BAB I

PENDAHULUAN

A. Latar Belakang

Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi (*informasi technology*) memang peran penting, baik di masa kini maupun dimasa yang akan datang. Teknologi informasi diyakini membawa kuntungan dan kepentingan yang besar bagi Negara Negara di dunia. Setidaknya ada dua hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia. Pertama, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti computer, modem, sarana untuk membagun jaringan internet dan sebagainya. Kedua, adalah memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis lainnya. Teknologi informasi telah berhasil memicu dan memacu perubahan tatanan kebutuhan hidup masyarakat di bidang *social* dan ekonomi, yang notabene sebelumnya bertransaksi ataupun bersosialisasi secara konvensional menuju transaksi ataupun sosialisasi secara elektronik. Hal ini dinilai lebih efektif dan efesien.[1] Di era globalisasi ini, selain ada hal positif yang bisa dimanfaatkan oleh setiap bangsa, khususnya di bidang teknologi, juga menyimpan kerawanan yang tentu saja sangat membahayakan. Bukan hanya soal kejahatan konvensional yang gagal diberantas akibat terimbas oleh pola-pola modernitas yang gagal mengedepankan prinsip humanitas, tetapi juga munculnya kejahatan di alam maya yang telah menjadi realitas

masyarakat dunia. Munculnya kejahatan bernama "*cyberspace*" atau dengan nama lain "*cybercrime"* merupakan suatu pembenaran, bahwa era global ini identik dengan era ranjau

[1] Budi Suhariyanto, *Tindak P knologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah hukumnya* , (Jakarta : Raja Grafindo 2012), hal. 1

ganas. Sebuah ruang imajiner dan maya, area atau zona bagi setiap orang untuk melakukan aktivitas yang bisa dilakukan dalam kehidupan sosial sehari-hari dengan artifisial.

Setiap orang bisa saling berkomunikasi, menikmati liburan, dan mengakses apa saja yang menuntut bisa mendatangkan kesenangan. *Cyber crime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. *Volodymyr Golubev* menyebutnya sebagai *the new form of anti-social behaviour* (bentuk baru dari perilaku anti-sosial). *Cyber crime* merupakan satu sisi gelap dari kemajuan teknologi yang mempunyai dampak *negative* sangat luas bagi seluruh bidang kehidupan modern saat ini.

Kejahatan ini merupakan tindak kejahatan melalui jaringan system komputer dan sistem komunikasi baik lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual dengan melibatkan pengguna internet sebagai korbannya. Kejahatan tersebut seperti misalnya manipulasi data *(the Trojan horse), spionase, hacking*, penipuan kartu kredit online *(carding),* merusak sistem *(cracking),* pengcopyan data dari kartu ATM (*Skimming* ATM) dan berbagai macam lainnya. Pelaku *cybercrime* ini memiliki latar belakang kemampuan yang tinggi di bidangnya sehingga sulit untuk melacak dan memberantasnya secara tuntas.

Sekalipun kemajuan teknologi informasi memberikan banyak kemudahan bagi kehidupan manusia, tetapi kemajuan inipun secara bersamaan menimbulkan berbagai permasalahan yang tidak mudah ditemukan jalan keluarnya. Salah satu masalah yang muncul akibat perkembangan teknologi informasi adalah lahirnya kejahtan-kejahatan yang sifatnya baru, khususnya yang mempergunakan internet sebagai alat bantunya.[2] Oleh karena itu, pemerintah mengeluarkan Undang-Undang No. 11 tahun 2008 dan telah di perbaharui dengan Undang-undang Nomor 19

[2] http://repository.unpas.ac.id/28086/3/BAB%20I.pdf. Diakses pada tanggal 24 Juni 2020 pada pukul 03.26 wib.

tahun 2016 Tentang Informasi dan Transaksi Elektronik (ITE).

Teknik pembobolan kartu ATM nasabah melalui metode *skimming* ini pertama kali terjadi pada tahun 2009 di ATM Citibank, Woodland Hills, California. Saat itu diketahui bahwa metode atau cara kerja skimming dilakukan dengan mengggunakan alat *skimmer* yang ditempelkan pada tempat memasukkan kartu ATM (atau pada slot mesin ATM). Sehingga data nasabah yang tersimpan pada *magnetic srtripe* ATM tercuri dan dapat digandakan.[3] Di Indonesia kasus *skimming* sudah banyak terjadi yang melibatkan jaringan penjahat internasional. Dalam kurun waktu 2011 hingga 2017, kasus pembobolan ATM dengan skimming terus meningkat. Pada tahun 2015 saja, di Indonesia terjadi sekitar 1.549 kasus skimming atau 1/3 dari kasus skimming di dunia.[4]

Pada dasarnya kasus pelanggaran informasi dan transaksi elektronik (ITE) sangat sering dijumpai di kalangan masyarakat guna untuk menguntungkan diri sendiri dengan mengambil hak orang lain secara skimming dengan cara kerja melalui Mesin ajungan Tunai (ATM) dan tentunya merugikan suatu objek serta melanggar peraturan yang tercantum dalam UU ITE.

