

**TINJAUAN YURIDIS TINDAK PIDANA PENCURIAN  
DATA NASABAH PERBANKAN MELALUI  
ANJUNGAN TUNAI MANDIRI**

**SKRIPSI**

**Diajukan Untuk Memenuhi Syarat  
Mendapatkan Gelar Sarjana Hukum**

**Oleh :**

**MHD. WAIS AL-QADRI**

**1806200035**



**FAKULTAS HUKUM**

**UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**

**MEDAN**

**2023**



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH  
**UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**  
**FAKULTAS HUKUM**

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 99/SK/BAN-PT/Akred/PT/III/2019  
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003  
<http://fahum.umsu.ac.id> [fahum@umsu.ac.id](mailto:fahum@umsu.ac.id) [umsumedan](#) [umsumedan](#) [umsumedan](#) [umsumedan](#)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

### KARTU BIMBINGAN SKRIPSI MAHASISWA

NAMA : MHO. WAIS AL-QABRI Z.S  
NPM : 1806200035  
PRODI/BAGIAN : Ilmu Hukum / Hukum PIDANA  
JUDUL SKRIPSI : TINJAUAN YURIDIS TINDAK PIDANA PENCURIAN  
DATA NASABAH PERBANKAN MELAWI ANJUNGAN  
TUNAI MANDIRI  
Pembimbing : RACHMAD ABOUH, S.H., M.H.

TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
19-09-2022	Pegangan Judul.	[Signature]
11-11-2022	Perbaikan Proposal.	[Signature]
26-12-2022	Seminar proposal.	[Signature]
28-01-2023	Perbaikan Kerangka Skripsi.	[Signature]
03-02-2023	Kamus Perakata (Perbaikan)	[Signature]
12-02-2023	Keanggotaan Interaktif	[Signature]
29-02-2023	Keanggotaan Perbaikan	[Signature]
07-03-2023	Penyempurnaan Skripsi	[Signature]
10-3-2023	All uida dihidangkan	[Signature]

Diketahui,  
DEKAN FAKULTAS HUKUM

[Signature]  
(Dr. FAISAL, SH., M.Hum)

DOSEN PEMBIMBING

[Signature]  
(RACHMAD ABOUH, S.H.M.H.)



MAJLIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PESAT MUHAMMADIYAH  
**UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**  
**FAKULTAS HUKUM**

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019  
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003  
<http://fahum.umsu.ac.id> [fahum@umsu.ac.id](mailto:fahum@umsu.ac.id) [f umsumedan](#) [ig umsumedan](#) [t umsumedan](#) [y umsumedan](#)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**BERITA ACARA**  
**UJIAN MEMPERTAHANKAN SKRIPSI SARJANA BAGI**  
**MAHASISWA PROGRAM STRATA I**

Panitia Ujian Sarjana Strata-I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Rabu tanggal 10 Mei 2023 Jam 08.30 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan, menimbang:

**MENETAPKAN**

NAMA : MHD. WAIS AL-QADRI ZS  
NPM : 1806200035  
PRODI/BAGIAN : HUKUM/ HUKUM PIDANA  
JUDUL SKRIPSI : TINJAUAN YURIDIS TINDAK PIDANA PENCURIAN  
DATA NASABAH PERBANKAN MELALUI ANJUNGAN  
TUNAI MANDIRI

Dinyatakan : ( A ) Lulus Yudisium dengan predikat Lebih Baik  
( ) Lulus Bersyarat, memperbaiki/ujian ulang  
( ) Tidak Lulus

Setelah lulus, dinyatakan berhak dan berwenang mendapatkan gelar Sarjana Hukum (SH) dalam Bagian Hukum Pidana

**PANITIA UJIAN**

Ketua

Dr. FAISAL, S.H., M.Hum  
NIDN: 0122087502

Sekretaris

Dr. ZAINUDDIN, S.H., M.H  
NIDN: 0118047901

**ANGGOTA PENGUJI:**

1. RAHMAT RAMADHANI, SH., M.H.
2. Assoc. Prof. Dr. ADI MANSAR, S.H., M.Hum.
3. RACHMAD ABDUH, S.H., M.H.

1.

2.

3.



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH  
**UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**  
**FAKULTAS HUKUM**

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019  
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003  
<http://fahum.umsu.ac.id> [fahum@umsu.ac.id](mailto:fahum@umsu.ac.id) [umsumedan](#) [umsumedan](#) [umsumedan](#) [umsumedan](#)

### PERNYATAAN KEASLIAN SKRIPSI

Saya saya bertanda tangan di bawah ini:

Nama : **MHD. WAIS AL QADRI ZS**  
NPM : 1806200035  
Program : Strata-1  
Fakultas : Hukum  
Program Studi : Hukum  
Bagian : Hukum Pidana  
Judul Skripsi : **TINJAUAN YURIDIS TINDAK PIDANA PENCURIAN  
DATA NASABAH PERBANKAN MELALUI ANJUNGAN  
TUNAI MANDIRI**

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis, secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Dan apabila ternyata dikemudian hari data-data dari skripsi ini merupakan hasil Plagiat atau merupakan hasil karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik dari Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Saya yang menyatakan

**MHD. WAIS AL QADRI ZS**



**UMSU**  
Unggul | Cerdas | Terpercaya

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH  
**UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**  
**FAKULTAS HUKUM**

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 39/SK/BAN-PT/Akred/PT/III/2019  
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003  
<http://fahum.umsu.ac.id> [fahum@umsu.ac.id](mailto:fahum@umsu.ac.id) [umsumedan](#) [umsumedan](#) [umsumedan](#) [umsumedan](#)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ


### LEMBAR PERSETUJUAN PEMBIMBING

NAMA : MHD. WAIS AL QADRI ZS  
NPM : 1806200035  
PRODI/BAGIAN : HUKUM/ HUKUM PIDANA  
JUDULSKRIPSI : TINJAUAN YURIDIS TINDAK PIDANA PENCURIAN  
DATA NASABAH PERBANKAN MELALUI ANJUNGAN  
TUNAI MANDIRI

DISETUJUI UNTUK DISAMPAIKAN KEPADA  
PANITIA UJIAN SKRIPSI

Medan, Maret 2023

DOSEN PEMBIMBING

  
**RACHMAD ABDUH, S.H., M.H**  
NIDN : 9901114882

Unggul | Cerdas | Terpercaya



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PEMERINSAH PUSAT MUHAMMADIYAH  
**UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**  
**FAKULTAS HUKUM**

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019  
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003  
<http://fahum.umsu.ac.id> [fahum@umsu.ac.id](mailto:fahum@umsu.ac.id) [umsumedan](#) [umsumedan](#) [umsumedan](#) [umsumedan](#)



## PENDAFTARAN UJIAN SKRIPSI

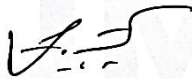
Pendaftaran Skripsi Sarjana Strata I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, bagi:

NAMA : MHD. WAIS AL QADRI ZS  
NPM : 1806200035  
PRODI/BAGIAN : HUKUM/ HUKUM PIDANA  
JUDUL SKRIPSI : TINJAUAN YURIDIS TINDAK PIDANA PENCURIAN DATA  
NASABAH PERBANKAN MELALUI ANJUNGAN TUNAI  
MANDIRI  
PENDAFTARAN : Tanggal, 29 MARET 2023

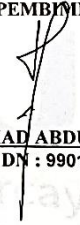
Dengan diterimanya Skripsi ini, sesudah lulus dari Ujian Skripsi penulis berhak memakai gelar: HUKUM PIDANA

## SARJANA HUKUM (S.H)

Diketahui  
DEKAN FAKULTAS HUKUM

  
Dr. FAISAL, S.H., M.Hum.  
NIDN: 0122087502

PEMBIMBING

  
RACHMAD ABDUH, S.H., M.H  
NIDN : 9901114882

Unggul | Cerdas | Terpercaya

## KATA PENGANTAR



### ***Assalamu'alaikum Warahmatullahi Wabarakatuh***

Pertama-tama disampaikan rasa syukur kehadiran Allah SWT yang maha pengasih lagi maha penyayang atas segala rahmat dan karuniaNya sehingga skripsi ini dapat diselesaikan. Skripsi merupakan salah satu persyaratan bagi setiap mahasiswa yang ingin menyelesaikan studinya di Fakultas Hukum Muhammadiyah Sumatera Utara. Sehubungan dengan itu, disusun skripsi yang berjudul “Tinjauan Yuridis Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri”

Dengan selesainya skripsi ini, perkenankanlah diucapkan terimakasih yang sebesar-besarnya kepada: Rektor Universitas Muhammadiyah Sumatera Utara Bapak Prof. Dr. Agussani., M.AP atas kesempatan dan fasilitas yang diberikan kepada kami untuk mengikuti dan menyelesaikan pendidikan program Sarjana ini. Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Bapak Dr. Faisal, S.H.,M.Hum. atas kesempatan menjadi mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Demikian juga halnya kepada Wakil Dekan I Bapak Dr. Zainuddin, S.H.,M.H. dan Wakil Dekan III Ibu Atikah Rahmi, S.H.,M.H.

Terimakasih yang tak terhingga dan penghargaan yang setinggi-tingginya diucapkan kepada Bapak Rachmad Abduh, S.H., M.H. selaku Pembimbing, dan

Bapak Rahmat Ramadhani, S.H., M.H. selaku Pembanding, yang dengan penuh perhatian telah memberikan dorongan, bimbingan dan arahan sehingga skripsi ini selesai. Disampaikan juga penghargaan kepada seluruh staf pengajar Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Teristimewa kepada Ayah Tersayang Zulyantoni, S.E. dan Mama Leni Marlina, S.E yang telah membesarkan, mengasuh dan memberikan semangat sehingga penulis dapat menyelesaikan skripsi ini. Terima kasih kepada Adik Lidya Syahfitri dan Mhd. Fikri Haikal yang sedang berjuang untuk melanjutkan pendidikan nya ke Universitas yang ia inginkan yang telah memberikan semangat kepada penulis untuk menyelesaikan skripsi ini.

Tiada gedung yang paling indah, kecuali persahabatan, untuk itu, dalam kesempatan diucapkan terimakasih kepada sahabat-sahabat yang telah banyak membantu saya terutama kepada sahabatku Muammar Zein, Yasser Atmanegara, Rizky Ananda Pratama, Arya Alvesaldy, Farhan At Thariq Achmad sebagai tempat curahan hati selama ini dalam menyelesaikan penulisan skripsi ini.

Akhirnya, Tiada gading yang tak retak, retaknya gading karena alami, tiada orang yang tak bersalah, kecuali ilahi Rabbi. Mohon maaf atas segala kesalahan semua ini, begitupun disadari bahwa skripsi ini jauh dari sempurna. Untuk itu, diharapkan ada masukan yang membangun untuk kesempurnaannya. Terima kasih semua, tiada lain yang diucapkan selain kata semoga kiranya mendapat balasan dari Allah SWT Aamiin. Sesungguhnya Allah maha mengetahui akan niat baik hamba-hambanya.



*Assalamu'alaikum Warahmatullahi Wabarakatuh*

Medan, 13 Februari 2023

Hormat Saya

Penulis,

Mhd. Wais Al-Qadri

1806200035

## ABSTRAK

### TINJAUAN YURIDIS TINDAK PIDANA PENCURIAN DATA NASABAH PERBANKAN MELALUI ANJUNGAN TUNAI MANDIRI

Kemajuan teknologi berjalan sedemikian rupa sehingga dalam perkembangannya juga menimbulkan celah bagi pelaku kejahatan dalam menggunakan metode kejahatan yang lebih canggih juga. Kemajuan teknologi informasi menimbulkan evolusi yang mengarah kepada fasilitas perbankan digital. Fasilitas ini bertujuan meningkatkan efisiensi kegiatan operasional dan mutu pelayanan bank kepada nasabahnya. Perkembangan teknologi tentu memudahkan beraktivitas para nasabah bank. Kehadiran teknologi yang semakin hari semakin canggih membuat aktivitas nasabah perbankan menjadi mudah. Perkembangan teknologi ini tidak hanya memberikan kemudahan bagi nasabah tapi juga dibarengi dengan aspek negatif yaitu menimbulkan modus baru dalam kasus pencurian dana nasabah dengan metode *skimming*. *Skimming* adalah salah satu jenis kejahatan siber yang berkembang saat ini lebih khususnya kejahatan terhadap privasi seseorang (*Infringments of Privasi*). *Skimming* adalah tindakan pencurian informasi kartu kredit atau debit dengan cara mengcopy informasi yang terdapat pada strip magnetik kartu secara ilegal.

Penelitian ini menggunakan hukum normatif (*Yuridis Normatif*). Dimana dalam Penelitian ini hukum dikonsepsikan sebagai apa yang bertuliskan peraturan perundang-undangan (*law in book*), Penelitian hukum normatif ini didasarkan kepada bahan hukum primer dan sekunder, yaitu penelitian yang mengacu kepada norma-norma yang terdapat dalam peraturan perundang-undangan tertentu atau hukum tertulis.

metode yang dilakukan pelaku kejahatan bagian perbankan untuk mencuri data-data nasabah yang terdapat dalam kartu ATM nasabah. Modusnya dengan cara memasang alat skimmer pada slot untuk memasukan kartu ATM pada mesin ATM. Sedangkan ATM adalah salah satu alat elektronik atau sistem elektronik yang digunakan dalam langkah perbankan. Dasar hukum pada kejahatan tindak pidana skimming yaitu: Pasal 55 ayat (1) KUHP, Pasal 362 KUHP, Pasal 2 ayat (1) Undang-Undang No. 8 Tahun 2010, Pasal 5 ayat (1) UU Nomor. 8 Tahun 2010, Pasal 30 ayat (1) UU Nomor. 11 Tahun 2008, Pasal 30 ayat (3) UU Nomor. 11 Tahun 2008, Pasal 32 ayat (2) Undang-Undang No. 11 Tahun 2008, Pasal 32 ayat (3) UU Nomor. 11 Tahun 2008, Pasal 36 UU Nomor. 11 Tahun 2008, Pasal 81 UU Nomor. 3 Tahun 2011, Pasal 83 ayat (1) UU Nomor. 3 Tahun 2011, Pasal 83 ayat (2) UU Nomor. 3 Tahun 2011, UU No. 10 Tahun 1998 tentang Perbankan, UU No. 36 Tahun 1999 tentang Telekomunikasi.

Kata Kunci: *Tindak Pidana, Perbankan, Skimming*

## DAFTAR ISI

KATA PENGANTAR .....	i
ABSTRAK .....	iv
DAFTAR ISI .....	v
<b>BAB I PENDAHULUAN</b>	
<b>A. Latar Belakang.....</b>	<b>1</b>
1. Rumusan Masalah .....	13
2. Faedah Penelitian .....	14
<b>B. Tujuan Penelitian.....</b>	<b>15</b>
<b>C. Defenisi Operasional .....</b>	<b>15</b>
<b>D. Keaslian Penelitian.....</b>	<b>19</b>
<b>E. Metode Penelitian.....</b>	<b>19</b>
1. Jenis Dan Pendekatan Penelitian.....	19
2. Sifat Penelitian .....	20
3. Sumber Data .....	21
4. Alat Pengumpulan Data.....	23
5. Analisis Data.....	24
<b>BAB II TINJAUAN PUSTAKA</b>	
1. Tinjauan Tentang Tindak Pidana .....	26
2. Pengertian <i>Cybercrime</i> .....	28
3. Pengertian Perbankan.....	29
4. Pengertian Anjungan Tunai Mandiri.....	31
<b>BAB III HASIL PENELITIAN DAN PEMBAHASAN</b>	
A. Modus Operandi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri.....	33
B. Pengaturan Hukum Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri.....	48

C. Tinjauan Yuridis Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri .....	59
<b>BAB IV KESIMPULAN DAN SARAN</b>	
A. Kesimpulan.....	67
B. Saran.....	68
<b>DAFTAR PUSTAKA .....</b>	<b>69</b>

# BAB I

## PENDAHULUAN

### A. Latar Belakang

Dewasa ini, Perkembangan progress teknologi telah memberikan dampak yang signifikan terhadap kehidupan social. Di sekujur dunia, teknologi menawarkan banyak sarana yang terutama melalui konektivitas internet.<sup>1</sup> Pemanfaatan teknologi internet sudah begitu banyak merambah pada bidang kehidupan masyarakat, terutama merambah kebidang hukum. Hasil survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) yang dapat dilihat dalam laman [statistic.apjii.or.id](http://statistic.apjii.or.id), tertatah pada Tahun 2017 jumlah pemakai internet di Indonesia mencapai 143,26 juta jiwa. Angka tersebut meningkat dibandingkan pada tahun 2016 yang sampai 132,7 juta jiwa.<sup>2</sup> Internet sudah menjadi salah satu kewajiban dalam kehidupan saat ini. Kemudahan yang ditawarkan Internet semakin membuat manusia menjadi terlalai. Internet menghubungkan setiap penggunanya. Tidak ada batasan waktu, wilayah ataupun gender. Teknologi Informasi saat ini seolah-olah menjadi pedang bermata dua, karena selain memberikan manfaat bagi peningkatan kemajuan, kesejahteraan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

---

<sup>1</sup> Sinta Dewi Rosadi. 2015. Cyberlaw “*Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*”, Bandung: PT Refika Aditama, halaman 4.

