpinan lembaga perbankan

¹¹ Saskara, Komang Aldi & Arthani. Ni Luh Gede Yogi, "Tinjauan Kriminologi terhadap Kejahatan *Skimming* melalui ATM di Polda Bali", *Jurnal Mahasiswa Hukum Saraswati (Jumaha)*, Vol. 01, No. 01, 2021, hal. 109-127.

yang ada di Bali agar mengingatkan setiap nasabahnya berhati-hati dan *safety* dalam menggunakan kartu ATM setiap melakukan transaksi di mesin ATM. Dan selanjutnya yang terakhir upaya represif dilakukan dengan cara melakukan penegakan hukum berupa sanksi terhadap pelaku.

2. Pakpahan dan Aryo (2021), Tindak Pidana Turut Serta Mengakses Komputer dan/atau Sistem Elektronik dengan Modus *Skimming*.¹² Penulisan Artikel ini bertujuan untuk mengetahui dan menganalisis tentang bagaimana modus operandi dari skimming dan pertimbangan serta ketentuan peraturan perundang-undangan yang diterapkan kepada pelaku kejahatan *skimming* disertai dengan analisis yuridisnya dalam perkara Nomor 334/Pid.Sus/2020/PN.Mlg. Artikel jurnal ini menggunakan penelitian hukum normatif dengan pendekatan *case approach* dan *statue approach*. Hasil penelitian ini memberikan pengetahuan mengenai modus operandi *skimming* yang dalam pelaksanaannya menggunakan *router* dan/atau alat skimmer yang dapat menyalin data kartu ATM atau sekaligus PIN ATM serta menggunakan hidden kamera untuk mendapatkan PIN ATM. Setelah mendapat data dan PIN ATM, kemudian disalin menggunakan MSR900SEN untuk mengkloning ATM tersebut guna melakukan penarikan uang tunai. Sedangkan pertimbangan hakim pada putusan No.334/Pid.Sus/2020/PN.Mlg dakwaan Pasal 30 ayat 3 UU ITE terdapat upaya atau cara yang sesuai dengan *skimming* yaitu melanggar, menerobos, melampaui, atau memasuki sistem pengamanan

dengan cara ilegal dan dalam dakwaan Pasal 30 ayat 1 UU ITE tidak merinci mengenai upaya atau cara dalam melakukan perbuatan kejahatan skimming serta untuk mengetahui perbuatan para pelaku termasuk tindak pidana turut serta *uitlokker* yang mana terdapat pembuat penganjur yang menganjurkan orang yang dianjurkan agar niat dari orang tersebut terbentuk untuk melakukan perbuatan tindak pidana dimana pembuat penganjur tidak berperan aktif dalam perbuatan tindak pidana.

3. Setiawan (2018), Perkembangan Modus Operandi Kejahatan *Skimming* dalam Pembobolan Mesin ATM Bank sebagai Bentuk Kejahatan Dunia Maya (*Cybercrime*).¹³ Tujuan penelitian ini untuk mengetahui perkembangan modus operandi kejahatan skimming dalam pembobolan ATM bank sebagai bentuk kejahatan dunia maya (*cybercrime*) dan upaya langkah-langkah hukum dalam menanggulangi kejahatan penggunaan sistem informasi dan transaksi elektronika. Hasil penelitian disimpulkan bahwa kejahatan perbankan yang berbasis Teknologi Informasi salah satunya yang menyerang sistem perbankan Indonesia adalah modus kejahatan perbankan umumnya berupa *skimming*, *phishing*, dan *malware*. Dalam hal pencurian dana nasabah bank melalui penggandaan kartu ATM, pelaku kejahatan biasanya menggunakan teknologi komputer dan memanipulasi data dengan cara memindahkan data elektronik

¹² Pakpahan, Hatarto & Aryo, Ahmad, "Tindak Pidana Turut Serta Mengakses Komputer dan/atau Sistem Elektronik dengan Modus *Skimming*", *Bhirawa Law Journal*, Vol. 2, No. 2, November 2021, hal. 218-225.