Kejahatan *Skimming* adalah suatu tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada strip magnetik kartu kredit atau debit secara ilegal[5]. Melalui *skimmer* para pelaku menduplikasi atau penyadapan data strip magnetik pada kartu ATM, lalu mengubah ke kartu ATM kosong. Proses ini bisa dilakukan dengan cara manual, seperti pelaku kembali ke ATM dan mengambil cip data yang sudah disiapkan

[3] http://www.jogjatronik.com/v3/2018/03/mengenal-kejahatan-skimming/.Diakses Pada tanggal 18 Agustus 2020 Pada pukul 22.15 wib.

[4] https://www.wartaekonomi.co.id/read173977/tuyul-itu-bernama-skimming.Diakses Pada tanggal 18 Agustus 2020 Pada pukul 22.34 wib.

[5] https://money.kompas.com/read/2020/01/24/184000326/waspadai-skimming-ini-cara-menghindarinya-#:~:text=Skimming%20adalah%20suatu%20tindakan%20pencurian,kredit%20 atau%20debit%20secara%20ilegal. Diakses pada tanggal 01 Juli 2020 pada pukul 16:21 wib

sebelumnya. Atau bila menggunakan alat *skimmer* yang lebih canggih, data-data yang telah dikumpulkan dapat diakses dari mana pun secara nirkabel.

Dengan menyalin segala informasi yang terdapat pada *strip magnetic* kartu secara *illegal* dan nantinya informasi atau data nasabah tersebut disalin kedalam kartu yang masih kosong. Tak lain tujuan dari kejahatan ini adalah pembobolan dana terhadap nasabah bank tersebut. Kejahatan tersebut merupakan salah satu contoh penyalahgunaan teknologi informasi yang di pergunakan sebagai sarana melakukan kejahatan oleh orang-orang yang tidak bertanggung jawab dan hal ini dapat menyulitkan pihak Kepolisian atau pihak lainnya jika tidak paham tentang kejahatan yang berbasis teknologi seperti kejatan skimming tersebut. Kartu baru hasil duplikat memungkinkan setiap pelaku untuk mengeluarkan uang dari rekening secara biasa. Korban sering tidak menyadari bahwa kartunya telah terduplikasi sampai korban melakukan transaksi dengan ATM yang telah diduplikat oleh para pelaku tersebut. Dalam kasus terbaru ini proses penarikan uang dapat dilakukan dari luar negeri karena nominal uang yang ditarik tidak bulat dan adanya pengenaan biaya administrasi.

Dalam Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang ITE telah dijelaskan bahwa "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".

Seperti kasus diatas Gilcha-Amzulescu George Silviu dan Stancu Razvan Aurelia alias Aurelian kedua terdakwa bersama-sama melakukan tindak pidana penyadapan ATM melalui cara *Skimming*. Terdakwa satu dan terdakwa dua berencana memasang alat skimming dengan berkeliling kota menggunakan sepeda motor untuk mencari lokasi ATM yang tepat untuk

melancarkan aksi kedua terdakwa tersebut. Pada tengah malam mereka melakukan pemasangan alat skimmer pada dua mesin ATM BNI, terdakwa satu bertugas memasang alat skimmer dan terdakwa dua bertugas memasangkan kamera tersembunyi atau CCTV pada kedua mesin ATM tersebut. Adapaun rekaman yang tersimpan pada memeri card yang telah terintegrasi dengan CCTV dan di pindahkan ke laptop dan kemudian hasil rekaman ataupun data hasil skimmer dikirim ke via situs Sendspace.com dengan tujuan untuk dibuka dikarenakan data tersebut masih terkunci dan membukanya melalui situs tersebut. Tetapi ATM mengalami kesalahan yang mengakibatkan kartu ATM nasabah tertelan kemudian melaporkannya, dan melakukan pengecekan dilokasi. Saksi Ardiansyah pegawai kantor PT.SSI (swadaya sarana informasi) menemukan benda yang sengaja dipasang pada tempat memasukkan kartu yang ada di mesin ATM yaitu alat skimmer tersebut, dan melaporkannya kepada pihak kepolisian Polda Sulsel, dari hasil laporan tersebut pihak Polda Sulses, pihak BNI dan PT. SSI bekerja sama melakukan pemantauan pada mesin ATM tersebut guna untuk menemukan pelaku pembuat alat skimmer tersebut, dan sekira pukul 00.48 wita kedua terdakwa kembali mengecek mesin ATM dan tidak lama kemudian mereka ditangkap.

Penulis sadari bahwah Skimming ATM telah menyentuh setiap kalangan dimasyarakat. Hal-hal tersebut yang Penulis tertarik untuk mengkaji lebih dalam lagi sehingga penulis tertarik mengangkat skripsi dengan judul "**PERTANGGUNG JAWABAN PIDANA MELAKUKAN PENYADAPAN TERHADAP INFORMASI ELEKTRONIK DAN ATAU DOKUMEN ELEKTRONIK MELALUI KEJAHATAN SKIMMING (Studi Putusan Nomor 282/ Pid.Sus/2020/ PN. MKS)**

B. Rumusan Masalah

Berdasarkan uraian latar belakang diatas teradap rumusan masalah dalam penelitian ini adalah :

1. Bagaimanakah pertanggungjawaban pidana dalam kasus Penyadapan ataupun Pembobolan ATM Melalui Teknik *Skimming* Dihubungkan Dengan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ?
2. Bagaimanakah cara menanggulangi kasus penyadapan ataupun pembobolan ATM melalui teknik skimming yang terjadi dalam Studi Kasus Putusan Nomor 282/pid.sus/2020/PN.MKS ?