<sup>2</sup> Faisal Riza, Rachmad Abduh. 2019. *Alternatif Penyelesaian Sengketa Secara Arbitrase Melalui Pemanfaatan Teknologi Informasi*. Jurnal De Lega Lata. Vol. 4 No. 1. halaman 78. <http://jurnal.umsu.ac.id/index.php/delegalata/article/view/3171/2888>

Kepentingan akan teknologi jaringan komputer semakin meningkat dari waktu ke waktu. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunitas komersial menjadi bagian terbesar dan pesat pertumbuhannya serta menembus berbagai batas Negara. Bahkan melalui jaringan ini, segala macam informasi di dunia bisa diketahui selama 24 jam. Melalui dunia internet atau bisa disebut juga *cyberspace*, apapun dapat dilakukan. Segi positif dari dunia maya ini tentu saja akan menambah trend dalam perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Akan tetapi dampak negatif pun tidak bisa dihindari. Sejalan dengan berkembangnya teknologi internet, menyebabkan munculnya kejahatan yang disebut dengan *cybercrime* atau kejahatan melalui jaringan internet.

Munculnya beberapa kasus *cybercrime* atau kejahatan melalui jaringan internet, seperti pencurian kartu kredit, hacking beberapa situs, kejahatan phishing, kejahatan skimming. Sehingga dalam kejahatan *Cybercrime* dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki Komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya *cybercrime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet.<sup>3</sup>

---

<sup>3</sup> Alcianno G. Gani. 2018. Cybercrime “Kejahatan Berbasis Komputer”. Jurnal Sistem Informasi. Vol. 5 No. 1, halaman 17.

<https://journal.universitassuryadarma.ac.id/index.php/jsi/article/view/18>

Sebutan kejahatan siber menunjukkan bahwa bentuk kejahatan ini hanya dapat dilakukan dengan perangkat atau alat yang menghasilkan realita siber seperti sistem dan rangkaian komputer yang terkoneksi dengan internet.

Dalam dua dokumen Kongres PBB tentang hal *The Prevention of Crime and the Treatment of Offenders di Havana, Cuba* pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal<sup>4</sup>:

1. *Cybercrime* dalam arti sempit disebut *computer crime*, yaitu perilaku ilegal atau melanggar secara langsung menyerang system keamanan suatu computer atau data yang diproses oleh komputer
2. *Cybercrime* dalam arti luas disebut *computer related crime*, yaitu perilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dari beberapa pendapat diatas, secara singkat dapat dikatakan bahwa *cybercrime* dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. *Cybercrime* ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia IT khususnya media internet.

Maraknya tindak kriminal di dunia maya tergantung dari sejauh mana sumber daya baik berupa hardware/software maupun pengguna teknologi yang bersangkutan mempunyai pengetahuan dan kesadaran tentang pentingnya keamanan di dunia maya, seorang penyedia layanan/target *Cybercrime* harus

---

<sup>4</sup> Eddy Army. 2020. *Bukti Elektronik Dalam Praktik Peradilan*, Jakarta: Sinar Grafika , halaman 175.

mempunyai pengetahuan yang cukup tentang metode yang biasanya seorang *cybercrime* lakukan dalam menjalankan aksinya.<sup>5</sup>

Dalam *Cybercrime* terdapat dua bentuk perbedaan, yaitu:<sup>6</sup>

1. Kejahatan yang menggunakan teknologi informasi sebagai fasilitas. Bentuk ini menjadikan fasilitas teknologi sebagai instrumen untuk melakukan kejahatan. Dalam arti teknologi komputer dan jaringan dijadikan sebagai alat untuk melakukan kejahatan pencurian identitas terhadap nasabah pengguna *e-banking*. Misalnya pembajakan (*copyright* atau hak cipta intelektual dan lain-lain), pornografi, pemalsuan dan pencurian kartu kredit (*carding*), penipuan melalui e-mail, penipuan dan pembobolan rekening bank, perjudian online, situs sesat, dan materi-materi internet yang memuat kebencian yang berkaitan dengan SARA (suku agama ras dan golongan) dan transaksi dan penyebaran obat terlarang serta transaksi seks (*prostitusi cyber*).
2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran. Bentuk ini bukan memanfaatkan teknologi komputer dan internet sebagai media atau instrumen untuk melakukan kejahatan, namun menjadikannya sebagai sasaran, misalnya kejahatan

---

<sup>5</sup> Eliasta Ketaren. 2016. Cybercrime “*Cyber Space, dan Cyber Law*”. Jurnal Times, Vol. V No. 2. halaman 36. <https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/556>

<sup>6</sup> Waldi Nopriansyah. 2019. *Aspek Hukum Perbankan Syariah di Indonesia*, Jakarta: Prenadamedia. halaman 136.



pengaksesan suatu sistem secara ilegal (*hacking*), perusakan situs internet dengan virus dan server data (*cracking*) serta defacing.<sup>7</sup>

Dalam menjalankan kejahatan *cybercrime* terdapat motif dan timbulnya kejahatan tersebut yang dimana Motif berasal dari bahasa Latin *movere* yang berarti bergerak atau *to move*. Karena itu motif diartikan sebagai kekuatan yang terdapat dalam diri organisme yang mendorong untuk berbuat atau merupakan *driving force*. Motif kadang juga disebut sebagai alasan dasar atau sesuatu yang mendorong seseorang melakukan sesuatu. Dalam dunia siber, motif pelaku *cybercrime* dapat dikelompokkan menjadi dua, yaitu:<sup>8</sup>

- a. Motif intelektual. Motif ini bertujuan mendapatkan kepuasan pribadi atau intelektual dan menunjukkan bahwa dirinya telah mampu untuk merekayasa dan mengimplementasikan ilmu bidang teknologi informasi. Kejahatan dengan motif ini umumnya dilakukan secara individual. Dalam dunia *cybercrime* individu yang melakukan motif ini disebut hacker golongan putih.
- b. Motif ekonomi, politik dan kriminal. Motif ini bertujuan untuk mendapatkan keuntungan pribadi khususnya bidang ekonomi dan politik. Kejahatan dengan motif ini bersifat individu dan kelompok (korporasi). Di perbankan motif ini disebut motif ekonomi karena hacker bertujuan mencuri identitas nasabah guna menguras dana nasabah. Dalam dunia *cybercrime* pihak ini disebut hacker golongan hitam.

---

<sup>7</sup> *Ibid.* halaman 137.

<sup>8</sup> *Ibid*

Kemunculan hacker adalah dampak dari sistem globalisasi dunia, di mana setiap transaksi keuangan dan non-keuangan dapat menggunakan teknologi komputer, sehingga arus besar itu memaksa orang untuk menggunakan teknologi, sehingga hal ini memicu kelahiran *cybercrime*.

Faktor ini dapat dibagi menjadi dua aspek, yaitu:<sup>9</sup>

- a. Faktor teknologi. Keberadaan teknologi akan menghilangkan batas wilayah negara dan menjadikan dunia terasa dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya. Di samping itu, tidak meratanya penyebaran teknologi menjadikan pihak yang satu lebih kuat daripada yang lain. Sehingga muncul ungkapan: "siapa menguasai teknologi maka dia menguasai dunia."
- b. Faktor sosio-ekonomi. *Cybercrime* dapat dipandang sebagai produk ekonomi. Keamanan jaringan merupakan isu global yang dihubungkan dengan kejahatan tersebut dan muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Melihat kenyataan itu, *cybercrime* berada dalam skenario besar dari kegiatan ekonomi dunia.

*Cyberlaw* sebagai suatu Pemerintahan Hukum yang baru akan lebih memudahkan untuk dipahami dengan mengetahui ruang lingkup pengaturannya.

---

<sup>9</sup> *Ibid*

*Cyberlaw* dengan bentuk pengaturan yang bersifat khusus (*sui generis*) atas kegiatan-kegiatan di dalam *Cyber Space*, antara lain mencakup<sup>10</sup>:

1. Hak Cipta (*Copyright*)
2. Merek (*Trademark*)
3. Fitnah atau pencemaran nama baik (*Defamation*)
4. *Privacy*
5. *Duty Of Care*

Pembentuk UU ITE telah memfokuskan bahwa pemerintah perlu mendukung ekspansi teknologi informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk menangkal penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya, masyarakat Indonesia. Pendeknya, pada titik ini pemerintah mengharapkan bahwa dengan hadirnya UU ITE diharapkan dapat mencegah penyalahgunaan teknologi informasi. Dengan kata lain, mencegah terjadinya tindak pidana melalui informasi dan transaksi elektronik.

Agar tindak pidana siber tidak mudah terjadi, Pasal 3 UU ITE memfokuskan masyarakat agar menjunjung tinggi beberapa asas, antara lain: kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Asas-asas tersebut diharapkan dapat dijadikan panduan atau pedoman bagi masyarakat atau warga negara asing yang berdomisili di Indonesia ketika

---

<sup>10</sup> Danrivanto Budhijanto. 2017. Revolusi Cyberlaw Indonesia “*Pembaruan dan Revisi Undang-undang Informasi dan Transaksi Elektronik 2016*”, Bandung: PT Refika Aditama. halaman 2.

akan menggunakan internet dalam melakukan suatu aktivitas tertentu sehingga bisa dihindari terjadinya penyalahgunaan yang dapat menimbulkan permasalahan hukum di kemudian hari.

Apabila memperhatikan UU ITE, secara normatif, terdapat larangan penyalahgunaan komputer atau sistem elektronik, diantaranya<sup>11</sup>:

1. Pasal 30 ayat 1, menerangkan mengenai larangan bagi setiap orang menggunakan atau mengakses komputer dan sistem elektronik milik orang lain dengan cara apa pun, sedangkan dalam ayat 2, lebih mengarah kepada larangan peretasan diantaranya melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya;
2. Pasal 31, bahwa segala macam bentuk pemantauan, gangguan, pendokumentasian (merekam) yang dilakukan “tanpa ijin” merupakan tindakan yang dilarang.

Hukum Pidana adalah keseluruhan dari peraturan-peraturan yang menentukan perbuatan apa yang dilarang dan termasuk ke dalam tindak pidana, serta menentukan hukuman apa yang dapat dijatuhkan terhadap yang melakukannya.<sup>12</sup>

Penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktifitasnya di sisi lain memudahkan bagi pihak-pihak tertentu melakukan suatu perbuatan tindak pidana. Salah satunya perbuatan

---

<sup>11</sup> Hariman Satria. 2022. *Hukum Pidana Khusus*, Depok: Rajawali Pers. halaman 487.

<sup>12</sup> Kamri Ahmad dan Andi Khaedhir. 2022. *Pengantar Hukum Indonesia*, Depok: Rajawali Pers. halaman 119.

Tindak Pidana Formil (Delik Formil) yang dimana delik tersebut mengarah pada perbuatan. Misalnya Pasal 362 KUHP tentang Pencurian.<sup>13</sup>

Perbankan merupakan segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya. Berdasarkan penjelasan tersebut, dapat dikatakan bahwa sistem perbankan merupakan suatu system yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara, dan proses melaksanakan kegiatan usahanya secara keseluruhan.

Mengenai bagaimana system perbankan di Indonesia tentu segala sesuatunya dapat dilihat dalam Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998.<sup>14</sup>

Lembaga perbankan adalah lembaga yang berdiri pada kepercayaan masyarakat sehingga dikenal adanya kerahasiaan bank. Konsekuensinya apabila masyarakat sudah tidak mempercayai lagi suatu bank, bank tersebut akan sensitif terhadap gempuran masyarakat yang menarik dana sehingga berpotensi merugikan bank. Kemajuan pesat Teknologi Informasi (TI) dan globalisasi mendukung bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya melalui media elektronik atau dikenal dengan *Electronic Banking (e-banking)*. *E-banking* merupakan layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan

---

<sup>13</sup> Faisal. 2021. Hukum Pidana “*Dalam dinamika asas, teori, dan pendapat ahli pidana*”, Jakarta: Kencana. halaman 87.

<sup>14</sup> Hermansyah. 2020. *Hukum Perbankan Nasional Indonesia*, Jakarta: Kencana. halaman 30.

komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti Automatic Teller Machine (ATM).

Dasar Hukum Pencurian disyari'atkan berdasarkan Al-Qur'an dan Hadist:

1) Al-Qur'an

ارْقُؤْ أَيْدِيَهُمَا فِئْفِقُوا أَوْ السَّارِقَ فَتُؤَالِسْ جَزَاءُ بِمَا كَسَبَا نَكَالًا اللَّهُ عَزِيزٌ حَكِيمٌ

Artinya:

“Adapun orang laki-laki maupun perempuan yang mencuri, potonglah tangan keduanya (sebagai) balasan atas perbuatan yang mereka lakukan dan sebagai siksaan dari Allah. Dan Allah Maha perkasa, Maha bijaksana”<sup>15</sup>.

2) Hadist

" tidak, sungguh, aku melihatnya dineraka karena pakaian yang dia ambil dari harta rampasan perang yang belum di bagikan." (HR. Al-Bukhari dan Muslim)<sup>16</sup>

ATM atau yang lebih dikenal dengan nama Anjungan Tunai Mandiri merupakan suatu bentuk terminal/mesin komputer yang terhubung dengan jaringan komunikasi bank, yang memungkinkan nasabah melakukan transaksi keuangan secara mandiri tanpa bantuan dari teller ataupun petugas bank lainnya. Kartu ATM merupakan kartu plastik yang dilengkapi dengan magnetic stripe. Pada magnetic stripe akan terekam secara elektronik. ATM sering ditempatkan di

<sup>15</sup> Alqur'an Q.S. Al-Ma'idah : 38, Semarang : PT. Karya Toha Putra.

<sup>16</sup> Syamsul Rizal Hamid. 2017. *1500 Hadist dan Sunnah Pilihan*, Jakarta : Kaysa Media. halaman 313.

lokasi-lokasi strategis, seperti restoran, pusat perbelanjaan, bandar udara, stasiun kereta api, terminal bus, pasar swalayan, dan kantor-kantor bank itu sendiri. Kartu ATM adalah jenis alat pembayaran dengan menggunakan kartu (APMK) yang dapat digunakan untuk melakukan penarikan tunai atau pemindahan dana .

Kemajuan teknologi berjalan sedemikian rupa sehingga dalam perkembangannya juga menimbulkan celah bagi pelaku kejahatan dalam menggunakan metode kejahatan yang lebih canggih juga. Kemajuan teknologi informasi menimbulkan evolusi yang mengarah kepada fasilitas perbankan digital. Fasilitas ini bertujuan meningkatkan efisiensi kegiatan operasional dan mutu pelayanan bank kepada nasabahnya. Perkembangan teknologi tentu memudahkan beraktivitas para nasabah bank. Kehadiran teknologi yang semakin hari semakin canggih membuat aktivitas nasabah perbankan menjadi mudah. Perkembangan teknologi ini tidak hanya memberikan kemudahan bagi nasabah tapi juga dibarengi dengan aspek negatif yaitu menimbulkan modus baru dalam kasus pencurian dana nasabah dengan metode skimming.