¹³ Setiawan, Dian Alan, "Perkembangan Modus Operandi Kejahatan *Skimming* dalam Pembobolan Mesin ATM Bank sebagai Bentuk Kejahatan Dunia Maya (*Cybercrime*)", *Era Hukum (Jurnal Ilmiah Ilmu Hukum)*, Vol. 16, No. 2, Oktober 2018, hal. 174-191.

yang terdapat pada kartu ATM korbannya ke kartu ATM milik pelaku dengan bantuan program komputer, sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil yaitu perbuatan seseorang yang memasuki komputer orang lain tanpa izin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Upaya penanggulangan kejahatan melalui sarana pendekatan kriminal dapat menggunakan 2 (dua) sarana, yaitu sarana penal dan non penal. Kebijakan dengan sarana penal adalah upaya penanggulangan kejahatan dengan menggunakan sarana pidana. Sedangkan kebijakan kriminal dengan sarana non penal artinya upaya penanggulangan kejahatan dengan tidak melakukan hukum pidana. Upaya non penal dapat juga diartikan sebagai upaya yang bersifat preventif.

4. Kusuma (2018), *Penegakan Hukum Tindak Pidana Mengakses Komputer dan atau Sistem Elektronik Milik Orang Lain yang Dilakukan oleh Warga Negara Asing (Studi di Pengadilan Negeri Mataram)*.¹⁴ Penelitian ini bertujuan untuk mengetahui penegakan hukum tindak pidana mengakses komputer dan atau sistem elektronik milik orang lain yang dilakukan oleh Warga Negara Asing. Metode penelitian yang digunakan adalah studi lapangan (*field research*) melalui wawancara langsung kepada narasumber yang berkaitan dengan tulisan ini, penulis juga melakukan penelitian kepustakaan (*library research*) dengan mengumpulkan data dari berbagai literatur yang ada. Hasil yang penulis peroleh dari penelitian

ini, yaitu Penegakan hukum dalam upaya penanggulangan *cybercrime* (tindak pidana mengakses komputer dan atau sistem elektronik milik orang lain yang dilakukan oleh Warga Negara Asing) belum efektif disebabkan karena beberapa hal, diantaranya ialah laju pertumbuhan cyber crime yang begitu pesat dan upaya penanggulangan yang masih kurang maksimal mengingat masih banyaknya kasus *cyber crime* yang ditangani oleh aparat kepolisian. Kendala yang dihadapi oleh aparat kepolisian dalam upaya penanggulangan *cyber crime* dapat dibagi ke dalam 4 (empat) aspek, yaitu: aspek penyidik (Tingkat kemampuan dan skill penyidik), alat bukti (data yang rentan untuk diubah dan dihapus), fasilitas dan yurisdiksi.

F. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian penelitian ini adalah penelitian kepustakaan (*library research*). Penelitian kepustakaan merupakan jenis penelitian yang dilakukan dengan membaca buku-buku atau majalah dan sumber data lainnya untuk menghimpun data dari berbagai literatur, baik perpustakaan maupun di tempat-tempat lain.¹⁵ Penelitian kepustakaan tidak hanya kegiatan membaca dan mencatat data-data yang telah dikumpulkan. Tetapi lebih dari itu, peneliti harus mampu mengolah data yang telah terkumpul dengan tahap-tahap penelitian kepustakaan dan mengambil data baik secara tertulis

¹⁴ Kusuma, Jauhari Dwi, "Penegakan Hukum Tindak Pidana Mengakses Komputer dan atau Sistem Elektronik Milik Orang Lain yang Dilakukan oleh Warga Negara Asing (Studi di Pengadilan Negeri Mataram)", *Unizar Law Review*, Vol. 1, No. 2, Desember 2018, hal. 150-166.

untuk diuraikan, sehingga memperoleh gambaran serta pemahaman yang menyeluruh terkait tindak pidana *skimming* mesin ATM.