C. Tujuan Penelitian

Berdasarkan permasalahan diatas, maka tujuan penulisan hukum (skripsi) ini adalah

1. Untuk mengetahui bagaimana pertanggungjawaban pidana dalam kasus penyadapan ATM melalui teknik Skimming dihubungkan dengan UU no 19 Tahun 2016 Tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektornik dalam Studi Kasus Putusan Nomor 282/Pid.Sus/2020/PN.MKS?
2. Untuk mengetahui bagaimana menanggulangi kasus penyadapan ataupun pembobolan ATM melalui Teknik Skimming dalam Studi kasus Putusan Nomor 282/Pid.Sus/2020/PN.MKS.

D. Manfaat Penelitian

Adapun yang menjadi manfaat dalam penelitian ini adalah sebagai berikut:

1. Manfaat Teoritis

Secara Teoritis hasil penelitian ini diharapkan dapat memberikan sumbangan pemikiran bagi pengembangan ilmu hukum pidana, khususnya pengetahuan tentang Hukum Pidana Khusus

penyadapan terhadap Informasi Elektronik dan atau Dokumen Elektonik melalui Kejahatan *Skimming.*

2. Manfaat praktis

   Penulisan ini juga diharapkan dapat meberikan masukan bagi kalangan praktisi hukum, khusunya yang bergerak dalam bidang hukum pidana terutama para aparat penegak hukum, kepolisian, Kejaksaan, Kehakiman yang bertugas menangani kasus cybercrime tentang Penyadapan terhadap Informasi Elektronik dan atau Dokumen Elektronik melalui Kejahatan *Skimming*

3. Manfaat Bagi Penulis

   Penulisan ini tentunya sangat bermanfaat bagi penulis sebagai salah satu syarat dalam memperoleh Gelar Sarjana Hukum di Fakultas Hukum yang lebih tepatnya di Universitas HKBP Nommensen Medan.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Mengenai Pertanggungjawaban Pidana

1. Pengertian Pertanggungjawaban Pidana

Pertanggungjawabana pidana adalah suatu bentuk untuk menentukan apakah sesorang tersangka atau terdakwa dipertanggungjawabkan atas suatu tindak pidana yang telah terjadi. Dengan kata lain pertanggungjawaban pidana adalah suatu bentuk yang menentukan apakah seseorang tersebut dibebaskan atau dipidana. Pertanggungjawaban pidana sangat diperlukan dalam suatu system hukum pidana.

Syarat tidak dipertanggungjawabkannya pembuat adalah pada saat pembuat melakukan tindak pidana, karena adanya factor dalam diri pembuat maupun faktor di luar diri pembuat. Seseorang yang telah melakukan tindak pidana tidak akan dipidana apabila dalam keadaan sedemikian rupa sebagaimana yang dijelaskan di dalam *Memorie van toeliching (MvT)*. Apabila dalam diri seorang pembuat tidak terdapat keadaan sebagimana yang diatur dalam *Memorie van toeliching* tersebut, pembuat adalah orang yang dipertanggungjawabkan dan dijatuhi pidana.[6]

Dalam konsep hukum pidana konsep "pertanggungjawaban" itu merupakan konsep sentral yang dikenal dengan ajaran kesalahan. Dalam bahasa latin ajaran kesalahan dikenal sebagai *mens rea.* Doktrin *mens rea* dilandaskan pada suatu perbuatan tidak mengakibatkan seseorang bersalah kecuali jika pikiran orang itu jahat. Dalam bahasa inggris doktrin tersebut dirumuskan dengan *an act does not make aperson guilty, unless the mind is legally blameworthy.* Berdasarkan asas tersebut, ada dua syarat yang harus dipenuhi untuk dapat memidana seseorang, yaitu ada perbuatan lahiriah yang 1 9 /perbuatan pidana (*actus reus*), dan ada sikap batin jahat/tersela *(mens rea*).[7]

Van Hamel menyatakan pertanggungjawaban adalah suatu keadaan normal psikis dan kemahiran yang membawa tiga macam kemampuan, yaitu "pertama", mampu untuk mengerti makna serta akibat sungguh-sungguh dari perbuatan-perbuatan sendiri. Kedua, mampu untuk menginsyafi bahwa perbuatan-perbuatan itu bertentangan dengan keterlibatan masyarakat. Ketiga, mampu untuk menentukan kehendak berbuat.[8]

Perlu penjelasan lebih lanjut terkait ketiga kemampuan yang dikemukakan oleh Van Hamel adalah perihal kehendak berbuat. Bila dikaitkan antara kehendak berbuat dengan kesalahan sebagai elemen terpenting dari pertanggungjawaban, maka terdapat tiga pendapat.