*Skimming* adalah salah satu jenis kejahatan siber yang berkembang saat ini lebih khususnya kejahatan terhadap privasi seseorang (*Infringments of Privasi*). *Skimming* adalah tindakan pencurian informasi kartu kredit atau debit dengan cara mengcopy informasi yang terdapat pada strip magnetik kartu secara ilegal. Strip ini adalah garis lebar hitam yang berada di bagian belakang kartu ATM. Fungsinya kurang lebih seperti pita kaset, material feromagnetik yang dapat dipakai untuk menyimpan data. Pelaku bisa mendapatkan data nomor kartu kredit atau debit korban dengan menggunakan perangkat elektronik kecil (*skimmer*)

untuk menggesek kartu lalu menyimpan ratusan nomor kartu kredit korban. Melalui skimmer para pelaku menduplikasi data strip magnetik pada kartu ATM lalu mengganda 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. Kartu baru hasil yang digandakan memungkinkan para pelaku untuk mengeluarkan uang dari rekening secara biasa. Korban skimming sering tidak menyadari bahwa kartunya telah terduplikasi sampai mereka melihat tarikan yang tidak dilakukan di rekening mereka. Selain di mesin ATM, kejahatan *skimming* juga bisa menyerang pengguna internet banking. Saat menggunakan internet banking hindari penggunaan jaringan WiFi publik. Hal ini untuk mengurangi risiko pencopian data oleh pelaku *skimming*.<sup>17</sup>

Sebagai contoh kasus kejahatan *skimming* yang pernah menyerang Indonesia adalah enam warga Malaysia yang dirawat dengan menerapkan Mabes Polri berkolaborasi dengan Departemen Hukum serta Hak Asasi Manusia. Keenam masyarakat Malaysia ini ialah sindikat pencuri ATM dengan modus skimming kartu. Mereka berhasil memakan 112 tagihan konsumen Bank Central Asia di Jakarta serta Bandung. Total kerugian mencapai lebih dari 1, 25 miliar. Modus yang dimanfaatkan komplotan ini merupakan memasang skimmer serta kamera pengintai di mesin ATM. Skimmer digunakan untuk meminjam data di kartu

---

<sup>17</sup> Dian Eka Kusuma Wardani. 2019. *Kejahatan Skimming Sebagai Salah Satu Bentuk Cyber Crime*. Jurisprudentie, Vol 6 No. 1. halaman 167-169. <https://journal.uin-alauddin.ac.id/index.php/Jurisprudentie/article/view/9358/6598>



ATM korban, sebaliknya kamera pengintai digunakan untuk meminjam nomor pin korban. Kasus Kejahatan skimming tidak berkurang dari hari ke hari, tetapi korbannya semakin hari semakin bertambah dan alat kerja kejahatan skimming semakin canggih. Tindak pidana skimming ATM harus dilakukan dengan Kebijakan Formulasi Hukum dan integrasi sistem peradilan pidana yang terpadu agar dapat diharapkan menekan atau menanggulangi kejahatan ini. Indonesia sendiri belum mengatur secara khusus perundang-undangan tentang kejahatan *skimming*, untuk itulah perlu dilakukan upaya pencegahan dan penanggulangan terhadap *skimming* agar tidak semakin meluas dan membahayakan masyarakat.<sup>18</sup>

Dalam Identifikasi masalah diatas Penulis akan mencoba menjelaskan **“Tinjauan Yuridis Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri”**

#### 1. Rumusan Masalah

- A. Bagaimana modus operandi pelaku tindak pidana pencurian data nasabah perbankan melalui anjungan tunai mandiri?
- B. Bagaimana pengaturan hukum bagi pelaku tindak pidana pencurian data nasabah Perbankan melalui anjungan tunai mandiri?
- C. Bagaimana tinjauan yuridis pencurian data nasabah perbankan melalui anjungan tunai mandiri?

---

<sup>18</sup> Andi Tanwir Mappanyukki. 2022. *Analisis Tindak Pidana Skimming Oleh Kepolisian Daerah Sulawesi Selatan. IJI Publication*. Vol. 3 No. 1. halaman 74-75  
<https://journal.intelekmadani.org/index.php/ijipublication/article/view/386/293>

## 2. Faedah Penelitian

Dalam penulisan proposal ini, dinantikan dapat memberikan hal positif dan manfaat, baik manfaat teoritis maupun manfaat praktis. Faedah dari segi teoritis adalah faedah sebagai sumbangan baik kepada ilmu pengetahuan pada umumnya maupun pada ilmu hukum khususnya. Sedangkan faedah dari segi praktis adalah penelitian tersebut berfaedah bagi kepentingan negara, bangsa, masyarakat dan pembangunan.<sup>19</sup>

### 1. Manfaat Teoritis

- a) Hasil penelitian ini diharapkan dapat memberikan sumbangan akademis berupa pengetahuan terhadap perkembangan ilmu hukum khususnya dalam perkembangan hukum pidana.
- b) Dalam hasil Penelitian ini diharapkan dapat memberikan pemahaman kepada mahasiswa dan masyarakat luas pada umumnya, terkait Tinjauan Yuridis Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri

### 2. Manfaat Praktis

- a) Hasil Penelitian ini dapat sebagai bahan masukan bagi Nasabah Perbankan pada saat melakukan transaksi di ATM agar lebih berhati-hati lagi pada saat melakukan transaksi tersebut sehingga dapat diaplikasikan sesuai maksud dan tujuan dan bermanfaat bagi masyarakat secara umum.

---

<sup>19</sup> Ida Hanifah, dkk. 2018. *Pedoman Penulisan Tugas Akhir Mahasiswa*, Medan, CV Pustaka Prima. halaman 16.

- b) Hasil Penelitian ini dapat memberikan Tinjauan Yuridis Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri.

## **B. Tujuan Penelitian**

1. Untuk mengetahui tentang modus operandi pelaku tindak pidana pencurian data nasabah perbankan melalui anjungan tunai mandiri
2. Untuk mengetahui tentang pengaturan hukum bagi pelaku tindak pidana pencurian data nasabah perbankan melalui anjungan tunai mandiri
3. Untuk mengetahui tinjauan yuridis tindak pidana pencurian data nasabah perbankan melalui anjungan tunai mandiri

## **C. Definisi Operasional**

Definisi Operasional atau kerangka konsep adalah kerangka yang membuat hubungan anatar definisi-definisi atau konsep-konsep khusus yang akan diteliti.<sup>20</sup> Maka dari itu judul penelitian pada proposal skripsi ini adalah Tinjauan Yuridis Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri

Maka dengan ini dapat dijelaskan Definisi Operasional, yaitu:

1. Tindak Pidana

ada beberapa pengertian yang diberikan oleh para sarjana Barat dan sarjana Indonesia, yaitu antara lain menurut Fletcher definisi pendek strafbaar feit adalah sebagai yang ditentukan oleh undang-undang dapat dihukum, sedangkan definisi panjangnya

---

<sup>20</sup> *Ibid.* halaman 17.

adalah sebagai perbuatan melawan hukum yang dilakukan dengan sengaja atau karena kekhilafan oleh orang lain yang mampu dipertanggungjawabkan.

Menurut H. J van Schravendijk strafbaar feit adalah perbuatan yang boleh dihukum, yaitu kelakuan yang begitu bertentangan dengan keinsafan hukum asal dilakukan dengan seorang yang karena itu dapat dipersalahkan. Strafbaar feit menurut VOS yang merumuskan bahwa strafbaar feit adalah suatu kelakuan (gedraging) manusia yang dilarang dan oleh undang-undang diancam dengan pidana.<sup>21</sup>

Istilah tindak dari tindak pidana adalah merupakan singkatan dari Tindakan atau Petindak, artinya ada orang yang melakukan suatu tindakan, sedangkan orang yang melakukan itu dinamakan Petindak. Sesuatu tindakan dapat dilakukan oleh siapa saja tetapi dalam banyak hal sesuatu tindakan tertentu hanya mungkin dilakukan oleh seseorang dari yang bekerja pada negara atau pemerintah, atau orang yang mempunyai suatu keahlian tertentu.

Sesuatu tindakan yang dilakukan itu haruslah bersifat melawan hukum, dan tidak terdapat dasar-dasar atau alasan-alasan yang meniadakan sifat melawan hukum dari tindakan tersebut. Setiap tindakan yang bertentangan dengan hukum atau tidak sesuai dengan hukum, tidak disenangi oleh orang atau masyarakat, yang

---

<sup>21</sup> Sukardi. 2020. Restorative Justice Dalam Penegakan Hukum Pidana Indonesia. Depok: Rajawali Pers. halaman 173.

baik langsung maupun yang tidak langsung terkena tindakan tersebut. Pada umumnya untuk menyelesaikan setiap tindakan yang sudah dipandang merugikan kepentingan umum di samping kepentingan perseorangan, dikehendaki turunnya penguasa, dan jika penguasa tidak turun tangan maka tindakan-tindakan tersebut akan menjadi sumber kekacauan yang tidak akan habis-habisnya.

Suatu tindak pidana yang dilakukan oleh seseorang yang menurut kehendaknya dan merugikan kepentingan umum atau masyarakat termasuk kepentingan perseorangan, lebih lengkapnya harus ternyata bahwa tindakan tersebut terjadi pada suatu tempat, waktu dan keadaan yang ditentukan. Artinya, dipandang dari sudut tempat, tindakan itu harus terjadi pada suatu tempat di mana ketentuan pidana Indonesia berlaku, dipandang dari sudut waktu, tindakan itu masih dirasakan sebagai suatu tindakan yang perlu diancam dengan pidana, dan dari sudut keadaan, tindakan itu harus terjadi pada suatu keadaan di mana tindakan itu dipandang sebagai tercela.<sup>22</sup>

## 2. *Cybercrime*

*Cybercrime* dalam arti sempit disebut *computer crime*, yaitu perilaku illegal atau melanggar secara langsung menyerang system keamanan suatu computer atau data yang diproses oleh komputer. *Cybercrime* dalam arti luas disebut *computer related crime*, yaitu

---

<sup>22</sup> *Ibid*

prilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan. Secara singkat dapat dikatakan bahwa cybercrime dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. *Cybercrime* ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia IT khususnya media internet.<sup>23</sup>

### 3. Perbankan

Perbankan merupakan segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya. Berdasarkan penjelasan tersebut, dapat dikatakan bahwa sistem perbankan merupakan suatu system yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara, dan proses melaksanakan kegiatan usahanya secara keseluruhan.<sup>24</sup>

Menurut Kamus Besar Bahasa Indonesia, bank adalah badan usaha di bidang keuangan yang menarik dan mengeluarkan uang dalam masyarakat, terutama memberikan kredit dan jasa dalam lalu lintas pembayaran dan peredaran uang. Kemudian menurut Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan Pasal 1 angka 2 "Bank adalah badan usaha yang menghimpun dana dari masyarakat

---

<sup>23</sup> Eliasta Ketaren, op.cit., halaman 36.

<sup>24</sup> Hermansyah, op.cit., halaman 30.

dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak. Dengan demikian, berdasarkan definisi di atas bank memiliki dua fungsi utama, yaitu menghimpun dana dalam bentuk simpanan dan menyalurkan dana kepada masyarakat dalam bentuk kredit. Secara umum, simpanan yang ditawarkan oleh bank konvensional ditawarkan dengan memberikan imbalan dalam bentuk bunga dan menyalurkan dana kepada masyarakat dalam bentuk kredit dengan mengambil imbalan dalam bentuk bunga.<sup>25</sup>

Menurut Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan Pasal 1 angka 1 "Perbankan" adalah segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya.

Hukum perbankan adalah keseluruhan norma-norma tertulis maupun norma-norma tidak tertulis yang mengatur tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses melaksanakan kegiatan usahanya. Norma-norma tertulis dapat dipahami sebagai seluruh peraturan perundang-undangan yang mengatur mengenai bank, sedangkan norma-norma yang tidak

---

<sup>25</sup> Nur Wahid. 2021. Perbankan Syariah "Tinjauan Hukum Normatif dan Hukum Positif". Jakarta: Kencana. halaman 2.

tertulis adalah hal-hal atau kebiasaan-kebiasaan yang timbul dalam praktik perbankan.<sup>26</sup>

#### 4. Anjungan Tunai Mandiri

ATM adalah kartu plastic yang diberikan oleh bank yang dapat digunakan oleh pemegangnya untuk membeli barang-barang dan jasa secara tunai maupun kredit dan bisa berguna sebagai penarikan uang secara tunai. Sedangkan ATM (*Automatic Teller Machine*) adalah mesin/computer yang digunakan oleh bank untuk melayani transaksi keuangan seperti penyetoran uang, pengembalian uang tunai, pengecekan saldo, transfer uang dari satu rekening ke rekening lainnya, serta transaksi keuangan sejenis lainnya secara elektronik.<sup>27</sup>

### D. Keaslian Penelitian

Berdasarkan penelusuran kepustakaan dan pencarian melalui sarana internet, maka dari itu penulis membuat penelitian ilmiah yang berjudul tinjauan yuridis tindak pidana pencurian data nasabah perbankan melalui anjungan tunai mandiri.

### E. Metode Penelitian

Metode atau metodologi diartikan sebagai logika dari penelitian alamiah, studi terhadap prosedur dan teknik penelitian. Pada Kenyataannya Penelitian memiliki makna di mana penelitian adalah rangkaian kegiatan

---

<sup>26</sup> *Ibid*

<sup>27</sup> Ronny Prasetya. 2010. Pembobolan ATM Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan. Jakarta : Prestasi Pustaka. halaman 11-12.



ilmiah untuk menggali dan memecahkan permasalahan, atau untuk menemukan sesuatu kebenaran dari fakta-fakta yang ada. Metode penelitian bertujuan untuk untuk menjelaskan bagaimana penelitian itu dilakukan agar mendapatkan hasil yang maksimal.<sup>28</sup> Adapun metode penelitian yang digunakan dalam penelitian ini, yakni sebagai berikut:

Metode penelitian menguraikan tentang:

### **1. Jenis dan Pendekatan Penelitian**

Jenis penelitian hukum dapat dilakukan dengan menggunakan pendekatan penelitian hukum normatif (*Yuridis Normatif*). Penelitian hukum normatif disebut sebagai penelitian hukum doktrinal, dimana hukum dikonsepsikan sebagai apa yang bertuliskan peraturan perundang-undangan (*law in book*), Penelitian hukum normatif ini didasarkan kepada bahan hokum primer dan sekunder, yaitu penelitian yang mengacu kepada norma-norma yang terdapat dalam peraturan perundang-undangan tertentu atau hokum tertulis.<sup>29</sup> Selain itu, penulis juga menggunakan pendekatan penelitian dengan cara penelusuran studi pustaka dengan mengambil data-data melalui kepustakaan seperti buku, Jurnal, Artikel, dan Peraturan Perundang-undangan dan mengambil beberapa data terkait tinjauan yuridis tindak pidana pencurian data nasabah perbankan melalui anjungan tunai mandiri.

---

<sup>28</sup> Ida Hanifah, dkk, Op. Cit. halaman 19.

<sup>29</sup> *Ibid.*

## 2. Sifat Penelitian

Penelitian hukum bertujuan untuk mengetahui dan melahirkan keadaan sesuatu mengenai apa dan bagaimana keberadaan norma hukum dan bekerjanya norma hukum pada masyarakat. Berdasarkan tujuan penelitian hukum tersebut, maka kecenderungan sifat penelitian yang digunakan adalah deskriptif. Penelitian deskriptif adalah penelitian yang hanya semata-mata menggambarkan keadaan obyek atau peristiwanya tanpa suatu maksud untuk mengambil kesimpulan-kesimpulan yang berlaku secara umum.<sup>30</sup> Kemudian bahan-bahan tersebut disusun secara sistematis, dikaji dan ditarik kesimpulan dalam hubungannya dengan masalah yang diteliti yaitu tinjauan yuridis tindak pidana pencurian data nasabah perbankan melalui anjungan tunai mandiri.

## 3. Sumber Data

Sumber data yang dapat digunakan dalam melakukan penelitian ini terdiri dari :

- a) Data yang bersumber dari Hukum Islam yaitu Al-Qur'an dan Hadist (Sunnah Rasul). Data yang bersumber dari Hukum Islam tersebut lazim disebut pula sebagai data kewahyuan<sup>31</sup>.