2. Pendekatan Penelitian

Pendekatan penelitian menggunakan metode yang bersifat yuridis normatif, atau disebut juga penelitian hukum doktrinal yaitu penelitian hukum yang menggunakan sumber data sekunder, yaitu yang berupa hukum positif dengan meneliti bagaimana ketentuan hukum positif tersebut dalam prakteknya. Penelitian hukum normatif meletakkan hukum sebagai sebuah bangunan sistem norma yang dibangun mengenai asas-asas, norma, kaidah dari peraturan-perundangan, putusan pengadilan, perjanjian, serta doktrin.¹⁶

Penelitian hukum normatif dilakukan dengan maksud untuk memberikan argumentasi hukum sebagai dasar penentu apakah suatu peristiwa telah benar atau salah serta bagaimana sebaiknya peristiwa itu menurut hukum.¹⁷ Metode pendekatan yang dipakai dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan ini dilakukan karena memang belum ataupun tidak ada aturan hukum untuk masalah yang dihadapi sehingga diperlukannya pembaharuan hukum atau peraturan.

¹⁵ Mahmud, *Metode Penelitian Pendidikan*, Bandung: Pustaka Setia, 2011, hal. 31.

¹⁶ Fajar, Mukti & Achmad, Yulianto, *Dualisme Penelitian Hukum Normatif dan Empiris*, Yogyakarta: Pustaka Pelajar, 2017, hal. 33.

¹⁷ *Ibid.*, hal. 36.

3. Sumber Data

Penelitian ini menggunakan pendekatan normatif, maka bahan hukum yang digunakan diperoleh melalui penelusuran bahan hukum sekunder atau studi pustaka. Sumber data yang digunakan dalam penelitian kepustakaan ini antara lain bukul-buku teks, jurnal ilmiah, refrensi statistik, hasil-hasil penelitian, dan internet, serta sumber-sumber lainnya yang relevan.¹⁸ Sumber data yang digunakan penelitian ini adalah data yang dikumpulkan berasal dari data sekunder, meliputi bahan hukum primer, bahan hukum sekunder dan bahan hukum tertier berupa norma dasar, perundang-undangan, hasil penelitian ilmiah, buku-buku dan lain sebagainya.

- a. Bahan hukum primer merupakan bahan hukum yang isinya mempunyai kekuatan mengikat karena dikeluarkan pemerintah.¹⁹ Landasan utama yang dipakai dalam rangka penelitian ini adalah Kitab Undang-Undang Hukum Pidana dan Undang-Undang No. 11 Tahun 2008 jo Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik.
- b. Bahan hukum sekunder, adalah bahan-bahan yang membahas bahan primer.²⁰ Pada penelitian ini, yang menjadi bahan sekunder adalah buku ilmu hukum, hasil-hasil penelitian hukum, literatur hukum, jurnal penelitian terkait dengan tindak pidana *skimming*, dan lain-lain.
- c. Bahan Hukum Tersier, yaitu bahan hukum yang akan melengkapi atau menunjang bahan hukum primer dan sekunder.²¹ Bahan tersier pada

¹⁸ Sanusi, Anwar, *Metodologi Penelitian Bisnis*, Jakarta: Salemba Empat, 2016, hal. 32.

¹⁹ Ashafa, Burhan, *Metode Penelitian Hukum*, Jakarta: Rineka Cipta, 2013, hal. 103.

²⁰ *Ibid.*, hal. 103.

²¹ *Ibid.*, hal. 104.

penelitian ini diantaranya yaitu kamus hukum dan bahan dari internet yang berkaitan dengan tindak pidana *skimming*.

4. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan yaitu studi kepustakaan (*library research*) atau studi dokumen, yaitu suatu alat pengumpulan data dilakukan melalui data tertulis.²² Studi pustaka merupakan langkah awal dalam metode pengumpulan data, yang diarahkan kepada pencarian data dan informasi melalui dokumen-dokumen, baik dokumen tertulis, foto-foto, gambar, maupun dokumen elektronik yang dapat mendukung dalam proses penulisan. Studi kepustakaan berkaitan dengan kajian teoritis dan referensi lain yang berkaitan dengan nilai, budaya dan norma yang berkembang pada situasi sosial yang diteliti.²³

Oleh karena sumber data utama berupa data sekunder, yaitu data-data tertulis, maka teknik pengumpulan data dalam penelitian ini menggunakan studi kepustakaan dan teknik dokumentasi dengan pengkajian informasi tertulis mengenai hukum yang berasal dari berbagai sumber dan dipublikasikan secara luas serta dibutuhkan dalam penelitian hukum normatif.

5. Metode Analisis Data

Metode analisis yang digunakan dalam penelitian ini yaitu melalui pendekatan analisis kualitatif yaitu menguraikan data secara bermutu dalam bentuk kalimat yang teratur, runtun, logis, tidak tumpang tindih, dan selektif,

²² Soekanto, Soerjono, *Pengantar Penelitian Hukum*, Jakarta: UI Press, 2011, hal. 21.

²³ Sugiyono, *Op Cit.*, hal. 291.

sehingga memudahkan interpretasi data dan pemahaman hasil analisis.²⁴ Analisis dilakukan dengan mengadakan pengamatan data-data yang diperoleh dan menghubungkan tiap-tiap data yang diperoleh tersebut dengan ketentuan maupun asas-asas hukum yang terkait dengan permasalahan yang diteliti.

Teknik analisis data secara kualitatif dilakukan dengan cara mengelompokkan dan menseleksi data yang diperoleh dari penelitian lapangan menurut kualitas dan kebenarannya kemudian disusun secara sistematis, yang selanjutnya dikaji dengan metode berfikir secara deduktif dihubungkan dengan teori-teori dari studi kepustakaan (data sekunder), kemudian dibuat kesimpulan yang berguna untuk menjawab rumusan masalah dalam penelitian ini. Cara berfikir deduktif, yaitu suatu cara berfikir untuk menganalisis data dengan mengurai dan memposisikan sebuah deskripsi bersifat umum dijabarkan pada uraian yang lebih spesifik.²⁵

G. Sistematika Penulisan

Sistematika penulisan penelitian ini memberikan gambaran tentang isi skripsi untuk lebih memudahkan pembaca dalam memahami isi skripsi. Berikut sistematika penulisan skripsi dalam penelitian ini.

Bab I Pendahuluan. Berisi tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian dan sistematika penulisan.

²⁴ Muhammad, Abdukadir, *Hukum dan Penelitian Hukum*, Bandung: Citra Aditya Bakti, 2004, hal. 127.

²⁵ Hadi, Sutrisno, *Metodologi Research*, Yogyakarta: Andi Offset, 2001, hal. 36.

Bab II Tinjauan Konseptual. Bab ini menguraikan teori-teori terkait dengan permasalahan penelitian, meliputi tinjauan umum tentang tindak pidana, tinjauan umum tentang *skimming*, dan tinjauan umum tentang *cyber crime*.

Bab III Hasil Penelitian dan Pembahasan. Bab ini berisi hasil penelitian dan pembahasan tentang pengaturan hukum tindak pidana *skimming* pada sistem elektronika melalui mesin ATM dalam hukum positif di Indonesia dan penerapan hukum pidana terhadap tindak pidana *skimming* pada sistem elektronika melalui mesin ATM pada putusan nomor 106/Pid.B/2021/PN Slw.

Bab IV Penutup. Terdiri atas simpulan terkait dengan hasil penelitian dan saran-saran dari penulis terkait dengan tindak pidana pemerasan.