---

[6]Agus Rusianto, *Tindak Pidana dan Pertanggungjawaban Pidana* (Jakarta, Prenadamedia Grup.2018)1.
[7] Mahrus Ali, *Dasar-Dasar Hukum Pidana*.(Jakarta Timur,Penerbit Sinar Grafika,2011),155.
[8] Eddy O.S Hiariej, Prinsip-Prinsip Hukum Pidana, (Yogyakarta, Cahaya Adma Pustaka, 2016), 155

Pertama, indterminis yang menyatakan bahwa manusia mempunyai kehendak bebas dalam bertindak. Kedua, determinis yang menyatakan bahwa manusia tindak mempunyai kehendak bebas. Keputusan kehendak ditentukan sepenuhnya oleh watak dan motif yang mendapat ransangan dari dalam maupun dari luar. Ketiga, pendapat yang menyatakan bahwa kesalahan tidak ada kaitannya dengan kehendak bebas. Tegasnya, kebebasan kehendak merupakan suatu yang tidak ada hubungannya dengan kesalahan dalam hukum pidana.[9]

Simons juga memberikan pendapat yang berisikan "kemampuan bertanggung jawab dapat diartikan suatu keadaan psikis sedemikian rupa, sehingga penerapan suatu upaya pemidanaan, baik ditinjau secara umum maupun dari sudut orangnya yang dibenarkan" selanjutnya dikatakannya, seseorang pelaku tindak pidana mampu bertanggung jawab apabila mampu mengetahui/menyadari bahwa perbuatannya bertentangan dengan hukum dan mampu menentukan kehendaknya sesuai dengan kesadaran tadi. Gambaran simons ini menunjukkan bahwa "*toerekeningsvatbaar heid*" adalah "kesalahan".[10]

Sebab asas dalam peranggungjawaban dalam hukum pidana ialah: tidak dipidana jika tidak ada kesalahan (*gean starf jonder schuld; actus nin facit reum nisi mens sist rea)* asas ini tidak tersebut dalam hukum tertulis yang juga di Indonesia berlaku. Hukum pidana fiskal tidak memakai kesalahan. Jika seseorang melanggar ketentuan, dia diberi pidana denda atau ranpas. Pertanggungjawaban tanpa adanya kesalahan dari pihak yang melanggar, dinamakan *leer van heat materiele feit (fait materielle).*[11]

---

[9] Ibid, Hal 155
[10] Teguh Prasetyo, *Hukum Pidana*, (Jakarta, RajaGrafindo Persada, 2015), 85.
[11] Moeljatno, *Asas-Asas Hukum Pidana*, (Jakarta, Rineke Cipta, 2015), 165.

2. Syarat-syarat pertanggungjawaban pidana

Pertanggungjawaban pidana diartikan sebagai diteruskannya celaan yang objektif yang ada pada perbuatan pidana dan secara subjektif yang ada memenuhi syarat untuk dapat dipidana karena perbuatannya itu. Dasar adanya perbuatan pidana adalah asas legalitas, sedangkan dasar dapat dipidananya pembuat adalag asas kesalahan. Ini berarti bahwa pembuat perbuatan pidana hanya akan dipidana jika ia mempunyai kesalahan dan melakukan perbuatan pidana tersebut.

Tindak pidana jika tidak ada kesalahan adalah merupakan asas pertanggung jawaban pidana, oleh sebab itu dalam hal dipidananya seseorang yang melakukan perbuatan sebagaimana yang telah diancamkan, ini tergantung dari soal apakah dalam melakukan perbuatan ini dia mempunyai kesalahan.

B. Tinjauan Mengenai Penyadapan

Penyadapan (*wiretapping*) secara tidak sah adalah setiap perbuatan orang yang menggunakan peralatan teknis untuk mendengarkan, memonitor, mengawasi, atau mengcopy isi komunikasi pihak lain melalui internet, baik secara langsung, yaitu melaslui akses dengan penggunaan sistem komputer, maupun secara tidak langsung, yaitu melalui penggunaan peralatan system elektronik lain atau alat yang dapat membuat pencabangan saluran informasi. Dalam pengertian penyadapan termasuk juga merekam isi informasi dalam suatu system atau jaringan komputer secara tidak sah.[12]

Pada dasarnya, apabila dilihat dari segi historis atau sejarah, usaha-usaha untuk mengetahui informasi yang bersifat rahasia dari orang lain atau pihak lain atau suatu kelompok tertentu demi kepentingan pribadi sesungguhnya bukanlah hal yang baru melainkan telah

[12] Widodo. *Hukum Pidana di Bidang Teknologi Informasi Cybercrime Law* (Yogyakartra, Aswaja Pressindo,2011),57.

berkembang sejak dahulu kala. Meskipun demikian, perlu untuk dikemukakan bahwa proses atau cara yang digunakan untuk mendapatkan informasi rahasia dari pihak lain tersebut diatas tentu sudah mengalami perkembangan.

Di era moderenisasi dan globalisasi dewasa ini, usaha-usaha untuk mengetahui informasi rahasia dari orang atau pihak lain tidak lagi dilakukan secara manual atau konvensional dengan mengandalkan kemampuan fisik diri sendiri tetapi sudah dilakukan dengan menggunakan teknologi yang lebih modern, atau dapat dikatakan bahwa dengan adanya perkembangan masyarakat dan perkembangan zaman yang demikian pesat dewasa ini yang salah satunya dirincikan dengan adanya perkembangan di bidang teknologi informasi, menjadikan usaha-usaha untuk mengetahui informasi milik orang lain bersifat rahasia semakin mudah untuk dilakukan. Kegiatan seperti inilah yang penulis sebut kegiatan penyadapan pada umumnya.