---

<sup>30</sup> *Ibid.*

<sup>31</sup> *Ibid.*

b) Data sekunder, yaitu data yang diperoleh seorang peneliti secara tidak langsung dari sumbernya (objek penelitian), tetapi melalui sumber lain. Peneliti mendapatkan data yang sudah jadi yang dikumpulkan oleh pihak lain dengan berbagai cara atau metode baik secara komersial maupun non komersial. Misal: buku-buku teks, jurnal, majalah, koran, dokumen, peraturan, perundangan, dan sebagainya.<sup>32</sup> Yang termasuk dalam data sekunder terdiri dari :

- 1) Bahan Hukum Primer, yaitu bahan-bahan hukum yang mengikat, seperti Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Pidana, Peraturan perundang-undangan No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Serta peraturan perundang-undangan yang terikat lainnya.
- 2) Bahan Hukum Sekunder, yaitu bahan-bahan yang erat kaitannya dengan bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer, dapat berupa: Rancangan peraturan perundang-undangan, perundang-

---

<sup>32</sup> Suteki, Galang Taufani. 2018. *Metodologi Penelitian Hukum "Filsafat, Teori, dan Praktik"*, Depok: Rajawali Pers. halaman 215.

undangan yang tidak berlaku, hasil karya ilmiah para sarjana, hasil-hasil penelitian, Jurnal, dan lain sebagainya.

3) Bahan Hukum Tersier, yaitu Berupa komplementer untuk bahan hukum sekunder dan tersier contohnya adalah Kamus Hukum (Black's Law Dictionary), Indeks dan Bibliografi.<sup>33</sup>

c) Data Primer, yaitu data yang diperoleh langsung oleh peneliti dari informan atau narasumber di lapangan. Secara umum, berdasarkan sumber data, penelitian dapat dibedakan antara penelitian lapangan (field research), penelitian pustaka (library research), dan penelitian laboratorium. Penelitian laboratorium dalam arti penelitian yang dilakukan dalam suatu ruangan dengan peralatan tertentu, jarang dilakukan dalam penelitian hukum, meskipun sering disebut bahwa laboratorium penelitian hukum adalah masyarakat.<sup>34</sup>

#### **4. Alat pengumpulan Data**

Teknik pengumpulan data berkaitan dengan pengumpulan data. Teknik pengumpulan data dapat dilakukan melalui observasi (pengamatan), teknik komunikasi, dan studi dokumen. Untuk

---

<sup>33</sup> *Ibid.*

<sup>34</sup> Elisabeth Nurhaini Butarbutar. 2018. *Metode Penelitian Hukum "Langkah-langkah untuk Menemukan Kebenaran dalam Ilmu Hukum"*, Bandung: PT Refika Aditama. halaman 63.

menentukan teknik dan alat pengumpul data yang harus digunakan, maka harus disesuaikan dengan jenis dan sumber data yang dibutuhkan. Pada umumnya, apabila data yang dibutuhkan data primer, yaitu berupa fakta yang bersumber dari studi lapangan (field research), maka dapat dipilih teknik observasi ataupun teknik komunikasi, sebaliknya jika yang dibutuhkan adalah data sekunder, maka teknik atau studi dokumen dapat digunakan.<sup>35</sup>

## 5. Analisis Data

Analisis data adalah kegiatan memfokuskan, mengabstraksikan, mengorganisasikan data secara sistematis dan rasional untuk memberikan bahan jawaban terhadap permasalahan. Analisis data menguraikan tentang bagaimana memanfaatkan data yang terkumpul untuk dipergunakan dalam memecahkan permasalahan penelitian. Jenis penelitian data terdiri dari analisis kuantitatif dan kualitatif. Analisis data yang dipergunakan dalam penelitian hukum biasanya dilakukan dengan analisis kualitatif sesuai dengan tipe dan tujuan penelitian.<sup>36</sup>

## 6. Jadwal Penelitian

Penelitian ini dilakukan dengan cara bertahap. Tahapan yang dilakukan dalam penelitian ini meliputi beberapa tahap, yaitu :

---

<sup>35</sup> *Ibid.*

<sup>36</sup> Ida Hanifah, dkk, Op. Cit. halaman 21.

a. Tahap persiapan

Dalam tahap ini dilakukan persiapan dalam urusan pengajuan judul serta proposal, yang dijadwalkan selama 10 hari.

b. Tahap pengumpulan data

Dalam tahap ini dilakukan pengumpulan data yang berhubungan dengan penelitian, yang dijadwalkan selama 20 hari.

c. Tahap pengolahan data

Dalam tahap ini dilakukan pengolahan data terhadap semua data yang diperoleh, yang dijadwalkan selama 30 hari.

d. Tahap penyelesaian

Dalam tahap ini merupakan akhir rangkaian dalam penulisan skripsi, dan penyelesaian proses bimbingan, yang dijadwalkan selama 30 hari.<sup>37</sup>

---

<sup>37</sup> *Ibid.*

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **1. Tinjauan Umum Tentang Tindak Pidana**

Persoalan mendasar berkaitan dengan tindak pidana adalah menyangkut saat penetapan perbuatan yang dilarang tersebut (tindak pidana). Doktrin klasik menyatakan bahwa suatu perbuatan merupakan tindak pidana jika telah ditetapkan lebih dahulu melalui perundang-undangan yang kemudian dikenal dengan asas legalitas (legality principle) yang merupakan asas Hukum Pidana yang dikenal secara universal. Pentingnya asas legalitas berkaitan dengan aspek kepastian hukum (rechts zekerheid/legal certainty). Dalam konteks tertentu tidak dapat disangkal eksistensi asas itu, namun dalam konteks yang lain, jika dihubungkan dengan dinamika masyarakat, maka akan timbul dua masalah penting, yakni ketertinggalan aturan perundang-undangan dengan kebutuhan masyarakat. Kedua akan mendorong terjadinya kriminalisasi melalui undang-undang di luar KUHP. Dalam rangka menghadapi permasalahan pertama, seharusnya undang-undang merumuskan norma seabstrak mungkin, dengan merumuskan unsur tindak pidana secara stereotipe, yakni dengan menggunakan satu frasa, dapat merangkum beberapa perbuatan di dalamnya. Misalnya dalam delik pembunuhan-yang merupakan delik materiil atau delik dengan perumuan materiil (materiele omschijving)-cukup dirumuskan dengan frasa "menghilangkan nyawa orang lain" telah mencakup berbagai perbuatan

sepanjang menimbulkan akibat "hilangnya nyawa orang" sebagai mana dirumuskan dalam undang-undang. Namun untuk delik formil atau delik dengan perumusan formil (formale omschrijving) penyebutan unsur secara lengkap yang menggambarkan perbuatan yang dilarang harus dilakukan secara cermat. Kesemuanya tidak lain dimaksudkan agar undang-undang yang telah dibuat tidak lekas ketinggalan zaman. Perumusan tindak pidana dengan mengacu kedua jenis delik di atas tetap relevan untuk dipertahankan.<sup>38</sup>

Pengaturan tentang Tindak Pidana (Strafbaarfeit) konsep KUHP mengambil jalan tengah karena disamping mengakui asas legalitas dalam arti formil juga asas legalitas materiil. Artinya konsep bertolak dari undang-undang sebagai sumber utama dalam menentukan perbuatan yang dilarang; meskipun demikian dengan dilandasi oleh prinsip monodualistik atau menurut penulis, Prinsip Integralistik-eksistensi hukum yang hidup dapat dijadikan landasan dalam menentukan dapat dihukumnya perbuatan yang disebut dengan asas legalitas materiil.

Pengaturan tentang asas legalitas formil diatur dalam Pasal 1 RUU bahwa: "Tiada seorangpun dapat dipidana atau dikenakan tindakan kecuali perbuatan yang dilakukan telah ditetapkan sebagai tindak pidana dalam peraturan perundang-undangan yang berlaku pada saat perbuatan itu dilakukan". Dalam terjemahan KUHP sekarang, terjadi koreksi total terhadap perumusan pasal di atas, frasa "tiada seorangpun" merupakan

---

<sup>38</sup> Ali Zaidan. 2015. Menuju Pembaruan Hukum Pidana. Jakarta: Sinar Grafika. halaman 367.



koreksi terhadap frasa "tiada satu perbuatan" hal ini disebabkan menurut para ahli, yang dapat dihukum itu hanya orang, sementara perbuatan hanya dapat dilarang. Selain pidana dalam konsep juga diberikan ruang untuk dijatuhkannya sanksi berupa tindakan (treatment) seperti pidana pengawasan maupun pidana kerja sosial yang tidak dikenal dalam KUHP saat ini.<sup>39</sup>

## 2. Pengertian *Cybercrime*

Sebelum mengurai pengertian *cyber crime* secara terperinci, maka terlebih dahulu akan dijelaskan "induk" *cybercrimes* yaitu *Cyber space*. *Cyber space* dipandang sebagai sebuah dunia komunikasi yang berbasis komputer. Dalam hal ini, *cyber space* dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet.

Realitas baru ini dalam kenyataannya terbentuk melalui jaringan komputer yang menghubungkan antarnegara atau Antarbenua yang berbasis *protokol transmission control protocol/internet protocol*. Hal ini berarti, dalam sistem kerjanya dapatlah dikatakan bahwa *cyber space* (internet) telah mengubah jarak dan waktu menjadi tidak terbatas. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah Jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda.

---

<sup>39</sup> *Ibid*

Dalam perkembangan selanjutnya kehadiran teknologi canggih komputer dengan jaringan internet telah membawa manfaat besar bagi manusia. Pemanfaatannya tidak saja dalam pemerintahan, dunia swasta/perusahaan, akan tetapi sudah menjangkau pada seluruh sektor kehidupan termasuk segala keperluan rumah tangga (pribadi). Komputer (internet) telah mampu membuka cakrawala baru dalam kehidupan manusia baik dalam konteks sarana komunikasi dan informasi yang menjanjikan menembus batas-batas negara maupun penyebaran dan pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuwan di seluruh dunia. Akan tetapi, kemajuan teknologi informasi (internet) dan segala bentuk manfaat di dalamnya membawa konsekuensi negatif tersendiri di mana semakin mudahnya para penjahat untuk melakukan aksinya yang semakin meresahkan masyarakat. Penyalahgunaan yang terjadi dalam *cyber space* inilah yang kemudian dikenal dengan *cyber crime* atau dalam literatur lain digunakan istilah *computer crime*.<sup>40</sup>

### 3. Pengertian Perbankan

Perbankan merupakan segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya. Berdasarkan penjelasan tersebut, dapat dikatakan bahwa sistem perbankan merupakan suatu system yang menyangkut tentang bank, mencakup kelembagaan,

---

<sup>40</sup> Maskun. 2013. *Kejahatan Siber "Cybercrime"*. Jakarta: Kencana. halaman 46-47.

kegiatan usaha, serta cara, dan proses melaksanakan kegiatan usahanya secara keseluruhan.

Mengenai bagaimana system perbankan di Indonesia tentu segala sesuatunya dapat dilihat dalam Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998.<sup>41</sup>

Lembaga perbankan adalah lembaga yang berdiri pada kepercayaan masyarakat sehingga dikenal adanya kerahasiaan bank. Konsekuensinya apabila masyarakat sudah tidak mempercayai lagi suatu bank, bank tersebut akan sensitif terhadap gempuran masyarakat yang menarik dana sehingga berpotensi merugikan bank. Kemajuan pesat Teknologi Informasi (TI) dan globalisasi mendukung bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya melalui media elektronik atau dikenal dengan *Electronic Banking (e-banking)*. *E-banking* merupakan layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine (ATM)*.

ATM atau yang lebih dikenal dengan nama Anjungan Tunai Mandiri merupakan suatu bentuk terminal/mesin komputer yang terhubung dengan jaringan komunikasi bank, yang memungkinkan nasabah melakukan transaksi keuangan secara mandiri tanpa bantuan

---

<sup>41</sup> Hermansyah, op.cit., halaman 30.

dari teller ataupun petugas bank lainnya. Kartu ATM merupakan kartu plastik yang dilengkapi dengan magnetic stripe. Pada magnetic stripe akan terekam secara elektronik. ATM sering ditempatkan di lokasi-lokasi strategis, seperti restoran, pusat perbelanjaan, bandar udara, stasiun kereta api, terminal bus, pasar swalayan, dan kantor-kantor bank itu sendiri. Kartu ATM adalah jenis alat pembayaran dengan menggunakan kartu (APMK) yang dapat digunakan untuk melakukan penarikan tunai atau pemindahan dana .<sup>42</sup>

#### **4. Pengertian Anjungan Tunai Mandiri**

Untuk melengkapi dan menanggapi kebutuhan para nasabah dimana saja baik didesa maupun kota, khususnya dalam rangka memenuhi kebutuhan transaksi perbankan maka dunia perbankan harus terus memberikan pelayanan yang maksimal untuk para nasabahnya. Seiring kemajuan teknologi informasi maka dunia perbankan pun tidak mau ketinggalan, dengan memanfaatkan teknologi informasi diharapkan para nasabah dapat mengakses dengan mudah tanpa ada kendala yang dihadapi, salah satu fasilitas yang diberikan oleh perbankan merupakan ATM, dimana fungsi ATM adalah memindahkan uang atau menerima segala macam bentuk pembayaran dan setoran seperti pembayaran listrik, telpon, air, pajak, uang kuliah dan pembayaran lainnya.

Pelayanan bank yang paling sering digunakan oleh para nasabah adalah *Automatic Teller Machine* atau yang sering disebut dengan ATM,

---

<sup>42</sup> Dian Eka Kusuma Wardani, Op.cit. halaman 167-169.

ATM adalah salah satu solusi untuk mengadakan suatu transaksi yang cepat dan efektif. Dengan ATM para nasabah tidak harus pergi ke kantor bank dan tidak harus mengantri.<sup>43</sup>

---

<sup>43</sup> Nurwijayanti KN, Ganjar Eko Santoso. 2020. Analisa Jaringan Mesin Automatic Teller Machine (ATM) Dalam Rangka Pemeliharaan Di Pulau Jawa. Jurnal Teknologi Industri, Vol. 9 No. 1. halaman 92.

<https://journal.universitassuryadarma.ac.id/index.php/jti/article/download/964/932>

### **BAB III**

#### **PEMBAHASAN**

##### **A. Modus Operandi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri**

Modus operandi menurut *Blacks Law Dictionary* adalah: *Method of operating or doing things (M.O.) Terms by police and criminal investigators to describe the particular method of a criminal's activity. It refers to pattern of criminal behavior so distinct that separate crimes or wrongful conduct are recognize as work of same person* (Henry Campbell, 1990). Dalam bahasa latin modus operandi berarti cara bertindak atau procedure. Jadi modus operandi adalah cara melaksanakan, cara bertindak.<sup>44</sup>

Modus Operanadi bersumber dari bahasa latin yang memiliki arti langkah atau cara untuk bergerak mengetahui cara untuk melakukan sesuatu. Seseorang dapat disebut sebagai penjahat atau pelaku suatu tindak pidana apabila seseorang telah menjalankan sesuatu tindak perbuatan yang di mana perbuatan tersebut dapat diberi hukuman atau telah melanggar atau melakukan sesuatu perbuatan yang telah diatur dalam suatu aturan yang berlaku. Modus Operandi adalah cara proses orang-perorang atau kelompok penjahat dalam melakukan aksi rencana kejahatannya. Pengertian Modus

---

<sup>44</sup> Rohim. 2017. Modus Operandi. Depok: Alta Utama. halaman 31

Operandi dalam lingkup kejahatan yaitu proses, cara, atau teknik yang berciri khusus dari seorang penjahat dalam melakukan perbuatan jahatnya.<sup>45</sup>

Tugas suatu teknologi dibidang perbankan sangatlah bermanfaat, karena sudah bisa dipastikan sistem didunia perbankan tidak terlepas dari teknologi yang menjadi penyangga. Semakin berkembang dan kompleks fasilitas yang disediakan untuk pelayanan perbankan, semakin berkembang dan kompleks pula teknologi yang dipakai. Sudah menjadi kewajiban bahwa kemajuan suatu teknologi yang digunakan dalam dunia perbankan selain untuk melancarkan operasional dalam internal bank sendiri, tetapi juga untuk memberikan kemudahan pelayanan kepada konsumen bank atau nasabah bank. Apabila pada masa ini produk yang ditawarkan oleh seluruh bank memiliki kesamaan, maka yang menjadi persaingan dalam dunia perbankan saat ini adalah bagaimana memberikan produk yang serba mudah dan serba cepat.<sup>46</sup>

Penulis berpendapat bahwa tindak pidana atau kejahatan perbankan dapat dikatakan sebagai kejahatan dengan format kejahatan yang baru karena tindak pidana atau kejahatan perbankan sewaktu-waktu berkembang seiring dengan perubahan zaman dan perkembangan masyarakat. Ringkasnya, modus operandi tindak pidana atau kejahatan perbankan di tahun 2000-an tentunya akan berbeda dengan modus operandi tindak pidana atau kejahatan perbankan yang dilakukan di

---

<sup>45</sup> Alfitra, 2014. Modus Operandi Pidana Khusus di Luar KUHP, Jakarta: RAS. halaman 28.

<sup>46</sup> Ronny Prasetya. 2010. Pembobolan ATM, Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan. Jakarta: PT. Prestasi Pustaka. halaman 27.

tahun yang sekarang ini, demikian pula dengan tahun-tahun berikutnya, modus operandi tindak pidana atau kejahatan perbankan akan terus berkembang.

Tindak pidana perbankan saat ini baik secara kualitatif maupun secara kuantitatif telah mendapati peningkatan yang cukup tajam dari waktu ke waktu. Oleh karena itu, perlu dilakukan usaha untuk mencegah dan menanggulangi terjadinya tindak pidana perbankan ini. Demikian pula dengan modus operandi tindak pidana perbankan ini, hingga saat ini dapat dipastikan telah mengalami modifikasi yang cukup signifikan. Hal ini sudah tentu sangat berbahaya mengingat dampak dari tindak pidana perbankan sangat luas dan sangat berdampak negatif.<sup>47</sup>

Perbankan sebagai salah satu lembaga keuangan mempunyai nilai strategis di dalam perekonomian suatu negara. Lembaga tersebut dimaksudkan sebagai perantara antara pihak yang mempunyai kelebihan dana dan pihak yang kekurangan dana. Lembaga keuangan bank bergerak dalam kegiatan perkreditan, dan berbagai jasa yang diberikan bank melayani kebutuhan pembiayaan serta melancarkan mekanisme system pembayaran bagi semua faktor perekonomian. Perbankan sebagai lembaga keuangan berorientasi bisnis melakukan berbagai transaksi. Transaksi perbankan yang utama adalah menghimpun dana (funding) dan menyalurkan dana (lending) di samping itu transaksi perbankan lainnya dalam rangka mendukung kegiatan menghimpun dan menyalurkan dana adalah memberikan jasa-jasa bank lainnya (services).

---

<sup>47</sup> Kristian dan Yopi Gunawan. 2018. Tindak Pidana Perbankan Dalam Proses Peradilan Di Indonesia. Jakarta : Kencana. Halaman 23.



Sistem perbankan di Indonesia disebut dengan dual banking system, maksud dari dual banking system adalah terselenggaranya dua sistem perbankan (konvensional dan syariah) secara berdampingan yang pelaksanaannya diatur dalam berbagai peraturan perundang-undangan yang berlaku.<sup>48</sup>

Modifikasi modus operandi tindak pidana perbankan ini ditimbulkan oleh berbagai faktor di antaranya adalah kondisi sosial ekonomi masyarakat yang semakin maju, perkembangan dan kemajuan ilmu pengetahuan dan teknologi, kemajuan dunia usaha, kerja sama internasional serta kemajuan kebijakan pemerintah dalam pengaturan kegiatan bank. Modifikasi bentuk tindak pidana perbankan sebagaimana dikemukakan di atas merupakan sesuatu yang wajar. Dikatakan demikian karena hal ini sangat berkaitan dengan fungsi dan tugas dari lembaga perbankan sebagai pusat atau sentral dari lalu lintas pembayaran dan peredaran uang di suatu negara. Dengan ucapan lain, dapat dikatakan bahwa semakin besar lalu lintas pembayaran dan peredaran uang, maka semakin besar pula mungkin di dalam lembaga tersebut terjadi perilaku-perilaku yang dapat merugikan masyarakat, mengakibatkan gangguan dan hambatan terhadap keamanan dan kelancaran lalu lintas pembayaran dan peredaran uang serta dalam jangka panjang akan menimbulkan gangguan dan hambatan dalam pelaksanaan tugas dan fungsi perbankan dan perekonomian nasional. Hal ini tidak pula terlepas dari kompleksnya fungsi dan tugas perbankan dewasa ini, rigitnya prosedural perbankan dan kemajuan peralatan elektronik dan kemajuan peralatan

---

<sup>48</sup> Trisnadi dan Abd. Shomad. 2017. Hukum Perbankan. Jakarta: Kencana. halaman 1.

telekomunikasi yang semakin canggih yang mendukung dunia perbankan dewasa ini.

Dengan demikian, tindak pidana atau kejahatan perbankan adalah tindak pidana atau kejahatan dengan format kejahatan yang akan senantiasa berkembang baik modus operandi maupun alat yang dipakai seiring dengan kemajuan zaman, perkembangan masyarakat dan kemajuan ilmu pengetahuan dan teknologi. Untuk memecahkan hal ini, tentu hukum juga tidak boleh bersifat statis melainkan harus mengikuti kemajuan zaman, perkembangan masyarakat dan perkembangan dunia internasional khususnya dalam rangka penyelesaian (mencegah dan memberantas) tindak pidana kejahatan perbankan ini.<sup>49</sup>

Terkait perbankan, perbankan adalah suatu bentuk usaha yang memiliki kebebasan dalam menyatukan dan menyalurkan dana sehingga sangat strategis untuk dipakai sebagai sarana pencucian uang, baik melalui *placement*, *layering*, maupun *integration*. Selain itu, transfer dana secara elektronik juga dapat digunakan oleh pencuci uang untuk memindahkan dana secara cepat dan relatif murah serta aman ke rekening pihak lain, baik di dalam maupun di luar negeri.

Perbankan juga sangat rawan bagi tindak pidana yang terorganisasi sehingga sangat strategis untuk digunakan. Tindak pidana yang terorganisasi biasanya bersembunyi di balik suatu perusahaan atau nama lain (*nominees*) dengan melakukan perdagangan internasional palsu dan berskala besar dengan maksud untuk memindahkan uang yang tidak sah dari suatu negara ke negara lain.

---

<sup>49</sup> *Ibid.* halaman 24

Perusahaan yang digunakan untuk menyembunyikan kegiatan tindak pidana tersebut biasanya meminta kredit/pembiayaan dari bank untuk menyamarkan kegiatan pencucian uang. Modus operandi lainnya antara lain dengan menerapkan faktur (*invoice*) palsu yang di-mark-up atau L/C palsu sebagai upaya untuk menyulitkan pengusutan dikemudian hari. Oleh karena itu, perbankan harus berhati-hati terhadap kemungkinan dimanfaatkan sebagai sarana pencucian uang.<sup>50</sup>

Biasanya kepentingan yang diutamakan dalam perspektif masyarakat adalah mengamankan atau mencegah terjadinya suatu tindak kejahatan pada masa yang akan datang dan tidak terlalu menekankan pada rasa balas dendam atas kejahatan yang dilakukan oleh pelaku tindak kejahatan. Dalam kejahatan yang bersangkutan dengan teknologi yang berbasis komputer dan jaringan telekomunikasi terdapat beberapa modus operandi yang dikelompokkan sebagai berikut, yaitu:<sup>51</sup>

- a) *Unauthorized access to computer system and service*, adalah suatu bentuk kejahatan yang dilakukan untuk melalui atau membuka sistem jaringan komputer secara tidak sah atau tidak mempunyai izin dari pemilik sistem jaringan komputer. Adapun bentuk dari kejahatan ini seperti sabotase dan pencurian suatu informasi yang penting dan rahasia.

---

<sup>50</sup> Adrian Sutedi. 2010. Hukum Perbankan "Suatu Tinjauan Pencucian Uang, Merger, Likuidasi, dan Kepailitan. Jakarta: Sinar Grafika. halaman 30

<sup>51</sup> Dikdik M.Arif Mansur & Elisatris Gultom. 2005. *Cyber Law* Aspek Hukum Teknologi Informasi. Bandung: PT Refika Aditama. halaman 40.

- b) *Illegal contents*, yaitu bentuk kejahatan membagikan atau suatu data atau informasi mengenai sesuatu kedalam dunia maya (internet) yang di mana data dan informasi tersebut salah, kemudian melanggar aturan yang ada, serta menggagu ketertiban umum.
- c) *Data forgery*, merupakan bentuk kejahatan meniru data yang terdapat pada dokumen-dokumen penting melalui jaringan internet yang tersimpan dalam *scriptless document*. Kejahatan ini biasanya ditujukan untuk dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi “salah ketik” dan pada akhirnya memberikan keuntungan kepada pelaku karna korban akan memasukkan data pribadi atau nomor kartu kredit yang dapat disalahgunakan.
- d) *Cyber espionage*, merupakan bentuk kejahatan yang memakai jaringan internet untuk melihat secara diam-diam data suatu pihak. Kejahatan ini biasanya sering terjadi dalam kompetisi suatu bisnis yang di mana salah satu pihak menyimpan suatu data atau dokumen-dokumen yang penting dalam suatu sistem komputerisasi.
- e) *Offence against intellectual property*, adalah suatu bentuk kejahatan yang di tujukan kepada hak kekayaan intelektual seseorang di jaringan internet. Sebagai contoh pembuatan tiruan suatu situs web page milik orang lain secara illegal, penyiaran suatu informasi di internet yang merupakan rahasia dagang milik orang lain
- f) *Infringements of privacy*, merupakan suatu bentuk kejahatan yang ditujukan terhadap informasi seseorang yang sangat penting dan hal yang

sangat pribadi yang dimiliki oleh seseorang. Kejahatan ini biasanya dilakukan terhadap informasi pribadi dan keterangan pribadi seseorang yang terdapat dalam formulir data yang tersimpan secara komputerisasi. Yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara materil maupun imateril, seperti nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya.<sup>52</sup>

Dari keterangan keenam penggolongan modus operandi dalam kejahatan yang berhubungan dengan teknologi yang berbasis komputer dan jaringan telekomunikasi apabila melihat kepada objek dari tindak pidana *skimming* ini maka tindak pidana *skimming* ini masuk kedalam kategori *Infringements of privacy* yang mana objek dari tindak pidana *skimming* ini yaitu informasi dan data pribadi dari seseorang. Dalam keterangan modus operandi dari kasus tindak pidana *skimming* ini penulis akan menjelaskan rangkaian demi rangkaian yang dilakukan oleh pelaku dalam melakukan kejahatannya.

Titik yang paling lemah dan tanpa kita sadari yang menjadi sasaran kejahatan yakni peretas dengan cara *skimming*. Kejahatan ini adalah kejahatan yang melalui computer atau jaringan LAN computer dan salah satu tindakan kejahatan yang menjadi ancaman serius saat ini. Dengan kita memanfaatkan

---

<sup>52</sup> Maskun. 2013. *Kejahatan Siber Cyber Crime*. Jakarta: Kencana. halaman 50.

teknologi ini baik yang berbasis sistem computer atau yang lainnya, kita sebagai pengguna adalah korbannya.<sup>53</sup>

Tindak pidana peretas ini yang menggunakan *skimming* membuat banyak pihak merugi bahkan sampai pemerintah mengeluarkan kas Negara. Dengan kata lain, hancurnya sebuah perbankan tidak cuma hanya berefek pada intasi itu melainkan banyak pihak yang terkena imbasnya dan bank lainnya bahkan merasakan efek yang sama terkait sistem keuangan dan sistem pembayaran dari negara yang bersangkutan serta sistem pembayaran dunia juga ikut merasakan efeknya.<sup>54</sup>

Kejahatan terkait perbankan yang sedang ramai dibicarakan adalah *Skimming*, Dalam modus operandi “peretas bank” dengan cara *Skimming* dilakukan dengan proses mencuri data nasabah yang tersimpan dalam magnetik strip pada kartu ATM dan dikirim secara nirakabel. Cara pencurian data ini dilakukan dengan beberapa langkah, yaitu umumnya pertama-tama pelaku memasukkan alat *skimmer (electronic data capture)* pada mulut mesin ATM, lalu pelaku memasukkan kamera tersembunyi untuk menangkap gerakan jari nasabah saat menekan pin ATM yang ditutupi, misalnya dengan kotak brosur. Selain itu, pelaku juga mengkondisikan ATM untuk mengeluarkan pesan isi dari ATM sedang habis padahal sudah memasukkan pin dan kartu, selanjutnya setelah

---

<sup>53</sup> Michael Enrick. 2019. Pembobolan ATM Menggunakan Teknik *Skimming* Kaitannya Dengan Pengajuan Restitusi. *Jurist-Diction*. Vol. 2 No. 2. halaman 555. <https://e-journal.unair.ac.id/JD/article/download/14252/7941>

<sup>54</sup> Dian Ekawati. 2018. Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan *skimming* ditinjau dari perspektif teknologi informasi dan perbankan. *Unes Law Riview*. Vol.1 No. 2. halaman 157. <https://media.neliti.com/media/publications/270557-perlindungan-hukum-terhadap-nasabah-bank-3065a9d8.pdf>

pelaku mendapat data nasabah maka pelaku memindahkan data tersebut kedalam kartu palsu. Dalam beberapa kasus pelaku tidak melekatkan kamera tersembunyi namun hanya dengan mengintip dari balik bahu nasabah.<sup>55</sup>

Dalam penerapan Tindak pidana *skimming* ini dilakukan dengan berbagai macam cara. Ada yang memakai alat khusus yang berupa perangkat kecil (*skimmer*) yang dipakai di mulut mesin ATM. *Skimmer* memiliki fungsi untuk menyimpan data dan dapat disalin serta dipindahkan ke tempat penyimpanan data yang lain. Untuk alat *skimmer* yang canggih juga dapat mengcopy data dari kartu ATM dan nomor PIN ATM korban sekaligus yang dapat mengcopy data dan/atau PIN kartu debit atau kredit sekaligus.