Di Indonesia sendiri, tindakan penyadapan telah mulai dilakukan semenjak dikenal adanya teknologi informasiyang semakin marak tepatnya pada saat teknologi informasi mendapat perhatian secara serius di Indonesia. Hal ini ditandai dengan diluncurkannya satelit Palapa-A1 pada tanggal 9 juli 1976. Peristiwa peluncuran satelit ini menandakan dimulainya perkembangan teknologi informasi di Indonesia yang diantaranya juga menyangkut penyadapan.[13]

Pengertian peralatan teknis meliputi alat teknis yang ditempatakan pada jalur transmisi, misalnya alat untuk mengumpulkan dan merekam isi komunikasi yang tidak menggunakan kabel. Peralatan teknis dapat berupa perangkat lunak(*software*), kata sandin dan kode akses. Ketentuan tentang penggunaaan “peralatan teknis” perlu diatur secara tegas dalam hukum pidana

[13] Kristian dan Yopi Gunawan ,*Sekelumit Tentang Penyadapan Dalam Hukum Positif Di Indonesia*.(Bandung, Penerbit Nuansa Aulia,2013),20.

setiap Negara agar tidak terjadi *over*-kriminalsisasi. Tindak Pidana penyadapan (pe-nguping-an) diatur dalam pasal 31 UU-ITE berikut.

1) Setiap orang atau tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektroinik dalam suatu komputer dan/atau Sistem Elektronik tertentu milik orang lain.
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Eletronik yang tidak bersifat public dari, ke, dan dilam suatu komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
3) Kecuali intersepsi sebagai mana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan bersdasarkan UU.
4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagai mana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah (ketentuan ayat(4) ini sudah tidak berlaku karena sudah dibatalkan Mahkamah Konstitusi.

Dalam penjelasan Pasal 31 ayat (1) UU-ITE diuraikan bahwa yang dimaksud dengan" intersepsi atau penyadapan" adalah kegiatan untuk mendegarkan, merekam, membelokan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan *nirkabel*, seperti pancaran elektromagnestis atau radio frekuensi. Sedangkan ketentuan Pidananya diatur dalam Pasal 47 UU-ITE berikut. Setiap orang yang memenuhi unsur sebagai

mana yang dimaksud dalam pasal 31 ayat (1) atau ayat (2) di Pidana dengan Pidana penjara 10 tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).[14]

C. **Tinjauan Umum Megenai Informasi Elektronik dan/atau Dokumen Elektronik**

1. Pengertian Informasi Elektonik dan/atau Dokumen Elektronik.

Mengenai Informasi Elektronik, Pasal 1 angka 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyebutkan bahwa; "Informasi Elektronik adalah satu atau sekumpulan data eletktronik, termasuk, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Sedangkan Dokumen Elektronik adalah Setelah mengetahui pengertian dari informasi elektronik, maka perlu pula kita mengetahui arti dari dokumen elektronik. Dokumen elektronik adalah sebagaimana yang diatur dalam Pasal 1 angka 4 yang menyebutkan "dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya yang dapat dilihat, ditampilkan dan/atau didengar melalui Komputer atau Sistem Eletktronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya"[15]

Aplikasi teknologi informasi memiliki keterkaitan erat dengan informasi elektronik dan dokumen elektronik. Informasi elektronik merupakan satu atau sekumpulan data elektronik,

---

[14] Widodo, Op.cit,.57-58

[15] http://www.jurnalhukumdanperadilan.org/index.php/jurnalhukumperadilan/article/view/43/53

termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, symbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahami.[16]

Informasi merupakan inti dari globalisasi, khususnya bagi Negara-negara yang berambisi membangun dan mewujudkan perubahan, disebutkan Sardar (1989), bahwa sebagaimana Negara-negara dewasa ini yang berupaya mengendalikan sumber-sumber daya dan harga-harga komoditi, maka didalam waktu yang tidak terlalu lama, informasi, sebagai suatu komoditi yang sangat diperlukan oleh kekuatan produktif, akan menjadi penentu daya saing di seluruh dunia untuk meraih kekuasaan.[17]

Berbagai faktor yang ada dalam kehidupan di dunia ini dapat atau berpotensi untuk menimbulkan kejahatan, bahwa perbuatan baik pun dapat memicu seseorang untuk melakukan kejahatan. Kejahatan tidak dapat diprediksi kejadiannya karena begitu antik, tidak mempedulikan tempat dan suasana. [18] ketika ia hendak muncul dan tidak mengenal kasta atau status social pelaku dan korbannya. Ia begitu misterius ketika belum muncul dan ketika muncul ia menjadi bahan yang menarik untuk dibicarakan, baik di ruang-ruang seminar, lokakarya, penataran di warung kopi pinggir jalan.

2. Jenis-Jenis Informasi Elektronik dan/atau Dokumen Elektronik

Tindak pidana ITE diatur dalam 9 pasal, dari Pasal 27 sampai dengan Pasal 35. Dalam 9 pasal tersebut dirumuskan 17 bentuk/jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang

[16] Sugeng, *Hukum Telematika Indonesia*, (Jakarta, Prenadamedia Grup, 2020), 11.
[17] Abdul Wahid dan Mohammad Labib*, Kejahatan Masyarakat*, (Bandung, Refika Aditama, 2005). 5
[18] Agus Raharjo, *Cyber Crime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung, Citra Aditya Bakti, 2002),33.

diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 sampai dengan Pasal 34. Pasal 37 juga mengatur tentang dasar pemberatan pidana (dengan alasan yang lain dari Pasal 36) pada tindak pidana Pasal 27 sampai dengan Pasal 36. Sementara ancaman pidananya ditentukan di dalam Pasal 45 sampai Pasal 52.

a. Tindak Pidana Mendistribusikan Informasi Elektronik yang Memiliki Muatan yang Melanggar Kesusilaan Pasal 27 Ayat (1) jo 45 Ayat (1)
b. Tindak Pidana Mendistribusikan Informasi Elektronik dan/atau Dokumen Elektronik yang memuat Perjudian Pasal 27 Ayat (2) io 45 Ayat (1)
c. Tindak Pidana Dengan Sengaja dan Tanpa Hak Mendistribusikan Informasi Elektronik yang Memiliki Muatan Penghinaan dan/atau Pencemaran Pasal 27 Ayat (3) io 45 Ayat (1)
d. Tindak Pidana Mendistribusikan Informasi Elektronik yang Memiliki Muatan Pemerasan dan/atau Pengancaman [Pasa127 Ayat (4) 30 45 Ayat (1)
e. Tindak Pidana Sengaja dan Tanpa Hak Menyebarkan Berita Bohong yang Menyebabkan Kerugian Konsumen Transaksi Elektronik dan Menyebarkan Informasi Untuk Menimbulkan Rasa Kebencian atau Permusuhan Pasal 28 jo 45 Ayat (2)
f. Tindak Pidana Sengaja dan Tanpa Hak Mengirimkan Informasi Elektronik yang Berisi Ancaman Kekerasan atau Menakut-nakuti Pasal 29 jo 45 Ayat (3)
g. Tindak Pidana Mengakses Sistem Elektronik Milik Orang Lain Secara Melawan Hukum (Pasal 30 jo 46)
h. Tindak Pidana Intersepsi atau Penyadapan Informasi Elektronik Secara Melawan Hukum (Pasal 31 jo 47)
i. Tindak Pidana Mengubah dll. Informasi Elektronik Secara Melawan Hukum (Pasal 32 jo 48)

j. Tindak Pidana Sengaja Melakukan Tindakan yang Mengakibatkan Terganggunya Sistem Elektronik Secara Melawan Hukum (Pasal 33 jo 49)

k. Tindak Pidana Sengaja Memproduksi dll. Perangkat Komputer dan Sandi Lewat Komputer Secara Melawan Hukum (Pasal 34 jo 50)

l. Tindak Pidana Manipulasi dll. Informasi Elektronik yang Bertujuan Agar Informsi Elektronik Seolah-olah Data yang Otentik Pasal 35 jo 51 Ayat (1)

m. Tindak Pidana ITE di Luar Yuridiksi Indonesia Terhadap Sistem Elektronik yang Berada di Indonesia (Pasal 37)[19]

3. Unsur-Unsur Tindak Pidana Informasi Elektronik dan/atau Dokumen Elektronik

Pasal 28 Ayat 1 UU ITE yang menyatakan bahwa "setiap orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian knsumen dalam transaksi elektronik".

Unsur-Unsur yang terdapat pada pasal 28 ayat (1) UU ITE, yaitu:

1. Unsur obyektif:

a. Setiap orang;

Pengertian setiap orang disini, ditafsirkan sebagai indifidu juga badan hukum yang berbadan hukum sesuai ketentuan perundang-undangan.

b. Sengaja dan tanpa hak; Pengertian

sengaja dan tanpa hak, dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang-undang dan tindakan melalaikan yang diancamkan hukuman.

c. Yang disebarkan adalah berita bohong dan menyelesatkan.

[19] Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik* (Malang, Media Nusa Creativ, 2015), 9.

d. Pengertian berita bohong dan menyesatkan dapat kita tafsirkan dengan kata membujuk sebagai alat melakukan penipuan, yakni karangan perkataan bohong yang mana satu kata bohong tidak cukup.

e. Dari perbuatan tersebut timbul akibat konstitutifnya yaitu kerugian konsumen dalam transaksi elektronik. Adapun perbuatan optimum yang dianggap mengandung sifat ketidakadilan dan berdasarkan sifatnya, yang patut dilarang dan diancam dengan hukuman oleh udang-undang adalah mengakibatkan kerugian konsumen dalam transaksi elektronik.

2. Unsur Subyektif:

a. Unsur kesalahan yaitu dengan sengaja melakukan perbuatan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

b. Melawan hukum tanpa hak. Rumusan unsur-unsur yang terkandung dalam Pasal 28 Ayat (1) UU ITE dan pasal 378 tersebut dapat dipahami mengatur objek yang berbeda.Pasal 378 KUHP mengatur penipuan, sementara Pasal 28 Ayat (1) UU ITE mengatur mengenai barita bohong yang menyebabkan kerugian konsumen dalam transaksi elektronik. Walaupun demikian, yaitu dapat mengakibatkan kerugian bagi orang lain.[20]

Unsur syarat tambahan untuk dapatnya dipidana adalah unsur keadaan-keadaan tertentu yang timbul setelah perbuatan dilakukan, yang menentukan untuk dapat dipidanaya perbuatan. Artinya, bila setelah perbuatan dilakukan keadaan ini tidak timbul, maka perbuatan itu tidak bersifat melawan hukum dan si pembuat tidak dapat dipidana.

Unsur objek dalam hukum tindak pidana seringkali diletakkan dibelakang/sesudah unsur pembuat, missal: unsur mengilangkan nyawa orang lain pada pembunuhan (Pasal 338 KUHP).

---

[20] Siswanto Sunarso*, Hukum Informasi Dan Transaksi Elektronik* (Jakarta, Rineka Cipta, 2009), 99.

Menghilangkan merupakan unsur pembuatan, dan nyawa orang lain adalah objek tindak pidana. Contoh lain: Pasal378, 368, 369 KUHP.

Unsur kualitas subjek hukum tindak pidana adalah unsur kepada siapa rumusan tindak pidana itu ditujukan, misalnya kualitas pegawai negeri pada kejahatan jabatan(Bab XXVIII), orang dewasa (Pasal 292 KUHP), seorang dokter (Pasal 267KUHP), seorang ibu (Pasal 308, 341342 KUHP) dan lain-lain. Unsur syarat tambahan untuk memperingan pidana bukan berupada unsur pokok yang membentuktindak pidana. Ada 2 macam yaitu berifat obyektif (Pasal 373, 379, 352 KUHP), dan bersifat subjektif (Pasal 409 KUHP).[21]

D. Tinjauan Umum Mengenai Kejahatan Skimming

Kejahatan *Skimming* adalah suatu tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada strip magnetik kartu kredit atau debit secara illegal. Melalui *skimmer* para pelaku menduplikasi atau penyadapan data strip magnetik pada kartu ATM, lalu mengubah ke kartu ATM kosong. Proses ini bisa dilakukan dengan cara manual, seperti pelaku kembali ke ATM dan mengambil cip data yang sudah disiapkan sebelumnya. Atau bila menggunakan alat *skimmer* yang lebih canggih, data-data yang telah dikumpulkan dapat diakses dari mana pun secara nirkabel. Dengan menyalin segala informasi yang terdapat pada *strip magnetic* kartu secara *illegal* dan nantinya informasi atau data nasabah tersebut disalin kedalam kartu yang masih kosong. Tak lain tujuan dari kejahatan ini adalah pembobolan dana terhadap nasabah bank tersebut.

Belakangan ini di Indonesia sedang diramaikan dengan berita " pembobolan *ATM". Para nasabah tiba-tiba saja kehilangan saldo rekeningnya akibat dibobol oleh* orang-orang yang tidak bertanggungjawab. Untuk masalah tipu-menipu dan curi-mencuri adalah hal yang sepertinya sudah sangat biasa di Indonesia. Hal ini mungkin diakibatkan oleh kurangnya kesempatan kerja

[21] July Esther dan Anastasia Reni Widiastuti, Hukum Pidana, (Medan, Bina Media Perintis,2019),115.

dan tidak meratanya pendapatan. Berdasarkan data yang ada di TV dan surat kabar. Kasus pembobolan ATM ini di Indonesia (minggu-minggu ini) dimulai dibali, dengan korban nasabah dari lima Bank besar yakni BCA, Bank Mandiri, BNI, BII, dan Bank Permata. Diindikasikan oleh polisi dilakukan dengan teknik *skimmer*.

Modus pembobolan ATM dengan menggunakan *Skimmer* adalah:

1) Pelaku datang ke mesin ATM dan memasangkan *skimmer* kemuluit slot kartu ATM. Biasanya dilakukan saat sepi. Atau biasanya mereka dating lebih dari dua orang dan ikut mengantri. Teman yang dibelakang bertugas untuk mengisi antrian di depan mesin ATM sehingga orang tidak akan memperhatikan dan kemudian memeriksa pemasangan *skimmer*.
2) Setelah dirasa cukup (banyak korban), maka saatnya skimmer dicabut.
3) Inilah saatnya menyalin data ATM yang direkam oleh skimmer dan melihat rekaman no PIN yang ditekan korban.
4) Pada proses ketiga pelaku sudah memliki kartu ATM duplikasi (hasil generate) dan telah memeriksa kevalidan kartu. Kini saatnya untuk melakukan penarikan dana. Biasanya kartu ATM duplikasi disebar melalui jaringannya ke berbagai tempat. Bahkan ada juga yang menjual kartu hasil duplikasi tersebut.[22]

Secara garis besar langkah menghindari *skimmer* adalah sebagai berikut:

1. Kenali mesin ATM yang digunakan dengan baik
2. Gunakan ATM di lokasi yang sama sesering mungkin sehingga akan terlihat jika terjadi perubahan.
3. Perhatikan bila ada hal yang aneh pada mesin ATM seperti goresan, bercak, selotip, bekas lem dan hal-hal mencurigakan lainnya.

[22] Nurdiman Munir, *Pengantar Hukum Siber Indonesia*, (Depok, RajaGrafindo Persada), 2017.205.

4. Jika menemukan perubahan atau keganjilan pada ATM maka segera laporkan kepada pihak Bank dan tunda/jangan lakukan transaksi.
5. Upaya untuk mengakses ATM yang ada di dalam bank atau di lokasi yang ramai, terbuka dan terang untuk meminimalisir resiko.
6. Untuk penggunaan kartu di luar ATM (pada tempat belanja atau restoran) selalu perhatikan yang dilakukan petugas pada kartun dan tanyakan jika asa perilaku yang aneh.
7. Jika digunakan saat belanja, kartu harusnya hanya digesekkan pada mesin resmi dan mesin kasir, tanyakan pada petugas apabila menggesekkan kartu pada alat lain (terutama jika alat itu ada ditempat tersembunyi seperti di balik meja.
8. Untuk pihak Bank sebaiknya mengganti system gesek atau *magnetic script* rawan dibobol pencuri. Bank Indonesia sudah menganjurkan untuk mengganti kartu dengan teknologi chip EMV (Europay Mastercard Visa). Sementara pihak Bank Indonesia juga sudah seharusnya merevisi Peraturan Bank Indonesia Nomor 10/8/PB/2008 Tahun 2007 tentang Peraturan Bank Indonesia Tentang perubahan PBI Nomor 7/52/PB/2005 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Deangan Menggunakan kartu menjadi kartu (*Chip*) dengan system yang lebih aman.[23]