Adapun cara lain untuk melakukan *skimming* yaitu dengan cara memakai router ke mesin ATM dengan kabel sehingga dapat tersambung dengan sistem jaringan ATM yang bertujuan untuk mendapatkan data dari nasabah-nasabah bank, kemudian memasang kamera tersembunyi di cover pinpad yang bertujuan untuk mengambil gambar dari PIN yang diketik oleh nasabah. Setelah mendapat data dan PIN ATM, kemudian data dan PIN ATM tersebut dikloning atau disalin kedalam kartu kosong (*blank card*) yang bertujuan agar dapat melakukan tarik uang tunai yang telah ditemukan dimanapun dan kapanpun. Cara ini sering

---

<sup>55</sup> R. Toto Sugiharto. 2010. Tips ATM Anti Bobol: Mengenal Modus-modus Kejahatan Lewat ATM dan Tips Cerdik Menghindarinya, Yogyakarta: Media Pressindo, halaman 140.

dilakukan oleh pelaku kejahatan *skimming* yang melakukan kejahatannya di Indonesia.<sup>56</sup>

Perbuatan orang yang melakukan, yang menyuruh melakukan atau yang turut melakukan perbuatan itu, dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan dokumen elektronik dalam suatu computer atau system elektronik tertentu milik orang lain, seperti Putusan pengadilan negeri Ngawi Nomor 163/Pid.Sus/2020/PN Ngw, dimana terdakwa 1 SARYANTO ALADAM dan terdakwa 2 TRI WARNO terbukti secara sah dan meyakinkan menurut hukum bersalah telah melakukan tindak pidana “ turut serta melakukan, tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik ”. Bahwa pada waktu dan tempat sebagaimana tersebut diatas terdakwa II. TRI WARNO bin KARMONO mulanya datang ketoko sembako milik saksi korban YUDI PRAMONO dengan berpura-pura mau menitip transfer kemudian sambal melihat saksi korban memasukkan nomor PIN ke mesin BRI Link, kemudian terdakwa I masuk kedalam toko sembako berpura-pura membeli rokok untuk mengalihkan perhatian saksi korban kepada terdakwa II, dan saat pemilik toko melanyani terdakwa I membeli rokok, kemudian terdakwa II mengambil ATM milik saksi korban yang disimpan di dalam laci kemudian digesekan kealat berupa *Skimming Mini Tools* yang dibawa oleh terdakwa II, kemudian setelah selesai terdakwa I dan terdakwa II Kembali ke mobil jenis Pajero Sport warna putih No. Pol. AD-8005-KU dan

---

<sup>56</sup> Hatarto Pakpahan, Ahmad Aryo, 2021. Tindak Pidana Turut Serta Mengakses Komputer dan/atau Sistem Elektronik dengan Modus *Skimming*. Bhirawa Law Journal. Vol. 2 No. 2. halaman 220. <https://www.jurnal.unmer.ac.id/index.php/blj/article/view/6822/pdf>



pada saat berada di mobil alat berupa *Skimming Mini Tools* diserahkan kepada terdakwa I dan kemudian alat tersebut oleh terdakwa I dimasukkan kedalam Laptop dengan menggunakan kabel, kemudian terdakwa I membuka software dan data *Skimming Mini Tools* tersebut oleh terdakwa I di simpan di dalam Software setelah selesai terdakwa I ganti membuka *Skimming Mini Tools* pengisi data dengan menggunakan kabel yang terdakwa I sambungkan dengan laptop kemudian menggosokkan ATM yang tidak digunakan kedalam mesin *Skimming* pengisi data dan ATM tersebut sudah bisa digunakan sesuai dengan ATM aslinya, setelah berhasil akhirnya terdakwa mengambil uang tersebut di tempat mesin BRI Link dengan nomor PIN yang sudah dicatat dan diketahui oleh terdakwa II sebelumnya dan terdakwa II melakukan penarikan uang tunai sebanyak 4 (empat) kali dengan jumlah keseluruhan sebesar Rp. 36.000.000,- (tiga puluh enam juta rupiah), bahwa terdakwa I dan terdakwa II dalam mengambil data dalam kartu ATM milik saksi korban tidak seijin dari pemiliknya karena pada saat saksi korban menggosokkan nomor PIN ke BRI Link terlebih dahulu terdakwa II melihat PIN dan kemudian pada saat saksi korban melayani terdakwa I membeli rokok terdakwa II sempat mengambil ATM milik saksi korban di dalam laci.<sup>57</sup>

## **METODE**

Metode *skimming* merupakan metode yang dilakukan pelaku kejahatan bagian perbankan untuk mencuri data-data nasabah yang terdapat dalam kartu ATM nasabah. Modusnya dengan cara memasang alat skimmer pada slot untuk

---

<sup>57</sup> Putusan Pengadilan Negeri Ngawi Nomor 163/Pid.Sus/2020/PN Ngw, halaman 3-4.  
[https://www.sipp.pn-ngawi.go.id/index.php/detil\\_perkara](https://www.sipp.pn-ngawi.go.id/index.php/detil_perkara)

memasukkan kartu ATM pada mesin ATM. Sedangkan ATM adalah salah satu alat elektronik atau sistem elektronik yang digunakan dalam langkah perbankan.

Skimmer bukan satu-satunya alat yang dipakai oleh para pelaku *skimming*. Para pelaku biasanya juga menggunakan kamera pengintai (*spy cam*) untuk mengetahui gerakan jari nasabah saat memasukkan PIN kartu ATM. Namun kamera pengintai sudah jarang dimanfaatkan seiring dengan semakin canggihnya alat skimmer yang digunakan para pelaku. Laman *How Stuff Works* menyampaikan jika kini telah menyebar pula jenis skimmer yang dilengkapi dengan kemampuan membaca kode PIN kartu ATM. Dan hebatnya lagi, skimmer jenis ini juga bisa langsung menyampaikan data-data yang didapat via SMS pada pelaku.<sup>58</sup>

Metode yang digunakan oleh pembobol untuk meretas ATM nasabah yaitu:<sup>59</sup>

#### 1) Pemasangan Alat Skimmer

Teknik *Skimming* Pada ATM Pada saat kita memasukan kartu ATM ke mesin ATM, mesin ATM akan membaca informasi pada kartu ATM anda untuk digunakan sebagai kunci mengakses alat perbankan anda. Salah satu jalan termudah untuk mencuri data informasi pada Kartu ATM anda di mesin ATM yaitu dengan melekatkan alat tambahan (skimmer) di depan mulut tempat anda memasukan kartu ATM. Proses pemasangan Skimmer.

---

<sup>58</sup> Dian Ekawati, *op. cit.* halaman 163.

<sup>59</sup> Diang Alan Setiawan. 2018. Perkembangan Modus Operandi Kejahatan *Skimming* Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime). Era Hukum. Vol. 16 No. 2. halaman 183 <https://journal.untar.ac.id/index.php/hukum/article/view/4526>



**Gambar 1. Proses pemasangan skimmer**

Dengan terempelnya Skimmer pada mulut Atm, setiap nasabah yang datang melakukan transaksi dengan memasukan kartunya ke Atm, sebelum data tersebut dibaca oleh mesin Atm, alat skimmer pun telah membaca dan merekam data kartu anda untuk selanjutnya akan di-copykan ke kartu magnetik lainnya (bodong). Selanjutnya pencuri tinggal mengambil alat skimmernya, dan menduplikasi kartu-kartu Atm milik nasabah-nasabah yang sempat mengakses Atm tersebut.

## 2) Cara mengetahui PIN Nasabah

Para pencuri tersebut memasang hidden camera untuk merekam moment saat kita menekan nomor PIN di ATM tersebut. Camera tersebut bentuknya sangat kecil, dan memiliki internal memory yang cukup besar. Saat ini sangat mudah sekali mendapatkan camera seperti ini di Internet. pemasangan Camera untuk merekam aktifitas pemasukan PIN ATM.



**Gambar 2. Kamera merekam aktifitas**

### 3) Pembuatan Kartu Magnetik Palsu

Saat sang pencuri mengambil kembali skimmer & camera miliknya, dia sudah mendapatkan data-data kartu kita lengkap dengan nomor PIN. Selanjutnya, sang pencuri tinggal membuat kartu magnetic baru dengan data-data kartu kita didalamnya dengan alat yang umum seperti gambar dibawah ini:



**Gambar 3. Kartu magnetic**

Selanjutnya sang pencuri memiliki akses penuh selayaknya pemilik rekening yang dicuri. Untuk meminimasi resiko biasanya sang pencuri memilih ATM yang tidak ada camera CCTV nya, oleh sebab itu tidak

heran mengapa beberapa transaksi yg dilakukan pencuri memilih di ATM bank lain yang tidak memiliki CCTV (*switching*).<sup>60</sup>

## **B. Pengaturan Hukum Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri**

Secara umum dapat dikatakan bahwa hukum perbankan adalah hukum yang mengatur segala sesuatu yang berhubungan dengan perbankan. Tentu untuk memperoleh pengertian yang lebih mendalam mengenai pengertian hukum perbankan tidaklah cukup hanya dengan memberikan suatu rumusan yang demikian. Oleh karena itu, perlu dikemukakan beberapa pengertian hukum perbankan dari para ahli hukum perbankan.<sup>61</sup>

Hukum yang mengatur masalah perbankan disebut hukum perbankan (*Banking Law*) yakni merupakan seperangkat kaidah hukum dalam bentuk peraturan perundang-undangan, yurisprudensi, doktrin, dan lain-lain. Sumber hukum yang mengatur masalah-masalah perbankan sebagai lembaga, dan aspek kegiatannya sehari-hari, rambu-rambu yang harus dipenuhi oleh suatu bank, perilaku petugas-petugasnya, hak, kewajiban, tugas dan tanggung jawab, para pihak yang tersangkut dengan bisnis perbankan, apa yang boleh dan tidak boleh

---

<sup>60</sup> *Ibid.* halaman 184.

<sup>61</sup> Hermansyah. 2014. Hukum Perbankan Nasional Indonesia. Jakarta: Kencana. halaman 39.

dilakukan oleh bank, eksistensi bank, dan lain-lain yang berkenaan dengan dunia perbankan tersebut.<sup>62</sup>

Perbankan sebagai lembaga yang dijalankan atas dasar kepercayaan yang diberikan oleh masyarakat penyimpan dana dapat dengan mudah digoyahkan oleh praktik-praktik kejahatan ekonomi, seperti money launfering, advance fee fraud, penyalahgunaan warkat perbankan, penipuan dan pemalsuan dalam transfer uang secara elektronik. Adakalanya kejahatan ekonomi yang terorganisasi mendirikan phantom atau Bank fiktif atau Shell Bank (bank tanpa aset, tanpa stat) sebagai sarana menjalankan kejahatan mereka. Bank-bank seperti itu biasanya didirikan pada negara-negara yang tidak mempunyai bank sentral yang menjalankan fungsi pengawasan perbankan.

Malahan pada akhir-akhir ini timbul modus operandi kejahatan perbankan dengan mempergunakan sarana canggih berupa "komputer" (kejahatan dengan komputer) seperti yang terjadi pada kasus Mark Rifkin, pembobolan Amex Bank, pembobolan Bank Negara Indonesia 1946 di New York, dan Pembobolan Union Of Switzerland.<sup>63</sup>

Beberapa jenis computer fraud ialah:

1. *Computer input fraud*, yaitu memasukkan program palsu ke dalam data base untuk keuntungan pihak ketiga. Tujuannya adalah mengalihkan bunga ke rekening pembuat program palsu;

---

<sup>62</sup> Zainal Asikin. 2016. Pengantar Hukum Perbankan Indonesia. Jakarta: Rajawali Pers. halaman 19.

<sup>63</sup> *Ibid*, halaman 220

2. *Computer output fraud*, yaitu memanipulasi, mengubah dan merusak hasil output komputer dengan menekan tombol "repeat" yang mengakibatkan biaya pengeluaran suatu barang bisa sesuai dengan keinginan pelaku;
3. *Computer programme fraud*, yaitu dengan memprogramkan suatu instruksi maka suatu perusahaan bisa diuntungkan atau dirugikan;
4. Penyadapan data pada waktu transmisi (pengiriman data kekomputer)

Adapun jenis-jenis penyimpangan dalam dapat diidentifikasi sebagai berikut.

1. Pemindahan/pengrusakan dokumen termasuk instrumen;
2. Pembuatan penyimpangan dengan jalan membuka rekening dengan nama fiktif;
3. Penyimpangan melalui pemalsuan total atau perubahan dokumen/instrumen dengan bahan kimia;
4. Penyimpangan yang dilakukan oleh pegawai bank dengan memanfaatkan rekening tidur;
5. Membuat catatan palsu dalam pembukuan bank;
6. Pinjaman dengan persediaan barang, misalnya menjaminkan persediaan barang yang sama pada beberapa bank yang berbeda.<sup>64</sup>

*skimming* merupakan akibat dari penyalahgunaan oleh pihak ketiga. Yang dimaksud dengan pihak ketiga adalah "hacker dan phreaker, yaitu orang yang pekerjaannya memasuki atau mengakses secara tidak sah suatu sistem komputer

---

<sup>64</sup> *Ibid*

maupun internet”. Adapun cara-cara hacker mencuri data-data nasabah pemegang ATM adalah sebagai berikut:

1. Melalui komputer bank dan perusahaan kartu kredit;
2. Transhing, yaitu suatu cara dimana hacker membongkar/ memeriksa sampah perusahaan-perusahaan atau toko-toko yang diperkirakan menerima melalui kartu ATM.

Terkurasnya dana simpanan nasabah akibat kejahatan *skimming* menunjukkan bahwa nasabah bank tidak mendapatkan perlindungan hukum secara penuh. Bank menggunakan uang nasabah, yang dalam hal ini menghimpun dana sebanyak-banyaknya dalam bentuk simpanan lalu mengelola dana tersebut untuk disalurkan kembali ke kreditur atau nasabah lainnya dalam bentuk pinjaman atau kredit. Nasabah dalam konteks UU Perbankan dapat dibagi menjadi dua, yakni nasabah penyimpan dan nasabah debitur. Berdasarkan Pasal 1 ayat 17 UU Perbankan, “Nasabah penyimpan adalah nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan”. Sementara menurut Pasal 1 ayat (18) UU Perbankan, “Nasabah debitur adalah nasabah yang memperoleh fasilitas kredit atau pembiayaan berdasarkan prinsip syariah atau yang dipersamakan dengan itu berdasarkan perjanjian bank dengan nasabah yang bersangkutan”. Menurut Marhais Abdul Miru, “dalam praktik perbankan nasabah dibedakan menjadi tiga yaitu: Pertama, nasabah deposan yaitu nasabah yang menyimpan dananya pada suatu bank, misalnya dalam bentuk giro, tabungan dan deposito. Kedua, nasabah yang memanfaatkan fasilitas kredit atau pembiayaan perbankan misalnya kredit



kepemilikan rumah. pembiayaan murabahah, dan sebagainya. Ketiga, nasabah yang melakukan transaksi dengan pihak lain melalui bank (*walk in customer*), misalnya transaksi antara importir sebagai pembeli dengan eksportir di luar negeri dengan menggunakan fasilitas *letter of credit (L/C)*”.<sup>65</sup>

ATM adalah sarana transaksi perbankan yang ada di bawah pengawasan bank sehingga bank bertanggung jawab atas segala akibat yang disebabkan oleh ATM sesuai ketentuan Pasal 1367 BW. *Skimming* adalah perbuatan pencurian data kartu ATM nasabah dengan cara menyalin informasi pada *strip magnetic* secara ilegal. Akibat perbuatan *skimming* adalah uang nasabah yang dipercayakan dalam bank dapat diambil secara melawan hukum. Dikatakan melawan hukum karena tanpa sepengetahuan dan persetujuan dari nasabah atau pemilik uang yang dipercayakan dalam bank. *Skimming* yang berakibat hilangnya atau berkurangnya uang nasabah di bank jelas merupakan tanggung jawab bank karena alat yang digunakan, yang dalam hal ini adalah mesin ATM, adalah sarana di bawah pengawasan dan kepemilikan bank. Pertanggungjawaban bank terhadap hilangnya dana simpanan nasabah ditinjau dari regulasi yang diterapkan oleh regulator jasa keuangan, yaitu pihak bank harus bertanggung jawab atas hilangnya dana simpanan nasabah dan kerugian yang menimpa nasabah. Hal ini tertuang dalam Pasal 19 ayat (1) UU Perlindungan Konsumen, yakni “Pelaku usaha bertanggung jawab memberikan ganti rugi atas kerusakan, pencemaran, dan/atau kerugian konsumen akibat mengkonsumsi barang dan/atau jasa yang dihasilkan atau diperdagangkan”.

---

<sup>65</sup> Victoria Linggoraharjo. 2020. Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming. *Argumentum*. Vol. 7 No. 1. halaman 41.  
<https://journal.ubaya.ac.id/index.php/argu/article/download/3013/2261/>

Tanggung jawab bank atas hilangnya dana simpanan nasabah juga tertuang dalam Pasal 10 PBI No. 16/1/PBI/2014 yakni “Penyelenggara wajib bertanggung jawab kepada Konsumen atas kerugian yang timbul akibat kesalahan pengurus dan pegawai Penyelenggara.” Dipertegas dalam Pasal 29 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan (selanjutnya disebut sebagai POJK No.1/POJK.07/2013), bahwa “Pelaku Usaha Jasa Keuangan wajib bertanggung jawab atas kerugian Konsumen yang timbul akibat kesalahan dan/atau kelalaian, pengurus, pegawai Pelaku Usaha Jasa Keuangan dan/atau pihak ketiga yang bekerja untuk kepentingan Pelaku Usaha Jasa Keuangan”. Kecuali pelaku *skimming* ditemukan, yang dalam hal ini nasabah tetap meminta pertanggungjawaban atau pengembalian kerugian di bank karena berawal dari perikatan nasabah dan bank yang mempercayakan uangnya untuk dikelola bank, baru pihak bank akan menindaklanjuti dengan pelaku *skimming* yang tertangkap.<sup>66</sup>

Rekening, yakni suatu persiapan untuk menyimpan data-data transaksi perbankan yang berharga berupa aset, tanggungan, modal, pendapatan dan dana. Tujuan utama pemanfaatan rekening yakni untuk menyimpan data yang akan menjadikan dasar pembentukan laporan dalam kegiatan perbankan. Nilai jumlah rekening yang ditempatkan dalam pendataan suatu rekening didasarkan pada seberapa besar kepentingan pemilik rekening tersebut.

Anjungan Tunai Mandiri memiliki kegunaan bagi seluruh masyarakat yaitu: Kartu kredit atau debit yang dapat dimanfaatkan tanpa harus membayar secara

---

<sup>66</sup> *Ibid.* halaman 42.

tunai. Kartu Kredit bisa dimanfaatkan untuk melakukan pembayaran dalam situasi yang penting. Ada beberapa jenis Kartu Kredit dan debit yang memungkinkan dapat diterima oleh seluruh mesin Anjungan Tunai Mandiri (ATM) di dunia dan mencatat keseluruhan transaksi setiap bulannya.

Dapat dikatakan fungsi Rekening Anjungan Tunai Mandiri (ATM) menurut penulis adalah dalam sebuah pembayaran tanpa memanfaatkan uang tunai dan sangat mudah dipakai hanya dengan membawa kartu debit atau kredit Anjungan Tunai Mandiri (ATM). Jika kartu debit atau kredit Anjungan Tunai Mandiri (ATM) itu hilang bisa segera memberitahukan kepada pihak Bank yang bersangkutan dan dapat dilakukan pemblokiran sehingga uang yang ada di Kartu debit atau kredit tersebut tidak hilang. Serta adanya mutasi rekening jika ada yang menggunakan kartu debit atau kredit tidak diketahui pemilik.

Rekening ATM memiliki dasar hukum yaitu terdapat pada Pasal 3 ayat (3) UUD 1945, Pasal 1 ayat (1) Kitab Undang-undang Hukum Pidana, Pasal 1 ayat (1) UU Nomor. 10 Tahun 1998, Pasal 1 ayat (16) UU Nomor. 10 Tahun. 1998, Pasal 1 ayat (17) UU Nomor. 10 Tahun 1998, Pasal 1 ayat (18) UU Nomor. 10 Tahun 1998, Pasal 1 ayat (19) UU Nomor. 10 Tahun 1998.

Kejahatan perbankan melalui metode *skimming* masih kerap terjadi. sebagai pemegang rekening atau kartu Anjungan Tunai Mandiri (ATM) haruslah berhati-hati karena para pelaku *skimming* memiliki cara-cara yang canggih untuk membobol Anjungan Tunai Mandiri (ATM). Biasanya pelaku menggunakan

komputer/ laptop, software decoder hingga encoder kartu khusus. Kartu magnetik baru dan pembaca kartu tersebut.

Dasar hukum pada kejahatan tindak pidana skimming yaitu: Pasal 55 ayat (1) KUHP, Pasal 362 KUHP, Pasal 2 ayat (1) Undang-Undang No. 8 Tahun 2010, Pasal 5 ayat (1) UU Nomor. 8 Tahun 2010, Pasal 30 ayat (1) UU Nomor. 11 Tahun 2008, Pasal 30 ayat (3) UU Nomor. 11 Tahun 2008, Pasal 32 ayat (2) Undang-Undang No. 11 Tahun 2008, Pasal 32 ayat (3) UU Nomor. 11 Tahun 2008, Pasal 36 UU Nomor. 11 Tahun 2008, Pasal 81 UU Nomor. 3 Tahun 2011, Pasal 83 ayat (1) UU Nomor. 3 Tahun 2011, Pasal 83 ayat (2) UU Nomor. 3 Tahun 2011, UU No. 10 Tahun 1998 tentang Perbankan, UU No. 36 Tahun 1999 tentang Telekomunikasi.

Cara menghindari dari kejahatan skimming yaitu: dengan mengecek lokasi Anjungan Tunai Mandiri (ATM) apakah strategis atau berada di tempat yang sepi, melakukan penggantian pin secara berkala, memantau saldo secara rutin, dan memperketat daftar otentifikasi bank.<sup>67</sup>

Tindak pidana di bidang perbankan juga tidak hanya mencakup pelanggaran terhadap undang-undang perbankan saja, melainkan mencakup pula tindak pidana penipuan, penggelapan, pemalsuan dan tindak pidana-tindak pidana lainnya sepanjang berkaitan dengan lembaga perbankan. Suatu perbuatan dapat dikatakan sebagai tindak pidana di bidang perbankan manakala perbuatan tersebut

---

<sup>67</sup> Komang Saeramessatya Purwadi Sastra, dkk. 2020. Sanksi Pidana Terhadap Tindak Pidana Pembobolan Rekening Melalui Anjungan Tunai Mandiri (ATM). Jurnal Analogi Hukum. Vol 2. No 2. halaman 237 <file:///C:/Users/User/Downloads/Documents/1913-Article%20Text-8874-2-10-20200720.pdf>

berkaitan dengan lembaga perbankan meskipun perbuatan itu merupakan tindak pidana berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) [misalnya Pasal 378, 372, 374, 263, 362, 363 ayat (1) ke-4, 244-250, 250 bis] dan peraturan undang-undangan hukum pidana khusus lainnya, misalnya Undang-Undang Republik Indonesia Nomor 31 Tahun 1999 sebagaimana telah diubah oleh Undang-Undang Republik Indonesia Nomor 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi, Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang dan lain sebagainya.

Dalam praktik banyak dijumpai perbuatan-perbuatan di bidang perbankan yang dapat dikenakan sanksi sebagaimana ditetapkan dalam Kitab Undang-Undang Hukum Pidana (KUHP) ataupun perundang-undangan lain yang berlaku di Indonesia. Jenis-jenis tindak pidana dimaksud dapat dikelompokkan berdasarkan kegiatan bidang perbankan, yaitu:

- a. Di bidang lalu lintas pembayaran giral dan peredaran uang, seperti pemalsuan warkat bank (Pasal 263 dan 264 KUHP), tindak pidana penggelapan dalam kegiatan usaha perbankan dalam lembaga penyimpanan barang dan surat berharga dalam safe deposit box, serta lembaga penitipan untuk kepentingan pihak lain. Dalam hal tindak pidana penggelapan tersebut dapat dikenakan ketentuan Pasal 372 KUHP, Pasal 374 KUHP, dan Pasal 415 KUHP, pemalsuan uang dan uang yang dimanipulasikan (Pasal 244 dengan Pasal 252 KUHP), memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada

Sistem Elektronik Orang lain yang tidak berhak (Pasal 32 ayat (2) dan Pasal 35 Undang-Undang republik Indonesia No. 11 tahun 2008 sebagaimana telah diubah dengan undang-undang republik Indonesia No. 19 tahun 2016).<sup>68</sup>

- b. Tindak pidana di bidang perkreditan, seperti penipuan (Pasal 378 KUHP) dan pemalsuan dokumen (Pasal 263 dan 264 KUHP) serta Undang-Undang Republik Indonesia No. 7/Drt/1955 tentang Tindak Pidana Ekonomi.
- c. Tindak pidana pemalsuan dan penggandaan agunan kredit verband di mana objek krediet verband yang ada bukan merupakan haknya dan/atau diagunkan beberapa kali dengan tanpa sepengetahuan pihak lain (bank dan orang yang mempunyai atau turut mempunyai hak kebendaan). Rumusan tindak pidana ini terdapat dalam ketentuan Pasal 385 KUHP.
- d. Tindak pidana persaingan curang. Semakin meningkatnya persaingan antarbank dewasa ini, tidak menutup kemungkinan adanya persaingan tidak sehat (curang) di antara kompetitor, baik untuk menguntungkan diri sendiri maupun orang lain (perusahaannya). Salah satu bentuk dari persaingan curang yang dimaksud di antaranya ialah penyebaran isu (kabar bohong) tentang bank yang kalah kliring. Terhadap tindak pidana tersebut dapat dikenakan ketentuan Pasal 382 bis dan Pasal 390 KUHP.<sup>69</sup>

---

<sup>68</sup> Kristian dan Yopi Gunawan. 2018. Tindak Pidana Perbankan Dalam Proses Peradilan Di Indonesia. Jakarta : Kencana. halaman 28

<sup>69</sup> *Ibid*

Tindak pidana perbankan merupakan tindak pidana yang lazimnya dilakukan oleh orang-orang yang mempunyai kemampuan intelektual dan mempunyai posisi penting di dalam masyarakat atau pekerjaannya. Adapun tindak pidana di bidang perbankan merupakan salah satu bentuk dari tindak pidana di bidang ekonomi, yaitu tindak pidana konvensional yang mencari keuntungan dengan motif-motif ekonomi seperti: pencurian, penggelapan, perampokan, penipuan, dan lain sebagainya yang dalam hal ini ditunjukkan terhadap bank atau setidaknya berhubungan dengan lembaga perbankan sehingga bank mengalami kerugian. Dalam pengertian yang demikian, maka dalam istilah “tindak pidana di bidang perbankan” tercakup perbuatan-perbuatan melawan hukum yang menjadikan bank sebagai sarana atau media (*crimes throug the bank*) atau bank sebagai sasaran dari suatu tindak pidana (*crimes against the bank*).<sup>70</sup>

Berbicara mengenai pertanggungjawaban pidana, hukum pidana mengenal asas legalitas (*principle of legality*), yang tertuang dalam Pasal 1 ayat (1) KUHP, yaitu setiap perbuatan pidana harus dirumuskan oleh suatu aturan undang-undangan sebelum perbuatan seseorang dapat dipidana. *Skimming* merupakan kejahatan yang dalam KUHP secara konvensional tindak pidana Pasal 263 KUHP dan Pasal 362 KUHP. Pengertian “membuat surat palsu” menurut Chainur Arrasjid adalah “membuat surat sedemikian rupa seakan-akan berasal dari sumber yang benar atau berhak untuk membuat surat tersebut sama sekali dari pihak yang tidak benar atau tidak berhak. Sedangkan pengertian “memalsukan surat” adalah “mengadakan perubahan dan isinya, sehingga sebab perubahan tersebut

---

<sup>70</sup> *Ibid*

mengakibatkan materi atau substansi surat tersebut tidak sesuai lagi dengan isi yang sebenarnya atau dengan kata lain sudah tidak sesuai lagi dengan redaksi atau bunyi aslinya”. Tindakan pelaku skimming yang dengan sengaja mendapatkan data nasabah secara melawan hukum yang kemudian mengkloning data yang diperoleh secara melawan hukum ke dalam kartu ATM yang kosong untuk melakukan aksi skimming merupakan perbuatan “membuat surat palsu”. Perbuatan pelaku skimming yang menggunakan surat palsu sehingga mengakibatkan kerugian terhadap nasabah memenuhi unsur-unsur pidana sebagaimana tertuang dalam Pasal 263 KUHP.<sup>71</sup>

### **C. Tinjauan Yuridis Pencurian Data Nasabah Perbankan Melalui Anjungan Tunai Mandiri**

Pengertian Tindak pidana dalam bidang perbankan dan tindak pidana perbankan memiliki perbedaan mendasar. Pengertian pertama harus ditafsirkan perbuatan dalam bidang perbankan yang diperkuat dengan sanksi pidana, sedangkan pengertian kedua, perbuatan yang bersanksi pidana. Perbedaan kedua, pengertian pertama mengutamakan sanksi administratif sebagai *primum remedium* dan sanksi pidana merupakan *ultimum remedium*. Adapun pengertian kedua, sanksi pidana merupakan *primum remedium* dan sanksi administratif merupakan *ultimum remedium*. Perbedaan ketiga, pengertian pertama bertujuan memulihkan secara administratif kerugian terhadap pihak korban sedangkan pengertian kedua, menghukum pihak yang merugikan. Perbedaan ketiga, pengertian pertama

---

<sup>71</sup> *Ibid*



menghendaki ancaman sanksi yang lebih ringan dibandingkan dengan pengertian kedua.<sup>72</sup>

Dalam penyusunan ketentuan sanksi dalam UU Perbankan seharusnya semua ketentuan sanksi terhadap pelaku perbankan cukup merujuk pada ketentuan KUHP. Hal ini didukung oleh penempatan beberapa perbuatan dalam UU Perbankan masih membedakan perbuatan sebagai kejahatan dan sebagai pelanggaran. Penulis sependapat agar penggunaan terminologi kejahatan dalam lingkup UU Perbankan harus secara hati-hati dan selektif dengan mempertimbangkan implikasinya terhadap kepercayaan masyarakat terhadap dunia usaha perbankan.<sup>73</sup>

Tindak Pidana *skimming* telah sesuai dengan Pasal 46 ayat (2) UU ITE yang menjelaskan sebagai berikut: “Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)”. Pasal 30 ayat (2) tersebut menjelaskan perbuatan memperoleh Informasi Elektronik dan/atau Dokumen Elektronik menjelaskan sebagai berikut: “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik”.

Sehingga ketentuan yang diuraikan dalam Pasal 30 ayat (2) UU ITE tersebut dapat dijabarkan ke dalam unsur-unsur sebagai berikut:

---

<sup>72</sup> Romli Atmasasmita. 2021. Hukum Dan Penegakan Hukum. Jakarta: Kencana. halaman 81

<sup>73</sup> *Ibid*

- a. Sengaja
- b. Tanpa hak atau melawan hukum
- c. Mengakses Komputer dan/atau Sistem Elektronik
- d. Tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik

Terkait dengan unsur kesengajaan sebenarnya menjelaskan terkait dengan bentuk kesalahan pada delik yang diatur. Pengaturan terhadap bentuk kesalahan secara jelas ini berarti pembentukan pasal ini dilakukan dengan pandangan monistis, dimana dalam perbuatan pidana unsur perbuatan dan kesalahan merupakan satu kesatuan. Kesalahan haruslah memiliki kesengajaan (*Dolus*) atau kealpaan (*Culpa*). Pada perbuatan memperoleh data nasabah dengan Skimmer jelas memiliki unsur kesengajaan sebagai maksud untuk memperoleh data nasabah itu sendiri.<sup>74</sup>

Unsur tanpa hak atau melawan hukum menjelaskan terkait dengan sifat dari tindak pidana tersebut hanya dilanggar bila dilakukan tanpa hak atas akses komputer dan/atau Sistem Elektronik atau dilakukan dengan melawan hukum. Pada skimming, perbuatan memperoleh data pribadi nasabah memiliki sifat melawan hukum yang jelas yang melanggar ketentuan peraturan perundangundangan. Perbuatan melawan hukum tersebut perlu memperhatikan Pasal 26 ayat (1) UU ITE yang menjelaskan: “kecuali ditentukan lain oleh peraturan perundangundangan, penggunaan setiap informasi melalui media

---

<sup>74</sup> Michael Enrick. 2019. Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dengan Pengajuan Restitusi. *Juris-Diction*. Vol 2. No 2. halaman 569. <https://ojs2.e-journal.unair.ac.id/JD/article/view/14252/7941>

elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan”. Sehingga berdasarkan ketentuan tersebut jelaslah bahwa memperoleh data nasabah yang dilakukan tanpa hak adalah perbuatan melawan hukum.

Kemudian unsur mengakses Komputer dan/atau Sistem Elektronik merupakan unsur perbuatan dalam tindak pidana yang diatur dalam tindak pidana skimming. Pada Pasal 1 angka 14 UU ITE mendefinisikan “Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan”. Kemudian pada Pasal 1 angka 5 UU ITE “Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik”.