Seluruh tindakan tersebut diatas jelas melanggar berbagai kaidah hukum yang berlaku. Namun untuk melaksanakan tindakan Hukum (khususnya pembuktian) terhadap kejahatan tersebut perlu dipahami terlebih dahulu bahwa pada dasarnya hukum terbagi dua yaitu Hukumperdata (hukum privat) dan Hukum Pidana (hukum publik). Kedua jenis hukum tersebut

[23] Resa Raditio, Aspek Hukum Transaksi Elektronik Perikatan, Pembuktian, dan Penyesesaian Sengketa,(Yogyajarta, Graha Ilmu, 2014), 22.

adalah hukum materil atau kaidah yang menentukan dan menentukan dan mengatur hak-hak dan kewajiban

BAB III

METOLOGI PENILITIAN

A. Ruang Lingkup Penelitian

Penelitian merupakan terjemahan dari bahasa Inggris, yaitu *research*. Kata research berasal dari *re* (kembali) dan to *seacrh* (mencari). *Reseacrh* berarti mencari kembali. Oleh karena itu penelitian berhubungan dengan upaya pencarian pengetahuan benar. Penelitian merupakan suatu sarana pokok dalam pengembangan ilmu pengetahuan maupun teknologi oleh, karena itu penelitian bertujuan umtuk mengungkapkan kebenaran sistematis, metodologis, dan konsisten. Melalui proses penelitian tersebut diadakan analisis dan kontruksi terhadap bahan yang telah dikumpulkan dan diolah.

Ruang lingkup penilitian bertujuan untuk membatasi permasalahan yang akan dibahas di dalam penelitian ini. Adapun ruang lingkup penelitian dalam penulisan ini adalah bagaimana pertanggungjawaban tindak pidana melakukan kejahatan dengan sengaja atau tanpa hak melawan hukum, melakukan penyadapan terhadap informasi elektronik dan/atau dokumen elektronik dalam Putusan No.282/Pid.Sus/2020/PN.MKS)

B. Jenis Penilitian

Jenis penilitian ini adalah hukum normatif, penelitian hukum normative (*Normativ law search*) adalah metode yang dilakukan dengan cara meneliti bahan-bahan pustaka, yaitu buku, jurnal, artikel-artikel resmi, menelusuri doktrin-doktrin dan teori hukum dari berbagai literature dan peraturan perundang-undangan yang 26 u dan berkaitan dengan permasalahan yang dibahas.[24]

C. Metode Pendekatan Masalah

1. Metode Pendekatan Perundang-undangan (*statue approach)* yaitu dilakukan dengan menelaah ketentuan Perundang-undangan yang berlaku dalam kasus tersebut yaitu Undang-Undang no 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
2. Metode Pendekatan Kasus (*case approach*) yaitu dengan cara menganalisis Putusan Nomor 282/Pid.Sus/2020/PN MKS.[25]

D. Sumber Bahan Hukum

Dalam penilitian ini, penulis memperoleh data dari dua sumber bahan hukum, yaitu bahan hukum primer dan bahan hukum sekunder

a. Bahan Hukum Primer Bahan hukum primer adalah bahan hukum yang memiliki otoritas. Bahan hukum primer adalah penelitian ini terdiri dari peraturan perundang-undangan yang meniliki kaitan dengan permasalahan yang dibahas dalam penelitian yaitu Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dann Undang-undang Nomor Tahum 1981 tentang hukum Acara Pidana.

[24] Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Pranada Media Grup, 2015) Hal.181.
[25]Ibid,Hal.181.

b. Bahan Hukum Sekunder

Bahan hukum sekunder yang paling utama adalah buku-buku hukum, kamus hukum dan jurnal hukum.

E. Metode Penelitian

Penelitian ini mengunakan metode analisis yang dilakukan untuk mengumpulkan dan cara studi kepustakaan. Penelitian kepustakaan (*library research*) yaitu penelitian yang dilakukan dengan cara meneliti bahan pustaka atau buku-buku baik koleksi pribadi maupun dari perpustakaan, artikel resmi dari media cetak dan media elektronik, menelusuri pendapat hukum atau doktrin atau teori-teori yang diperoleh dari riteratur hukum dan peraturan Perundang-undangan yang berkaitan dengan judul skripsi.

F. Analisis Bahan Hukum

Bahan hukum yang dilakukan dalam penelitian ini adalah secara kualitatif yaitu penelitian yang mengacu pada norma hukum yang terdapat pada Peraturan Perundang-undangan dan analisis terhadap Putusan Nomor 282/Pid.Sus/2020/PN.MKS yaitu tentang Pertanggungjawaban Pidana Melalui Penyadapan Terhadap Informasi Elektronik Dan Atau Dokumen Elektronik Melalui Kejahatan Skimming. Kemudian dilakukan pembahasan dan penafsiran yang ada pada akhirnya dapat ditarik kesimpulan tentang masalah-masalah yang diteliti.