Dalam memperoleh data nasabah atau korban, pelaku menggunakan alat yang bernama skimmer untuk mengakses data nasabah dimana akses yang dilakukan oleh pelaku ditujukan pada kartu elektronik yang berisi data nasabah. Berdasarkan definisi Informasi Elektronik maka pada dasarnya adalah data elektronik yang secara luas dengan bentuk yang tidak terbatas pada apa yang dijelaskan dari pengertian Informasi Elektronik itu sendiri. Sehingga apabila dikaitkan dengan analisa terkait perolehan data pribadi nasabah atau korban yang dapat dijabarkan

sebagai informasi elektronik maka unsur tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik jelas terpenuhi.<sup>75</sup>

Terkait unsur-unsur subjektif pada perbuatan melakukan transaksi atas nama nasabah menggunakan kartu elektronik palsu jelas terpenuhi. Unsur maksud untuk menguntungkan diri sendiri atau orang lain, jelas terlihat dari rangkaian perbuatan yang telah dijelaskan pada bagian Modus Operandi yakni tujuan perolehan uang sebagai tujuan akhir dari “pembobolan bank” itu sendiri. Sedangkan unsur secara melawan hukum terlihat dari penggunaan kartu elektronik palsu yang berisi data nasabah yang telah diperoleh yang merupakan hasil dari tindak pidana.

Unsur menggunakan nama palsu, atau martabat palsu, atau tipu muslihat, atau rangkaian kebohongan merupakan unsur perbuatan. Pada unsur ini perbuatan yang disyaratkan disusun secara alternatif, pemenuhan salah satu perbuatan saja cukup untuk memenuhi unsur tersebut. Pada transaksi atas nama nasabah menggunakan kartu elektronik palsu melibatkan baik mesin ATM ataupun mesin debit, yang mana dapat diartikan sebagai Komputer, jaringan Komputer, dan/atau media elektronik lainnya dalam definisi transaksi elektronik dalam Pasal 1 angka 2 Undang-Undang Informasi dan Transaksi Elektronik. Karena transaksi tersebut merupakan Transaksi Elektronik, maka cara transaksi dilakukan merupakan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana diatur dalam Pasal 17 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik. Dengan terbatasnya interaksi dalam Transaksi Elektronik pada Informasi Elektronik dan/atau Dokumen Elektronik, maka pada transaksi

---

<sup>75</sup> *Ibid*

atas nama nasabah menggunakan kartu elektronik palsu, penggunaan Informasi Elektronik berupa data pribadi nasabah oleh pelaku merupakan bentuk dari nama palsu dan martabat palsu.

Unsur menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang berarti ada orang yang terbujuk untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang. Pada transaksi dengan kartu palsu, secara fisik yang bertemu adalah pelaku dengan mesin. Mesin ATM adalah mesin/ komputer yang digunakan oleh bank untuk melakukan kegiatan-kegiatan penyetoran uang, pengambilan uang, pengecekan saldo, transfer antar rekening, dan transaksi keuangan lain yang dilakukan secara elektronik.<sup>76</sup>

Kasus pembobolan beberapa rekening nasabah dari berbagai Bank besar di Indonesia saat ini telah menjadi buah bibir dan pembicaraan hangat di media massa dan masyarakat. Lantas bagaimana para penegak hukum, pihak perbankan dan pemerintah dalam menyikapi kejadian ini guna memberikan rasa aman bagi para nasabah. Untuk itulah adanya Undang-undang yang akan mengatur setiap tindakan warga negara agar selalu bertindak pada koridor yang benar di mata hukum. Tidak terkecuali tindakan yang dilakukan melalui perangkat elektronik yang dapat melanggar hukum.<sup>77</sup>

---

<sup>76</sup> Ronny Prasetya. 2010. Pembobolan ATM Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan. Jakarta: Prestasi Pustaka. halaman 12.

<sup>77</sup> *Ibid.* halaman 38

Dalam kasus Pembobolan ATM Bank yang banyak terjadi saat ini, pelaku pembobolan rekening nasabah bank bisa dijerat dengan pasal-pasal dalam Undang-undang Informasi dan Transaksi Elektronik (UU ITE). Dengan ancaman hukumannya bisa sampai 12 tahun kurungan dan denda Rp 12 miliar.

UU ITE yang bisa digunakan untuk menjerat para pelaku pembobolan atm bank, yakni pasal 30 ayat 1 30 ayat 3, pasal 32 ayat 2, dan pasal 36.

Adapun isi pasal-pasal tersebut adalah sebagai berikut:

Pasal 30 ayat 1, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem elektronik milik orang lain dengan cara apapun."

Pasal 30 ayat 3, "Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem elektronik dengan melanggar, menerobos, melampau, atau menjebol sistem pengamanan."

Pasal 32 ayat 2, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak."

Pasal 36, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 yang mengakibatkan kerugian bagi orang lain."<sup>78</sup>

Dalam penerapan undang-undang ITE terkait skimming tidak memberikan istilah yuridis secara jelas dan tegas suatu tindakan mengakses, memindahkan, dan/atau mentransmisikan sebagai suatu tindakan skimming. Sehingga dalam penerapannya jika ingin mengenakan skimming dengan UU ITE perlu dilakukan penafsiran agar dapat dikenakan undang-undang tersebut. Definisi skimming identik dengan frasa copy atau menyalin, maka konsep skimming harus dikaitkan dengan Pasal 1 angka 15 UU ITE tentang konsep akses. Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan. Berdasarkan konsep tersebut akses terkait dengan skimming dilakukan dengan cara saat pemilik kartu melakukan transaksi di mesin ATM dengan memasukkan kartu debit/kredit pada skimmer yang terlihat seperti slot kartu aslinya, kemudian informasi elektronik yang ada pada kartu tersebut telah tersalin dan tersimpan dalam skimmer agar dapat diakses oleh pelaku.<sup>79</sup>

Tindakan mengakses yang dilakukan oleh pelaku dengan tujuan memperoleh data atau dokumen elektronik dan memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik miliknya dan atau orang lain dengan mengirim mempergunakan transmisi kepada orang yang tidak berhak, kemudian memindahkan atau mentransfer ke dalam kartu

---

<sup>78</sup> *Ibid*

<sup>79</sup> Destya Fidela Pratiwi. 2019. Pertanggungjawaban Tindak Pidana Skimming, *Juris-Diction* Vol 2. No 4. halaman 1224. <https://e-journal.unair.ac.id/JD/article/view/14488/8014>

kosong/bodong lain dan dipergunakan untuk melakukan transaksi elektronik, dengan pemanfaatan yang dilakukan oleh plegen, dan atau doen plegen atau medeplegen tersebut menimbulkan kerugian bagi pemilik kartu/nasabah dan pihak Bank. Pelaku tindak pidana skimming dalam perumusan Pasal 30 ayat (1), ayat (2), dan ayat (3) karena adanya perbuatan mengakses dikenai sanksi pidana sebagaimana yang diatur dalam Pasal 46 ayat (1), ayat (2), dan ayat (3) UU ITE.

Oleh karena itu jika unsur objektif dan subjektif dalam Pasal 30 atau 32 UU ITE dapat dibuktikan bahwa pelaku melakukan kesalahan atau menimbulkan kerugian, maka akan dikenakan sanksi pidana sebagaimana diatur dalam Pasal 46 apabila terbukti melanggar Pasal 30 maupun Pasal 48 apabila melanggar Pasal 32 tersebut dan pengenaan sanksi pidana ini merupakan pertanggungjawaban pidana bagi pelaku tindak pidana skimming. Dalam UU ITE tidak mengatur secara jelas siapa saja yang dapat dikatakan sebagai pelaku, sehingga pemahaman seseorang dianggap sebagai pelaku agar dapat dihukum mengikuti pengaturan dalam Pasal 55 ayat (1) ke-1e KUHP, yaitu orang yang melakukan peristiwa pidana meliputi orang yang melakukan, yang menyuruh melakukan, atau turut melakukan perbuatan itu.<sup>80</sup>

---

<sup>80</sup> *Ibid*



## BAB IV

### KESIMPULAN DAN SARAN

#### A. Kesimpulan

Berdasarkan Pemaparan diatas, dapat ditarik kesimpulan sebagai berikut:

1. Modus Operandi adalah cara proses orang-perorang atau kelompok penjahat dalam melakukan aksi rencana kejahatannya. Metode *skimming* merupakan metode yang dilakukan pelaku kejahatan bagian perbankan untuk mencuri data-data nasabah yang terdapat dalam kartu ATM nasabah. Modusnya dengan cara memasang alat skimmer pada slot untuk memasukan kartu ATM pada mesin ATM. Sedangkan ATM adalah salah satu alat elektronik atau sistem elektronik yang digunakan dalam langkah perbankan.
2. Dasar hukum pada kejahatan tindak pidana skimming yaitu: Pasal 55 ayat (1) KUHP, Pasal 362 KUHP, Pasal 2 ayat (1) Undang-Undang No. 8 Tahun 2010, Pasal 5 ayat (1) UU Nomor. 8 Tahun 2010, Pasal 30 ayat (1) UU Nomor. 11 Tahun 2008, Pasal 30 ayat (3) UU Nomor. 11 Tahun 2008, Pasal 32 ayat (2) Undang-Undang No. 11 Tahun 2008, Pasal 32 ayat (3) UU Nomor. 11 Tahun 2008, Pasal 36 UU Nomor. 11 Tahun 2008, Pasal 81 UU Nomor. 3 Tahun 2011, Pasal 83 ayat (1) UU Nomor. 3 Tahun 2011, Pasal 83 ayat (2) UU Nomor. 3 Tahun 2011, UU No. 10 Tahun 1998 tentang Perbankan, UU No. 36 Tahun 1999 tentang Telekomunikasi.

3. Dalam memperoleh data nasabah atau korban, pelaku menggunakan alat yang bernama skimmer untuk mengakses data nasabah dimana akses yang dilakukan oleh pelaku ditujukan pada kartu elektronik yang berisi data nasabah. Berdasarkan definisi Informasi Elektronik maka pada dasarnya adalah data elektronik yang secara luas dengan bentuk yang tidak terbatas pada apa yang dijelaskan dari pengertian Informasi Elektronik itu sendiri. Sehingga apabila dikaitkan dengan analisa terkait perolehan data pribadi nasabah atau korban yang dapat dijabarkan sebagai informasi elektronik maka unsur tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik jelas terpenuhi.

## **B. Saran**

1. Pada saat melakukan Transaksi di mesin ATM hendaknya kepada masyarakat harus memerhatikan mesin ATM tersebut benar-benar aman pada saat memasukkan kartu ATM.
2. Sangat diperlukannya peraturan perundang-undangan yang lebih dalam lagi mengenai kejahatan tindak pidana skimming untuk menjamin perlindungan dan memberikan kepastian hukum baik kepada nasabah.
3. Pemerintah atau penegak hukum harus melaksanakan tindakan hukum atau upaya penaggulangan terhadap kasus skimming di ATM atau ditempat yang berkemungkinan bisa terjadi skimming, dengan memakai Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas UU 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai peraturan untuk menjerat pelaku tindak pidana skimming.

## DAFTAR PUSTAKA

### A. Buku-buku

- Rosadi, S. D. 2015. *Cyberlaw “Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Bandung: Refika Aditama.
- Army, E. 2020. *Bukti Elektronik Dalam Praktik Peradilan*, Jakarta: Sinar Grafika,
- Nopriansyah, W. 2019. *Aspek Hukum Perbankan Syariah di Indonesia*. Jakarta: Prenadamedia.
- Budhijanto, D. 2017. *Revolusi Cyberlaw Indonesia “Pembaruan dan Revisi Undang-undang Informasi dan Transaksi Elektronik 2016*. Bandung: Refika Aditama.
- Satria, H. 2022. *Hukum Pidana Khusus*. Depok: Rajawali Pers.
- Hermansyah. 2020. *Hukum Perbankan Nasional Indonesia*. Jakarta: Kencana.
- Khaedhir, K. A. 2022. *Pengantar Hukum Indonesia*. Depok: Rajawali Pers.
- faisal. 2021. *Hukum Pidana “Dalam dinamika asas, teori, dan pendapat ahli pidana”*. Jakarta: Kencana.
- Hamid, S. R. 2017. *1500 Hadist dan Sunnah Pilihan*. Jakarta: Kaysa Media.
- Ida Hanifah, dkk. 2018, “*Pedoman Penulisan Tugas Akhir Mahasiswa*.”, Medan, CV Pustaka Prima.
- Suteki, T. G. 2018. *Metodologi Penelitian Hukum “Filsafat, Teori, dan Praktik”*, Depok: Rajawali Pers.
- Butarbutar, N.E. 2018. *Metode Penelitian Hukum “Langkah-langkah untuk Menemukan Kebenaran dalam Ilmu Hukum”*, Bandung: PT Refika Aditama.
- Zaidan, A. 2015. *Menuju Pembaruan Hukum Pidana*. Jakarta: Sinar Grafika.
- Sukardi. 2020. *Restorative Justice Dalam Penegakan Hukum Pidana Indonesia*. Depok: Rajawali Pers.
- Rohim. 2017. *Modus Operandi*. Depok: Alta Utama.
- Alfitra, 2014. *Modus Operandi Pidana Khusus di Luar KUHP*, Jakarta: RAS.
- Prasetya, R. 2010. *Pembobolan ATM, Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan*. Jakarta: PT. Prestasi Pustaka.

- Kristian, Y. G. 2018. *Tindak Pidana Perbankan Dalam Proses Peradilan Di Indonesia*. Jakarta : Kencana.
- Trisnadi, A. S. 2017. *Hukum Perbankan*. Jakarta: Kencana.
- Sutedi. A. 2010. *Hukum Perbankan "Suatu Tinjauan Pencucian Uang, Merger, Likuidasi, dan Kepailitan*. Jakarta: Sinar Grafika.
- Dikdik, E. G. 2005. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: PT Refika Aditama.
- Maskun. 2013. *Kejahatan Siber Cyber Crime*. Jakarta: Kencana.
- Sugiharto, R. T. 2010. *Tips ATM Anti Bobol: Mengenal Modus-modus Kejahatan Lewat ATM dan Tips Cerdik Menghindarinya*, Yogyakarta: Media Pressindo.
- Asikin, Z. 2016. *Pengantar Hukum Perbankan Indonesia*. Jakarta: Rajawali Pers.
- Atmasasmita, R. 2021. *Hukum Dan Penegakan Hukum*. Jakarta: Kencana.
- Wahid, N. 2021. *Perbankan Syariah "Tinjauan Hukum Normatif dan Hukum Positif"*. Jakarta: Kencana.

## **B. Artikel, Makalah, Jurnal dan Karya Ilmiah**

- Faisal Riza, R. A. 2019. *Alternatif Penyelesaian Sengketa Secara Arbitrase Melalui Pemanfaatan Teknologi Informasi*. Jurnal De Lega Lata, Vol. 4 No.1.
- Gani, A. G. 2018. *Cybercrime "Kejahatan Berbasis Komputer"*. Jurnal Sistem Informasi, Vol. 5 No. 1.
- Ketaren, E. 2016. *Cybercrime, Cyber Space, dan Cyber Law*. Jurnal Times, Vol.V No. 2
- Wardani, D. E. 2019. *Kejahatan Skimming Sebagai Salah Satu Bentuk Cyber Crime*. Jurisprudentie, Vol 6 No. 1
- Enrick, M. 2019. *Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dengan Pengajuan Restitusi*. Jurist-Diction. Vol. 2 No. 2.
- Ekawati, D. 2018. *Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan*. Unes Law Riview. Vol.1 No. 2.

- Setiawan, A. D. 2018. *Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime)*. Era Hukum. Vol. 16 No. 2.
- Linggoraharjo, V. 2020. *Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming*. Argumentum. Vol. 7 No. 1.
- Sastra, P. S. K. dkk. 2020. *Sanksi Pidana Terhadap Tindak Pidana Pembobolan Rekening Melalui Anjungan Tunai Mandiri (ATM)*. Jurnal Analogi Hukum. Vol 2. No 2.
- Pratiwi, F. D. 2019. *Pertanggungjawaban Tindak Pidana Skimming, Juris-Diction* Vol 2. No 4.
- Mappanyukki, T. A. 2022. *Analisis Tindak Pidana Skimming Oleh Kepolisian Daerah Sulawesi Selatan*. IJI Publication. Vol. 3 No. 1.
- Nurwijayanti KN, G. E. S. 2020. *Analisa Jaringan Mesin Automatic Teller Machine (ATM) Dalam Rangka Pemeliharaan Di Pulau Jawa*. Jurnal Teknologi Industri, Vol. 9 No. 1.

### **C. Peraturan Perundang-undangan**

Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik