

**SANKSI PIDANA *CYBERFRAUD* DALAM UNDANG-UNDANG
NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN
TRANSAKSI ELEKTRONIK DITINJAU
MENURUT HUKUM PIDANA ISLAM**

SKRIPSI



Diajukan oleh:

AL-VIRATUN

NIM. 160104003

Mahasiswa Fakultas Syari'ah Dan Hukum
Prodi Hukum Pidana Islam

**FAKULTAS SYARI'AH DAN HUKUM
UNIVERSITAS ISLAM NEGERI AR-RANIRY
BANDA ACEH
2020 M/ 1441 H**

**SANKSI PIDANA *CYBERFRAUD* DALAM UNDANG-
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI
DAN TRANSAKSI ELEKTRONIK DITINJAU
MENURUT HUKUM PIDANA ISLAM**

SKRIPSI

Diajukan Kepada Fakultas Syari'ah dan Hukum
Universitas Islam Negeri Ar-Raniry Darussalam Banda Aceh
Sebagai salah satu Beban Studi Program Sarjana (S1)
Dalam Ilmu Hukum Pidana Islam

Oleh:

AL-VIRATUN

NIM. 160104003

Mahasiswi Fakultas Syari'ah Dan Hukum
Prodi Hukum Pidana Islam

Disetujui untuk Dimunaqasyahkan oleh:

Pembimbing I,

Pembimbing II,

Dr. Abdul Jalil Salam, S. Ag., MA.
NIP . 197011091997031001

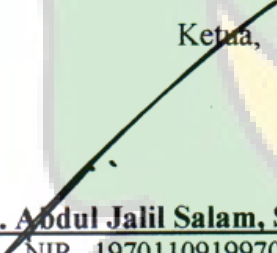
Syarifah Rahmatillah, M. H.
NIP . 198204152014032002

**SANKSI PIDANA *CYBERFRAUD* DALAM UNDANG-
UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI
DAN TRANSAKSI ELEKTRONIK DITINJAU
MENURUT HUKUM PIDANA ISLAM**

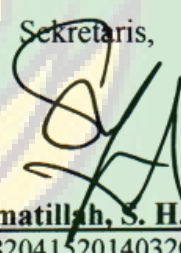
SKRIPSI

Telah Diuji oleh Panitia Ujian Munaqasyah Skripsi
Fakultas Syariah dan Hukum UIN Ar-Raniry
Dan Dinyatakan Lulus Serta Diterima
Sebagai Salah Satu Beban Studi
Program Sarjana (S-1)
Dalam Hukum Pidana Islam
Pada Hari/Tanggal: Selasa, 14 Juli 2020 M
22 Dzulqa'dah 1441 H
Di Darussalam, Banda Aceh
Panitia Ujian Munaqasyah Skripsi:

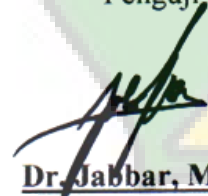
Ketua,


Dr. Abdul Jalil Salam, S. Ag., MA.
NIP. 197011091997031001

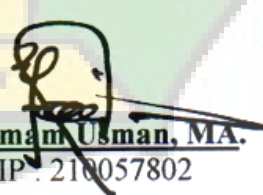
Sekretaris,


Syarifah Rahmatillah, S. H., M. H.
NIP. 198204152014032002

Penguji I,


Dr. Jabbar, MA.
NIP. 19740203200501010

Penguji II,


Bustaman Usman, MA.
NIP. 210057802

Mengetahui,
Dekan Fakultas Syariah dan Hukum
UIN Ar-Raniry Banda Aceh



Muhammad Siddiq, M.H., Ph.D.
NIP. 1963032008011015



**KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
FAKULTAS SYARIAH DAN HUKUM**

Jl. Syekh Abdur Rauf Kopelma Darussalam Banda Aceh
Telp. 0651-7557442 Email : fsh@ar-raniry.ac.id

LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan di bawah ini

Nama : Al-Viratun
NIM : 160104003
Program Studi : Hukum Pidana Islam
Fakultas : Syariah dan Hukum UIN Ar-Raniry

Dengan ini menyatakan bahwa dalam penulisan skripsi ini, saya:

1. ***Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan.***
2. ***Tidak melakukan plagiasi terhadap naskah karya orang lain.***
3. ***Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya***
4. ***Tidak melakukan manipulasi dan pemalsuan data.***
5. ***Mengerjakan sendiri karya ini dan mampu bertanggungjawab atas karya ini.***

Bila kemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap untuk dicabut gelar akademik saya atau diberikan sanksi lain berdasarkan aturan yang berlaku di Fakultas Syariah dan Hukum UIN Ar-Raniry.

Demikian pernyataan ini saya buat dengan sesungguhnya.

Banda Aceh, 25 Juni 2020
Yang Menyatakan,



Al-Viratun

ABSTRAK

Nama : Al- Viratun
NIM : 160104003
Fakultas/Prodi : Syari'ah dan Hukum/Hukum Pidana Islam
Judul : Sanksi Pidana *Cyberfraud* dalam Undang-Undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik Ditinjau Menurut Hukum Pidana Islam
Tanggal Sidang : 14 Juli 2020
Tebal Skripsi : 65 Halaman
Pembimbing I : Dr. Abdul Jalil Salam, S. Ag., MA.
Pembimbing II : Syarifah Rahmatillah, S. H. I., M. H.
Kata kunci : Sanksi Pidana *Cyberfraud*, Undang-Undang ITE, Hukum Pidana Islam

Penelitian ini membahas mengenai bagaimana bentuk *cyberfraud* serta tinjauan hukum pidana Islam terhadap sanksi pidana *cyberfraud* dalam undang-undang nomor 11 tahun 2008 tentang informasi dan Transaksi Elektronik. Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kualitatif dengan menggunakan pendekatan perundang-undangan. Jenis penelitian yang digunakan ialah penelitian kepustakaan (*library research*). Teknik analisis data yang digunakan adalah analisis yuridis normatif dengan cara mengumpulkan data-data yang diperlukan kemudian dilakukan analisis terhadap pandangan-pandangan, pernyataan-pernyataan yang tertuang dalam data-data tersebut yang berkaitan dengan objek penelitian skripsi ini.

Hasil dari penelitian ini dapat disimpulkan bahwa bentuk *cyberfraud* terdiri dari *misuse (compromise) of card data*, *Counterfeiting*, *Wire Tapping* dan *Phishing*. Berdasarkan bentuk-bentuk tersebut dapat diketahui bahwa dalam undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik maupun hukum islam telah diatur hukumannya. Dalam undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik terdapat dalam pasal 35 yang sanksi pidananya diatur dalam pasal 51 ayat 1 dengan ancaman pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). *Cyberfraud* termasuk dalam jenis kejahatan pencurian. Pencurian bila ditinjau dari syariat Islam ada dua macam, diantaranya: pencurian yang hukumnya *ḥad* dan pencurian yang hukumnya *ta'zīr*.

KATA PENGANTAR

الحمد لله، والصلاة والسلام على رسول الله، وعلى الله وأصحابه ومن والاه، لما بعد:

Syukur Alhamdulillah penulis panjatkan kepada Allah SWT yang telah memberikan kekuatan dan petunjuk dalam menyelesaikan skripsi ini yang berjudul **“Sanksi Pidana *Cyberfraud* Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Ditinjau Menurut Hukum Pidana Islam”**. Shalawat beriring salam tak lupa penulis sanjungkan kepangkuan Nabi Muhammad SAW beserta para keluarganya, dan sahabat-sahabatnya, karena perjuangannya kita dapat menikmati indahnya ilmu pengetahuan.

Berbagai pengarahan, bimbingan dan bantuan dari banyak pihak telah penulis dapatkan dalam proses penulisan skripsi ini. Oleh karena itu, penulis menyampaikan ungkapan terima kasih yang sebesar-besarnya kepada Bapak Dr. Abdul Jalil Salam, S. Ag., MA., sebagai pembimbing I dan Ibu Syarifah Rahmatillah, S. H. I., M. H., sebagai pembimbing II. Motivasi dan bimbingan secara ikhlas dan sungguh-sungguh telah diberikan sehingga skripsi ini dapat diselesaikan dengan baik.

Dalam pelaksanaan penulisan dan penelitian skripsi ini penulis mengucapkan terima kasih yang sedalam-dalamnya kepada:

1. Dekan Fakultas Syari'ah dan Hukum Universitas Islam Negeri Ar- Raniry Banda Aceh.
2. Ketua Prodi Hukum Pidana Islam Universitas Islam Negeri Ar- Raniry serta Bapak/Ibu staf pengajar yang telah memberi bekal berbagai ilmu pengetahuan kepada penulis sehingga karya tulis dapat terselesaikan.
3. Teristimewa penulis sampaikan rasa terima kasih kepada kedua orang tua yaitu Ayah (Syamaun) dan Ibu (Ruwaida) atas segala cinta, dorongan dan

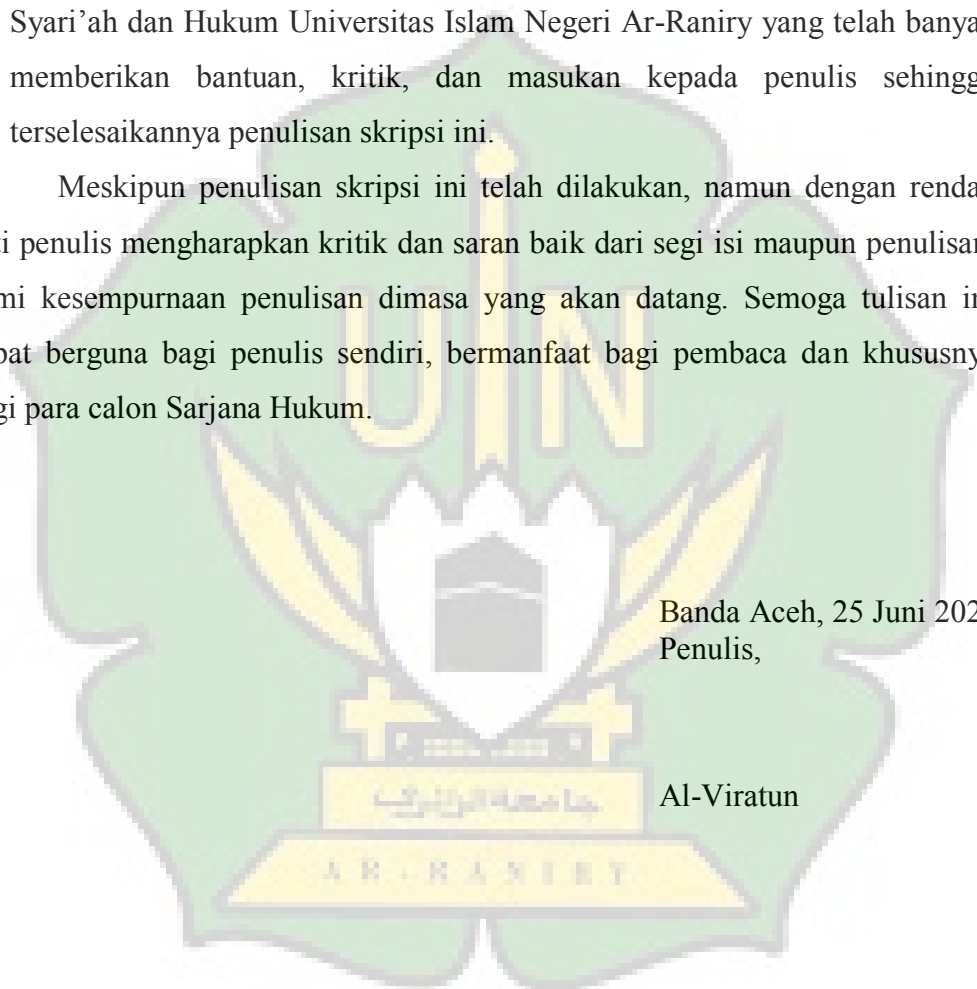
doa yang selalu diberikan, serta keluarga besar penulis yang telah memberikan bantuan baik secara moril maupun material demi kesuksesan penulisan skripsi ini.

4. Kepada sahabat (Lizar Yasni, Rizka Adinda, Rosa Arlinda, dan Jannatun Naim) dan teman-teman angkatan 2016 Hukum Pidana Islam Fakultas Syari'ah dan Hukum Universitas Islam Negeri Ar-Raniry yang telah banyak memberikan bantuan, kritik, dan masukan kepada penulis sehingga terselesaikannya penulisan skripsi ini.

Meskipun penulisan skripsi ini telah dilakukan, namun dengan rendah hati penulis mengharapkan kritik dan saran baik dari segi isi maupun penulisan, demi kesempurnaan penulisan dimasa yang akan datang. Semoga tulisan ini dapat berguna bagi penulis sendiri, bermanfaat bagi pembaca dan khususnya bagi para calon Sarjana Hukum.

Banda Aceh, 25 Juni 2020
Penulis,

Al-Viratun



TRANSLITERASI

Dalam skripsi ini banyak dijumpai istilah yang berasal dari bahasa Arab ditulis dengan huruf latin, oleh karena itu perlu pedoman untuk membacanya dengan benar. Pedoman Transliterasi yang penulis gunakan untuk penulisan kata Arab adalah sebagai berikut:

1. Konsonan

No.	Arab	Latin	Ket	No.	Arab	Latin	Ket
1	ا	Tidak dilambangkan		١٦	ط	t	t dengan titik di bawahnya
2	ب	b		١٧	ظ	z	z dengan titik di bawahnya
3	ت	t		١٨	ع	‘	
4	ث	ś	s dengan titik di atasnya	١٩	غ	gh	
5	ج	j		٢٠	ف	f	
6	ح	h	h dengan titik di bawahnya	٢١	ق	q	
7	خ	kh		٢٢	ك	k	
8	د	d		٢٣	ل	l	
9	ذ	z	z dengan titik di atasnya	٢٤	م	m	
10	ر	r		٢٥	ن	n	
11	ز	z		٢٦	و	w	
12	س	s		٢٧	ه	h	
13	ش	sy		٢٨	ع	‘	
14	ص	ś	s dengan titik di bawahnya	٢٩	ي	y	
15	ض	ḍ	d dengan titik di bawahnya				

2. Konsonan

Vokal Bahasa Arab, seperti vokal bahasa Indonesia, terdiri dari vokal tunggal atau monoftong dan vokal rangkap atau diftong.

a. Vokal Tunggal

Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harkat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin
َ	<i>Fathah</i>	a
ِ	<i>Kasrah</i>	i
ُ	<i>Dammah</i>	u

b. Vokal Rangkap

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harkat dan huruf, transliterasinya gabungan huruf, yaitu:

Tanda dan Huruf	Nama	Gabungan Huruf
َ ي	<i>Fathah</i> dan ya	ai
َ و	<i>Fathah</i> dan wau	au

Contoh:

كيف = *kaifa*,

هول = *hauila*

3. *Maddah*

Maddah atau vokal panjang yang lambangnya berupa harkat dan huruf, transliterasinya berupa huruf dan tanda, yaitu:

Harkat dan Huruf	Nama	Huruf dan tanda
َ ا	<i>Fathah</i> dan <i>alif</i> atau ya	<i>ā</i>
ِ ي	<i>Kasrah</i> dan ya	<i>ī</i>
ُ و	<i>Dammah</i> dan wau	<i>ū</i>

Contoh:

قَالَ = *qāla*

رَمَى = *ramā*

قِيلَ = *qīla*

يَقُولُ = *yaqūlu*

4. Ta Marbutah (ة)

Transliterasi untuk ta marbutah ada dua.

a. Ta marbutah (ة) hidup

Ta marbutah (ة) yang hidup atau mendapat harkat *fathah*, *kasrah* dan *dammah*, transliterasinya adalah t.

b. Ta marbutah (ة) mati

Ta marbutah (ة) yang mati atau mendapat harkat sukun, transliterasinya adalah h.

c. Kalau pada suatu kata yang akhir huruf ta marbutah (ة) diikuti oleh kata yang menggunakan kata sandang al, serta bacaan kedua kata itu terpisah maka ta marbutah (ة) itu ditransliterasikan dengan h.

Contoh:

الْأَطْفَالُ رَوْضَةٌ : *raudah al-atfāl/ raudatul atfāl*

الْمُنَوَّرَةُ الْمَدِينَةُ : *al-Madīnah al-Munawwarah/*

al-Madīnatul Munawwarah

طَلْحَةُ : *Talḥah*

Modifikasi

1. Nama orang berkebangsaan Indonesia ditulis seperti biasa tanpa transliterasi, seperti M. Syuhudi Ismail. Sedangkan nama-nama lainnya ditulis sesuai kaidah penerjemahan. Contoh: Ḥamad Ibn Sulaiman.
2. Nama negara dan kota ditulis menurut ejaan Bahasa Indonesia, seperti Mesir, bukan Misr ; Beirut, bukan Bayrut ; dan sebagainya.
3. Kata-kata yang sudah dipakai (serapan) dalam kamus bahasa arab.



DAFTAR ISI

LEMBARAN JUDUL	i
PENGESAHAN PEMBIMBING	ii
PENGESAHAN SIDANG.....	iii
PERNYATAAN KEASLIAN KARYA TULIS	iv
ABSTRAK.....	v
KATA PENGANTAR	vi
PEDOMAN TRANSLITERASI.....	viii
DAFTAR ISI.....	xii
 BAB SATU PENDAHULUAN	 1
A. Latar Belakang	1
B. Rumusan Masalah	11
C. Tujuan Penelitian.....	12
D. Penjelasan Istilah.....	12
E. Kajian Pustaka	15
F. Metodologi Penelitian	17
1. Pendekatan Penelitian	18
2. Jenis penelitian	18
3. Sumber data	19
4. Teknik pengumpulan data	19
5. Teknik analisis data.....	20
6. Pedoman penulisan.....	20
G. Sistematika Pembahasan	20
 BAB DUA TINDAK PIDANA <i>CYBERFRAUD</i> DALAM UU	
NO. 11 TAHUN 2008	22
A. Sejarah dan Perkembangan <i>Cyberfraud</i>	22
B. Unsur-Unsur Kriminal dalam Tindak Pidana	
<i>Cyberfraud</i>	25
C. Pihak Terkait Pelaku <i>Cyberfraud</i>	29
D. Dampak Negatif Tindak Pidana <i>Cyberfraud</i>	32
E. Ketentuan Sanksi Pidana <i>Cyberfraud</i>	33
 BAB TIGA TINJAUAN HUKUM PIDANA ISLAM TERHADAP	
SANKSI PIDANA <i>CYBERFRAUD</i> DALAM UU NO.	
11 TAHUN 2008	37
A. Pendekatan pada <i>Cyberfraud</i>	37
B. Bentuk-Bentuk <i>Cyberfraud</i>	41
C. Ketentuan Sanksi Pidana <i>Cyberfraud</i>	
di Indonesia	43

D. Analisis Sanksi Pidana <i>Cyberfraud</i> pada UU No. 11 Tahun 2008 Perspektif Hukum Pidana Islam	56
BAB EMPAT PENUTUP.....	59
A. Kesimpulan.....	59
B. Saran	60
DAFTAR PUSTAKA	62
LAMPIRAN	66
DAFTAR RIWAYAT HIDUP.....	67



BAB SATU

PENDAHULUAN

A. Latar Belakang

Pesatnya kemajuan teknologi dan globalisasi saat ini sangat memudahkan setiap orang melakukan akses untuk mendapatkan informasi dengan mudah. Perkembangan teknologi informasi yang semakin pesat telah mengubah hidup manusia menjadi lebih mudah karena kecanggihan dan daya kerjanya yang efektif dan efisien. Keberadaan teknologi informasi bukan hanya digunakan oleh kalangan tertentu saja, namun sekarang hampir seluruh lapisan masyarakat sudah dapat menggunakannya.

Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus juga menjadi sarana efektif perbuatan melawan hukum.¹

Meningkat jumlah pemakai teknologi informasi dari tahun ke tahun terus meningkat oleh sebab itu, semakin banyaknya penyedia internet dan semakin terjangkau biaya akses internet yang membuat semakin banyak orang menggunakan internet. Hal ini menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru yang berkaitan dengan teknologi informasi.

¹Maskun, *Kejahatan Siber (Cyber Crime)*, Kencana, Jakarta, 2013, hlm. 29.

Kegiatan teknologi melalui media elektronik, disebut ruang siber (*cyberspace*) yang meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak didekati dengan ukuran dan kualifikasi hukum konvensional saja, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.²

Penyalahgunaan internet ini melahirkan berbagai bentuk tindak pidana. Seiring dengan kemajuan teknologi, bentuk-bentuk tindak pidana yang terjadi akibat penyalahgunaan internet juga mengalami perkembangan. Banyak jenis tindak pidana yang sebelumnya sulit untuk dilakukan, akibat kemajuan teknologi informasi menjadi hal yang mudah untuk dilakukan oleh siapa saja. Tindak pidana yang terjadi dengan menggunakan media teknologi harus diwaspadai karena dapat menyebabkan kerugian besar bagi korbannya baik individu atau badan hukum seperti bank dan lain-lain.

Perkembangan teknologi juga memunculkan kejahatan yang disebut dengan *cyber crime* atau kejahatan melalui jaringan internet. Munculnya beberapa kasus *cyber crime* di Indonesia merupakan fenomena, seperti pencurian kartu kredit, *hacking* terhadap berbagai situs, penyadapan transmisi data orang lain (misalnya email), dan manipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam *programer* komputer. Berbagai tindakan di atas dapat dikenakan tindak pidana, baik delik formil maupun materil. Delik formil karena menyangkut perbuatan seseorang mengakses data komputer orang lain tanpa izin, sedangkan delik materil adalah perbuatan tersebut telah menimbulkan akibat kerugian bagi orang lain.³

²*Ibid.*

³<https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi/> diakses pada hari senin 20 Mei 2019 Pukul 01:47 WIB

Salah satu kejahatan *cyber crime* dengan menggunakan kartu kredit ialah *carding*. Sebutan untuk pelaku tindak pidana *carding* ialah *Carder*. Menurut riset *Clear Commerce Inc*, perusahaan teknologi informasi yang berbasis di Texas – AS, Indonesia memiliki *carder* terbanyak kedua di dunia setelah Ukraina. Sebanyak 20 persen transaksi melalui internet dari Indonesia adalah hasil *carding*. *Carding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, dengan mencuri data di internet. Sebutan lain untuk kejahatan jenis ini adalah *cyberfraud* atau penipuan di dunia maya. Sifat *cyberfraud* secara umum adalah *non-violence* atau kekacauan yang ditimbulkan tidak terlihat secara langsung, tapi dampak yang ditimbulkan bisa sangat besar. Karena *cyberfraud* merupakan salah satu dari kejahatan *cybercrime* berdasarkan aktivitasnya. Salah satu contohnya dapat menggunakan nomor rekening orang lain untuk berbelanja secara *online* demi memperkaya diri sendiri yang sebelumnya tentu pelaku *cyberfraud* sudah terlebih dahulu mencuri nomor rekening dari korban.⁴

Namun sampai saat ini, belum terdapat aturan yang secara spesifik mengatur tentang tindak pidana *cyberfraud*. Hal ini bukan berarti pelaku tindak pidana *cyberfraud* dapat dengan mudah untuk lolos dari pidana yang telah dia lakukan karena tidak adanya aturan yang mengatur tindak pidana ini. Untuk menjerat pelaku tindak pidana *cyberfraud* dapat menggunakan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, karena tindak pidana *cyberfraud* ini adalah salah satu tindak pidana yang masuk ke dalam ranah *cybercrime*, sehingga untuk menjerat pelaku harus menggunakan penafsiran-penafsiran yang ada di dalam Undang-Undang dan dapat juga menggunakan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi apabila pelaku tindak pidana *cyberfraud* ini menggunakan alat *skimmer* (perangkat atau alat berbentuk tipis yang dipasang pada slot kartu di mesin

⁴<https://kejahatanduniacyber.wordpress.com/pembahasan/cyber-crime/> diakses pada hari Senin 20 Mei 2019 Pukul 00:02 WIB

ATM) untuk melakukan aksinya, karena dengan menggunakan alat *skimmer* tersebut artinya pelaku telah melakukan perekaman data milik korbannya.

Dalam pengaturan tindak pidana *cyberfraud* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, terdapat 2 Pasal yang dapat digunakan untuk menjerat pelaku tindak pidana *cyberfraud* yaitu dalam Pasal 31 dan Pasal 35. Dalam Pasal 31, membahas tentang melakukan intersepsi atau penyadapan, karena dalam tindak pidana ini, beberapa pelaku menggunakan alat *skimmer* untuk melakukan perekaman nomor kartu kredit atau data dari pemilik kartu kredit. Sedangkan dalam Pasal 35 membahas tentang melakukan manipulasi, penciptaan, penghilangan dan pengrusakan data dan atau dokumen elektronik, karena pada dasarnya pelaku tindak pidana *cyberfraud* melakukan penciptaan kartu kredit yang baru dan memanipulasi data seolah-olah kartu tersebut adalah asli merupakan milik pelaku.

Adapun bunyi dari Pasal 31 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah sebagai berikut:

Pasal 31

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

Secara rinci, isi dari Pasal 31 ayat (1) dan (2) menerangkan bahwa Pasal tersebut adalah perbuatan yang melawan hukum. Dalam Pasal 31 ayat (1) dan ayat (2) menerangkan “intersepsi atau penyadapan”. Menurut undang-undang ITE yang dimaksud dengan intersepsi atau penyadapan adalah mendengarkan,

merekam, mengubah, menghambat dan atau mencatat transmisi informasi elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel maupun nirkabel.⁵

Pola umum yang digunakan untuk menyadap sistem komputer adalah menyerang jaringan komputer dengan memperoleh akses terhadap *account user*, kemudian menggunakan sistem milik korban sebagai sarana untuk menyadap dokumen atau data elektronik atau berupa informasi, selanjutnya ditransmisi yang bersifat privasi dan tidak menyebabkan perubahan atau menghilangkan keutuhan data milik korban tersebut.

Pemidanaan apabila seseorang melakukan tindak pidana sebagaimana yang telah diatur dalam Pasal 31 ayat (1) atau ayat (2) terdapat di dalam Pasal 47 UU Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi:

Pasal 47

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Selain pasal 31 perbuatan *cyberfraud* juga bisa dipidana dengan pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

Pasal 35

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

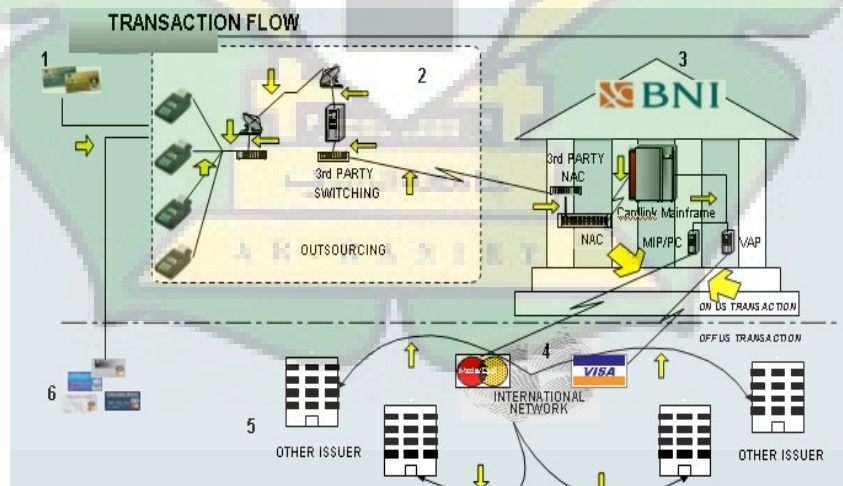
⁵Amandemen Undang-undang Informasi dan Transaksi Elektronik, Penjelasan Pasal 31 ayat (1), hlm. 131.

Pasal 35 menjelaskan tentang melakukan suatu manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik, karena pada umumnya pelaku tindak pidana menggunakan kartu kredit palsu akan melakukan sebuah penciptaan kartu baru dan melakukan manipulasi data agar kartu kredit tersebut seolah-olah milik dari pelaku tindak pidana ini. Pemidanaan apabila seseorang melakukan kejahatan sebagaimana yang telah diatur dalam Pasal 35 terdapat di dalam Pasal 51 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berbunyi :

Pasal 51

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Untuk melihat gambaran transaksi kartu kredit dalam suatu bank maka dapat disampaikan Gambar 1 (Bank X, EDC dan Network , 2009) sebagai berikut:



Gambar 1 Alur Transaksi Kartu Kredit di Suatu Bank

Gambar 1 menjelaskan proses singkat alur transaksi sebagai berikut (sesuai nomor):

1. Nasabah melakukan transaksi di *merchant* (toko). Lalu kartu kredit digosok atau dicolok di mesin EDC (*Elektronic Data Capture*). Data berisi informasi: nomor kartu kredit, *expiry date*, nama nasabah, *CVC* (*Card Verification Code*), *Credit limit*.
2. Data nasabah kemudian mengalir ke jaringan (*network*) LAN (*Local Area Network*) yang dikelola oleh pihak ketiga, dalam hal ini vendor atau perusahaan *switching* (*outsourcing*).
3. Aliran data kemudian masuk ke pusat data (*data center*) Bank X. Dari sini data kemudian diolah di dalam NAC (*Network Access Control*), *Cardlink Mainframe* dan MIP (*Mastercard Interface Processor*) /VAP (*Visa Access Point*).
4. Setelah selesai data nasabah kemudian masuk ke *network* Visa/Master melalui *gateway* international.
5. Dari jaringan Visa/Mastercard ini, data nasabah akan dipilah berdasarkan *issuernya*, apakah kartu tersebut kartu kredit Bank X, Citibank, Mandiri dan sebagainya.
6. Kemudian proses data berulang (*looping*) dan apabila data nasabah valid dan *outstanding* kredit lancar atau mencukupi maka transaksi akan langsung *diapproved* oleh mesin EDC. Nasabah membawa pulang barang belanjanya.

Dari Gambar 1 dapat memunculkan titik kritis terjadinya risiko kejahatan kartu kredit yakni pada poin 2 ketika data nasabah masuk ke LAN perusahaan *switching*. Terjadinya tindak kejahatan dapat dimulai pada poin 2 yang mana pelaku melakukan *illegal interception* (intersepsi ilegal) dengan menyadap data nasabah kartu kredit secara lengkap. Data nasabah yang lengkap itu kemudian dilakukan *reprint* baik menggunakan teknik *skimming* maupun langsung belanja *online* di internet. Dari titik ini sebenarnya proses *carding* itu kemudian

mencuat. Artinya *carder* mendapatkan data kartu kredit yang valid melalui hasil curian.⁶

Kasus *carding* yang dilakukan oleh seorang karyawan *Starbucks* di MT Haryono, Tebet, Jaksel (Tempointeraktif.com, 19 Juli 2010). Penggelapan data nasabah dilakukan sekitar Maret hingga Juni 2010 dan terbongkar setelah lebih dari 41 nasabah melaporkan adanya transaksi ilegal pada kartu kreditnya. Modus operandi yang digunakan pelaku adalah dengan melakukan *reprint* (cetak ulang) struk transaksi dan kemudian mencatat kode verifikasinya (CVC). Dari situ sang *carder* berhasil menguasai ratusan data kartu kredit. Data kartu kredit selanjutnya digunakan untuk membayar transaksi pembelian alat elektronik *Ipod Nano* dan *Ipod Touch* secara online di *Apple Online Store* Singapura hingga lebih dari 50 kali.

Kasus *carding* di Indonesia selanjutnya adalah yang dilakukan oleh Puluhan WNA sindikat *cyberfraud* digerebek polisi di empat lokasi yakni di Jl. Tukad XXI No. 22 Badung, Perumahan Puri Pesona Jl. Darmawangsa Gang SD Kutuh No. IX Badung, Kompleks Pecatu Indah Resort Jl. Sahadewa No. A1/47 Badung, dan di Perumahan Golden Gate Jl. Sunia Negara No. 5 Kepoan, Denpasar Selatan. Total ada 68 WNA, termasuk beberapa di antaranya WNI yang ditangkap dalam kasus tersebut. "*Mereka ditangkap atas dugaan cyberfraud, di mana sasaran atau korbannya adalah WNA di negara asal para pelaku,*" menurut Karo Penmas Divisi Humas Polri Brigjen M Iqbal kepada detikcom, Kamis (11/1/2018). Para sindikat ini ada yang berperan sebagai polisi, jaksa, maupun petugas bank."⁷

Berdasarkan kasus yang pernah terjadi di tahun 2010 dan tahun 2018 menunjukkan masih meningkatnya jumlah kejahatan *carding* atau *cyberfraud*

⁶Leo T. Panjaitan, "Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008: IncomTech". *Jurnal Telekomunikasi dan Komputer*, Vol. 3, No. 1, 2012, hlm. 4-5.

⁷<https://news.detik.com/berita/d-3810769/total-ada-68-wna-yang-ditangkap-terkait-cyber-fraud-di-bali> diakses pada hari Kamis 19 September Pukul 11.00 WIB.

dengan kerugian yang dialami oleh korban baik kerugian secara formil maupun materil semakin besar. Hal ini juga masih kerap terjadi dari tahun ke tahun. Perlindungan hukum baik kepada pihak perbankan dan nasabah harus menjadi perhatian semua pihak khususnya aparat penegak hukum dan legislator baik di Parlemen maupun Pemerintah.

Keberadaan UU ITE No.11 Tahun 2008 merupakan terobosan hukum yang luar biasa namun UU ITE belum secara eksplisit mengakomodasi transaksi perbankan melalui internet dengan menggunakan kartu (kredit dan debit) dan dampak-dampak yang berkaitan dengan kejahatan dunia maya (*cyber crime*). Oleh karena itu dalam kapasitasnya, UU ITE No. 11 Tahun 2008 layak disebut sebagai undang-undang semi *cyber crime*.

Hanya saja ada beberapa yang masih perlu dipertegas di dalam UU ITE yang berlaku saat ini seperti belum adanya undang-undang yang secara khusus membahas tindak pidana *cyberfraud*. Maka dalam menghadapi kasus-kasus yang berkaitan dengan kejahatan elektronik, perlu identifikasi yang kuat dan jelas untuk menghadapi tantangan serius dalam menghadapi *cyber crime*, serta diperlukan keberanian dan inovasi dari aparat penegak hukum untuk mengefektifkan peraturan yang ada, dengan melakukan interpretasi atau konstruksi hukum yang bersumber pada teori/ilmu hukum, pendapat para ahli, yurisprudensi, atau sumber lainnya agar tidak salah kaprah dalam mengimplementasikan hukum tersebut.⁸

Dalam kajian hukum Islam, memelihara harta merupakan tujuan hukum Islam yang kelima. Menurut ajaran Islam, harta adalah pemberian Tuhan kepada manusia, agar manusia dapat mempertahankan hidup dan melangsungkan kehidupannya. Oleh karena itu, hukum Islam melindungi hak manusia untuk memperoleh harta dengan cara-cara yang halal dan sah serta melindungi

⁸Barda Nawawi Arief, *Tindak Pidana Mayantara*, (Jakarta: PT Raja Grafindo Persada, 2006), hlm. 111.

kepentingan harta seseorang, masyarakat dan negara, misalnya dari penipuan (QS. An- Nisa': 29), penggelapan (QS. An- Nisa': 58), perampasan (QS. Al- Mā'idah: 33), pencurian (QS. Al- Mā'idah: 38), dan kejahatan lain terhadap harta orang lain.⁹

يَا أَيُّهَا الَّذِينَ ءَامَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَ
تِجَارَةً عَنْ تَرَاضٍ مِّنْكُمْ وَلَا تَقْتُلُوا أَنْفُسَكُمْ إِنَّ اللَّهَ كَانَ بِكُمْ رَحِيمًا ﴿٢٩﴾

Artinya: Hai orang-orang yang beriman, janganlah kamu saling memakan harta sesamamu dengan jalan yang batil, kecuali dengan jalan perniagaan yang berlaku dengan suka sama-suka di antara kamu dan janganlah kamu membunuh dirimu. Sesungguhnya Allah adalah Maha Penyayang kepadamu (QS. An-Nisa': 29).¹⁰

عن أبي هريرة أن رسول الله صلى الله عليه وسلم مر على صبرة طعام فادخل يده فيها فنالت أصابعه بللا فقال ما هذا يا صاحب الطعام ؟ قال أصابته السماء يا رسول الله أفلا جعلته فوق الطعام كي يراه الناس ؟ من غشا فليس مني (رواه مسلم)

Artinya : “Dari Abu Hurairah ra. berkata :”pada suatu ketika Rasulullah melewati tumpukan makanan {dipasar}”, lalu beliau memasukkan tangannya kedalam tumpukan itu setelah diangkat kembali, ternyata jari-jari beliau basah. lalu beliau bertanya “kenapa begini hai penjual makanan?”, “jawabannya” kena hujan ya Rasulullah “sabda beliau, mengapa tidak ditaruh di atas (yang basah) supaya dilihat orang; siapa yang menipu tidak termasuk golonganku.” (HR. Muslim).¹¹

⁹Mohammad Daud Ali, *Hukum Islam*, (Jakarta: PT RajaGrafindo Persada, 2011), hlm. 64-65.

¹⁰Al- Qur'an

¹¹Al-Nawawiy, Abu Zakaria Yahya ibn Syaraf. *Shahih Muslim bi Syarh al-Nawawiy*, (Beirut: Dar al-Fikr, 1983), Juz I, hlm. 99.

Dari hadits di atas jelas bahwa penipuan diharamkan karena penipuan merupakan suatu kebohongan yang dapat merugikan orang lain sehingga Islam melarang berbohong dan menganggapnya sebagai perbuatan dosa besar selain itu ada hadits yang menerangkan tentang berbuat dusta sebagaimana disebut dalam hadits di bawah ini.

Dalam fiqh dikatakan bahwa tidak dapat diingkari adanya perubahan hukum lantaran berubahnya masa. Maksud dari kaidah ini bahwa setiap perubahan masa, menghendaki kemaslahatan yang sesuai dengan keadaan masa itu. Hal ini mempunyai pengaruh yang besar terhadap pertumbuhan suatu hukum yang didasarkan pada kemaslahatan.¹² Tindak pidana *cyberfraud* di dalam hukum Islam tradisional tidak diatur secara khusus karena pada masa awal pembentukan hukum Islam belum adanya kejahatan tersebut. Tindak pidana *cyberfraud* baru muncul di era modern dengan teknologi yang semakin canggih.

Berdasarkan uraian latar belakang di atas, penulis tertarik untuk melakukan penelitian yang dituangkan dalam bentuk skripsi yang berjudul ***“Sanksi Pidana Cyberfraud dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Ditinjau Menurut Hukum Pidana Islam”***. Alasan penulis ingin melakukan penelitian yang dituangkan dalam bentuk skripsi karena *cyberfraud* termasuk ke dalam *cyber crime* atau kejahatan dunia maya yang masih minim dibicarakan dalam tinjauan hukum pidana Islam.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka dirumuskan dua permasalahan yaitu:

1. Bagaimana bentuk tindak pidana *cyberfraud*?

¹² Asmuni A. Rahman, *Qaidah-Qaidah Fiqih*, (Jakarta: Bulan Bintang, 1976), hlm. 107-108.

2. Bagaimana tinjauan hukum pidana Islam terhadap sanksi pidana *cyberfraud* yang ditentukan dalam Undang-Undang Nomor 11 Tahun 2008?

C. Tujuan Penelitian

Sesuai dengan permasalahan yang telah diuraikan di atas, maka penelitian ini bertujuan untuk:

1. Untuk mengetahui dan menjelaskan bentuk tindak pidana *cyberfraud*
2. Untuk mengetahui dan menjelaskan tinjauan hukum pidana Islam terhadap sanksi pidana *cyberfraud* yang ditentukan dalam UU No. 11 Tahun 2008.

D. Penjelasan Istilah

Untuk memudahkan dalam memahami skripsi ini, perlu kiranya penulis menjelaskan istilah-istilah yang terdapat dalam judul skripsi ini, sebagai berikut:

1. Sanksi Pidana

Sanksi berarti tanggungan (tindak-tindakan hukuman dan sebagainya) untuk memaksa orang menepati perjanjian atau menaati ketentuan undang-undang.¹³ Adapun pidana berarti kejahatan atau kriminal.¹⁴ Jadi dapat disimpulkan bahwa Sanksi pidana adalah suatu tanggungan yang ditimpakan kepada seseorang yang bersalah melakukan perbuatan yang dilarang oleh hukum pidana, dengan adanya sanksi tersebut diharapkan orang tidak akan melakukan tindak pidana.

2. *Cyberfraud*

Cyberfraud merupakan salah satu jenis *cyber crime*. *Cyber crime* adalah bentuk kejahatan dengan menggunakan komputer atau jaringan

¹³ Tri Kurnia Nurhayati, *Kamus Lengkap Bahasa Indonesia*, (Jakarta: Eska Media, 2005), hlm. 657.

¹⁴ *Ibid*, hlm. 537.

komputer/internet sebagai alat, sasaran atau tempat melakukan kejahatan tersebut. Cyber crime atau kejahatan komputer dapat dibedakan menjadi dua yaitu *computer fraud* dan *computer crime*. *Computer fraud* merupakan bentuk kejahatan yang dilakukan pada suatu sistem berbasis komputer. Sedangkan *computer crime* merupakan kegiatan kejahatan yang menggunakan media komputer sebagai tempat melakukan kejahatan. Sehingga dapat disimpulkan bahwa *cyberfraud* adalah kejahatan yang dilakukan dengan sistem berbasis komputer maupun jaringan internet dan bertujuan untuk memanipulasi data atau informasi keuangan untuk mengeruk keuntungan sebesar-besarnya atau kejahatan penipuan di dunia maya yang membuat atau meniru benda atau dokumen yang termasuk konten ilegal lalu membuat salinan dari tiruan tersebut untuk mendapatkan keuntungan.¹⁵

3. Sanksi Pidana *Cyberfraud* dalam UU No. 11 Tahun 2008 Tentang ITE

Di dalam UU No. 11 Tahun 2008 Tentang ITE belum ada peraturan khusus yang menyebutkan tentang tindak pidana *cyberfraud* namun bila dilihat dari unsur-unsurnya kejahatan *cyberfraud* dapat di jerat dengan pasal 31 *jo* pasal 47 dan pasal 35 *jo* pasal 51 ayat 1 UU ITE yang berisi sebagai berikut:

Pasal 31:

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

¹⁵Nadelaalim, "Pengertian Cyber Crime Fraud Beserta Hukumnya" dikutip dari <https://adelakhansa.wordpress.com> diakses 25 Juli 2020.

Pasal 47:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 35:

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 51 ayat 1:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).¹⁶

4. Hukum Pidana Islam

Hukum pidana Islam sepadan dengan fikih *jināyat* dalam fikih Islam. Kata *Jināyat* adalah bentuk jamak dari kata *jināyah*, yang berarti perbuatan dosa, perbuatan salah atau jahat. *Jināyah* adalah *masdar* (kata dasar) dari kata kerja (*fī'il maḍhi*) *janaa* yang mengandung arti suatu kerja yang digunakan bagi laki-laki yang telah melakukan perbuatan dosa atau jahat. Adapun sebutan untuk pelaku wanita ialah *jaanīah*, yang berarti dia (wanita) yang telah berbuat dosa. Kemudian mereka yang terkena dampak akibat perbuatan pelaku disebut *mujnā'alaih* atau korban.¹⁷

Konsep *jināyah* berasal dari kata *jana*, yakni yang berarti kejahatan, pidana, atau kriminal. *Jināyah* adalah perbuatan yang diharamkan atau dilarang karena dapat menimbulkan kerugian atau kerusakan agama, jiwa, akal, dan harta

¹⁶ Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

¹⁷ Ahmad Wardi Muslich, *Hukum Pidana Islam*, (Jakarta: Sinar Grafika, 2005), hlm. 12.

benda. Adapun hukum pidana Islam atau *jināyah* adalah hukum pidana yang ada dalam lingkup hukum Islam, terjemahan dari konsep ‘*uqūbah*, *jarīmah*, dan *jināyah*.¹⁸

Hukum pidana Islam merupakan terjemahan dari kata fiqh *jināyah*. Fiqh *jināyah* adalah segala ketentuan hukum mengenai tindak pidana atau perbuatan kriminal yang dilakukan oleh orang-orang mukallaf (orang yang dapat dibebani kewajiban), sebagai hasil dari pemahaman atas dalil-dalil hukum yang terperinci dari Al-Qur’an dan Hadis. Tindakan kriminal dimaksud, adalah tindakan-tindakan kejahatan yang mengganggu ketentraman umum serta tindakan melawan peraturan perundang-undangan yang bersumber dari Al-Qur’an dan Hadis.¹⁹

E. Kajian Pustaka

Berdasarkan penelusuran yang penulis lakukan di perpustakaan UIN Ar-Raniry Banda Aceh, Penulis belum menemukan tulisan khusus membahas tentang “*Sanksi Pidana Cyberfraud dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Ditinjau Menurut Hukum Pidana Islam.*” Permasalahan *cyberfraud* merupakan modus baru dari tindak pidana *cyber crime*, yakni tentang melakukan manipulasi, penciptaan, penghilangan dan pengrusakan data dan atau dokumen elektronik, karena pada dasarnya pelaku tindak pidana menggunakan kartu kredit palsu ini untuk melakukan penciptaan kartu kredit yang baru dan memanipulasi data seolah-olah kartu tersebut adalah asli merupakan milik pelaku.

Beberapa tulisan yang Penulis jadikan sebagai landasan literatur awal untuk menulis skripsi ini di antaranya buku *Kejahatan Siber (Cyber crime)*, yang ditulis oleh Maskun, memaparkan bentuk kejahatan dari dunia maya

¹⁸ Mustofa Hasan dan Beni Ahmad Saebani, *Hukum Pidana Islam, (Fiqh Jinayah)*, (Bandung: Pustaka Setia, 2013), hlm. 13.

¹⁹ Zainuddin Ali, *Hukum Pidana Islam*, (Jakarta: Sinar Grafika, 2012), hlm. 1.

(cyber) seperti *hacking*, *carding*, *cyberporn*, dan lain-lain, serta memaparkan kesulitan dalam penerapan hukum positif serta ketidakmampuan atau keterbatasan KUHP dalam menjangkau modus operandi jenis kejahatan baru ini yang didasarkan aspek yuridis, alat bukti²⁰ dan buku yang berjudul *Tindak Pidana Informasi dan Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik* yang ditulis oleh Adami Ghazawi dan Ardi Ferdian.²¹

Kemudian buku lainnya berjudul *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, yang ditulis oleh Siswanto Sunarso, dalam tulisannya membahas secara detail tentang memahami undang-undang Informasi dan Transaksi Elektronik (ITE)²² dan jurnal yang berjudul *Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008*.²³

Terdapat juga skripsi yang ditulis oleh saudara Comex Crisna Wijaya, mahasiswa UIN Sunan Kalijaga, yang berjudul “*Kejahatan Carding dalam Perspektif Undang-Undang ITE dan Hukum Islam*”. Dalam tulisan tersebut, Comex Crisna Wijaya mencoba membandingkan kejahatan *carding* yang terdapat dalam undang-undang ITE, dengan kejahatan *carding* dalam hukum Islam yang diqiyaskan dengan *Sariqah*.²⁴ Tetapi dari pembahasan tersebut saudara Comex Crisna Wijaya tidak menjelaskan secara rinci bagaimana penerapan sanksi untuk tindak pidana *carding* yang masuk dalam ruang lingkup

²⁰ Maskun, *Kejahatan Siber (cyber crime)*, (Jakarta: Kencana, 2013), hlm. 15.

²¹ Adami Ghazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, (Malang: Media Nusa Creative, 2015), hlm. 1.

²² Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, (Jakarta: Rineka Cipta, 2009), hlm. 70.

²³ Leo T. Panjaitan, “Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008”, Jurnal: Telekomunikasi dan Komputer, Vol. 3, No. 1, 2012.

²⁴ Comex Crisna Wijaya, “*Kejahatan Carding dalam Perspektif Undang-Undang ITE dan Hukum Islam*”, Skripsi, tidak diterbitkan, Fakultas Syariah UIN Sunan Kalijaga, Yogyakarta, 2010.

cyber crime. Serta penulis tidak menemukan secara detail pandangan hukum Islam terhadap tindak pidana *carding* dalam *cyber crime*.

Sementara itu Yudha Tri Andhika, mahasiswa Universitas Lampung, menulis skripsi tentang “*Upaya Ditreskrimsus POLDA Lampung dalam Menanggulangi Tindak Pidana Pencurian Data dan Informasi Kartu Kredit (Carding)*”²⁵ dan skripsi yang ditulis oleh Ryan Shack Syah, mahasiswa Universitas Syiah Kuala, yang berjudul “*Kebijakan Pidana dalam Penanggulungan Tindak Pidana Carding Menurut Ketentuan Undang-Undang Nomor 11 Tahun 2008 Sebagaimana telah diubah dengan Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.*”²⁶ Dalam kedua tulisan tersebut hanya fokus membahas tentang upaya dan kebijakan penegak hukum terhadap tindak pidana *Carding*.

F. Metodologi Penelitian

Dalam penyusunan suatu karya ilmiah metode yang digunakan sangat menentukan untuk mencapai tujuan secara efektif, karena metode yang dipakai itu senantiasa mempengaruhi mutu dan kualitas karya tulis tersebut. Adapun penelitian kualitatif yang sumber datanya dokumen atau buku, dapat menggunakan metode penelitian kualitatif.²⁷ Dalam skripsi ini metode penelitian yang digunakan adalah metode penelitian kualitatif.

²⁵ Yudha Tri Andhika, “Upaya Ditreskrimsus POLDA Lampung dalam Menanggulangi Tindak Pidana Pencurian Data dan Informasi Kartu Kredit (*Carding*)”, Skripsi, tidak diterbitkan, Fakultas Hukum Universitas Lampung, Bandar Lampung, 2018.

²⁶ Ryan Shack Syah, “Kebijakan Pidana dalam Penanggulungan Tindak Pidana *Carding* Menurut Ketentuan Undang-Undang Nomor 11 Tahun 2008 Sebagaimana telah diubah dengan Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik”, Skripsi, tidak diterbitkan, Fakultas Hukum Universitas Syiah Kuala, Banda Aceh, 2018.

²⁷ Buku “*Pedoman Bimbingan Skripsi*” yang diterbitkan Fakultas Syari’ah dan Hukum Universitas Islam Negeri Ar-Raniry Darussalam Banda Aceh edisi revisi tahun 2019.

Penelitian kualitatif dapat diartikan sebagai penelitian yang tidak mengadakan perhitungan karena kualitas menunjuk segi alamiah yang dipertentangkan dengan kuantum atau jumlah tersebut.²⁸

1. Pendekatan Penelitian

Pendekatan yang digunakan pada penyusunan skripsi ini adalah pendekatan perundang-undangan. Dari perspektif tujuannya, penelitian hukum normatif dapat meneliti tentang sinkronisasi suatu peraturan perundang-undangan. Sinkronisasi peraturan perundang-undangan dapat ditelaah baik secara vertikal maupun secara horizontal.²⁹

Apabila sinkronisasi peraturan perundang-undangan itu ditelaah secara vertikal, berarti akan dilihat bagaimana hierarkisnya. Dalam skripsi ini peneliti melakukan sinkronisasi yang di telaah secara horizontal yang berarti sejauh mana peraturan perundang-undangan yang mengatur pelbagai bidang itu mempunyai hubungan fungsional secara konsisten atau yang dimaksud dalam skripsi ini yaitu antara produk hukum positif dengan ketentuan hukum pidana Islam.

2. Jenis Penelitian

Jenis penelitian yang digunakan pada penyusunan skripsi ini adalah Penelitian pustaka (*libery research*), yaitu penelitian yang menggunakan fasilitas pustaka seperti buku, kitab atau majalah dan yang lainnya yang berkaitan dengan pembahasan skripsi ini, sehingga ditemukan data-data yang akurat dan jelas.³⁰

²⁸ Lexy J. Moleong, *Metodologi Penelitian Kualitatif*, (Bandung: PT Remaja Rosdakarya, 2010), hlm. 3.

²⁹ Amiruddin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum*, (Jakarta: PT RajaGrafindo Persada, 2010), hlm.128-129.

³⁰ Winarno Surakhmad, *Pengantar Penelitian Ilmiah: Dasar, Metode Teknik*, Cet Ke-7, (Bandung: Pustaka Setia, 1994), hlm. 25.

3. Sumber Data

Sumber-sumber data yang akan dijadikan rujukan atau landasan utama dalam penelitian ini yaitu data primer, sekunder dan tersier adalah:

a. Sumber Data Primer

Data primer adalah bahan hukum yang mengikat. Adapun yang menjadi primer untuk dijadikan sebagai sumber rujukan di antaranya adalah undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan-peraturan dibawah undang-undang yang terkait, Al-Qur'an dan Hadist.

b. Sumber Data Sekunder

Data sekunder yaitu bahan yang erat hubungannya dengan data primer dan dapat membantu menganalisa dan memahami bahan primer, untuk dijadikan sumber rujukan di antaranya: buku karangan Maskun yang berjudul *Kejahatan Siber (Cyber Crime)*, dan buku yang berjudul *Tindak Pidana Informasi dan Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik* yang ditulis oleh Adami Ghazawi dan Ardi Ferdian.

Serta jurnal yang berjudul *Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008*. Data sekunder juga dapat dikumpulkan dari internet dan buku-buku lain yang berkaitan dengan permasalahan yang penulis tuangkan dalam bentuk skripsi ini.

c. Sumber Data Tersier

Data Tersier yaitu bahan yang memberikan penjelasan atau petunjuk mengenai bahan primer dan sekunder seperti kamus KBBI dan sumber internet.

4. Teknik Pengumpulan Data

Dalam penelitian yang menggunakan pendekatan *yuridis normatif* yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan-bahan pustaka.

Maka untuk memperoleh data yang mendukung kegiatan pengumpulan data dalam penelitian ini adalah dengan cara mengumpulkan data sekunder.³¹ Dengan jalan membaca, mencatat, mengkaji, serta mempelajari sumber-sumber tertulis.

5. Teknik Analisis Data

Suatu analisis yuridis normatif pada hakikatnya menekankan pada metode deduktif sebagai pegangan utama dan metode induktif sebagai tata kerja penunjang. Hal ini tetap merupakan penelitian ilmiah, karena mencakup kegiatan-kegiatan yang dilakukan secara sistematis dan menggunakan metodologi serta teknik-teknik tertentu.³² Setelah pengumpulan data-data yang diperlukan, selanjutnya dilakukan analisis secara sistematis terhadap pandangan-pandangan, pernyataan-pernyataan yang tertuang dalam data-data tersebut yang berkaitan dengan objek penelitian skripsi ini.

6. Pedoman Penulisan

Adapun untuk penyusunan dan penulisan karya ilmiah ini, penulis berpedoman kepada buku "*Pedoman Bimbingan Skripsi*" yang diterbitkan Fakultas Syari'ah dan Hukum Universitas Islam Negeri Ar-Raniry Darussalam Banda Aceh edisi revisi tahun 2019.

G. Sistematika Pembahasan

Untuk mengetahui gambaran tentang keseluruhan pembahasan dalam skripsi ini, maka pembahasan ini diklasifikasikan menjadi 4 (empat) bab sebagai berikut:

Bab satu, pendahuluan yang berisi latar belakang masalah, rumusan masalah, tujuan penelitian, penjelasan istilah, kajian pustaka, metodologi penelitian, dan sistematika pembahasan.

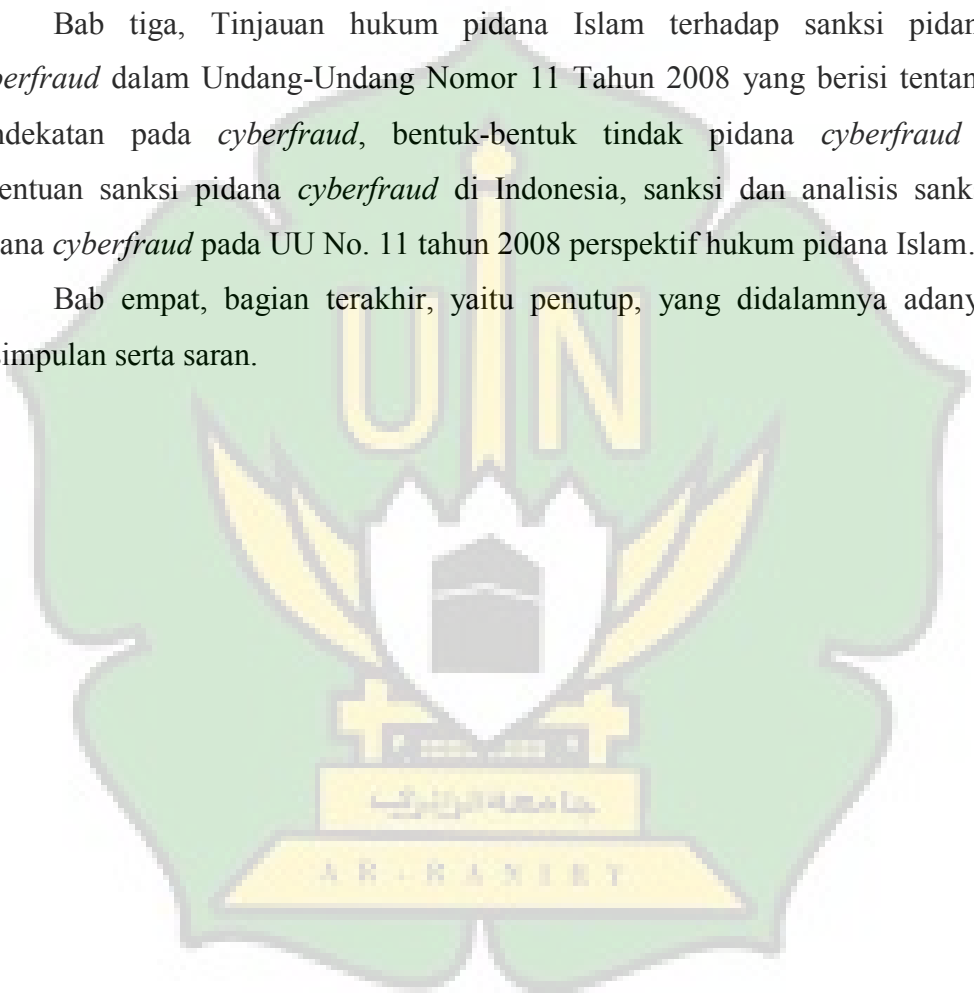
³¹Bambang Sunggono, *Metodologi Penelitian Hukum*, (Jakarta: PT. Grafindo Persada, 1997), hlm. 114.

³² Amiruddin dan Zainal Asikin, *Pengantar Metode Penelitian...*, hlm. 166-167.

Bab dua, tindak pidana *cyberfraud* dalam Undang-undang Nomor 11 Tahun 2008 yang berisi tentang sejarah dan perkembangan *cyberfraud*, unsur-unsur kriminal dalam tindak pidana *cyberfraud*, pihak terkait pelaku *cyberfraud*, dampak negatif tindak pidana *cyberfraud*, dan ketentuan sanksi pidana *cyberfraud*.

Bab tiga, Tinjauan hukum pidana Islam terhadap sanksi pidana *cyberfraud* dalam Undang-Undang Nomor 11 Tahun 2008 yang berisi tentang pendekatan pada *cyberfraud*, bentuk-bentuk tindak pidana *cyberfraud*, ketentuan sanksi pidana *cyberfraud* di Indonesia, sanksi dan analisis sanksi pidana *cyberfraud* pada UU No. 11 tahun 2008 perspektif hukum pidana Islam.

Bab empat, bagian terakhir, yaitu penutup, yang didalamnya adanya kesimpulan serta saran.



BAB DUA

TINDAK PIDANA *CYBERFRAUD* DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008

A. Sejarah dan Perkembangan *Cyberfraud*

Pertama kali terjadi penyalahgunaan komputer (*computer abuse*) itu dimulai dari sistem yang digunakan oleh militer, kemudian menyebar ke wilayah ilmiah, dan akhirnya ke aplikasi-aplikasi dunia bisnis dan pribadi. Perubahan dalam bidang teknologi yang semakin maju dan berkembang sehingga tidak dapat dihindari telah mengakibatkan kejahatan komputer menjadi semakin canggih dan semakin banyak keragamannya. Penyumbang utama dari pertumbuhan kejahatan komputer yang tiba-tiba dan secara besar-besaran berasal dari penggunaan komputer. Semakin meningkatnya kemajuan teknologi, maka semakin bertambah pula jumlah dan kompleksitas kejahatan komputer.³³ Pada akhir tahun 1970-an untuk pertama kalinya diperkenalkan *Teknologi Electronic Data Interchange* (EDI) dan *Electronic Funds Transfer* (EFT). Seterusnya pada tahun 1980-an juga diiringi dengan pertumbuhan dan penggunaan *Credit Cards*, *Automated Teller Machines* (ATM), dan *telephone banking* pada 1980-an.³⁴

Pengguna *Bulletin Board System* (BBS) dan penggunaan kata *cyberfraud* pada tahun 1980 telah digunakan untuk menjelaskan seputar praktik penipuan kartu kredit (*carding*). Metode yang digunakan dapat berupa mencari bukti transaksi di tong sampah, pencurian kotak surat dan bekerja menjadi kasir di toko merupakan cara yang efektif untuk mendapatkan informasi kartu. Kemudian semua informasi kartu tersebut digabungkan di suatu rumah atau apartemen yang tidak berpenghuni. Pada saat itu metode lainnya yang digunakan ialah *social engineering with mail order* yang merupakan penjualan

³³Sutan RemySjahdeini, *Kejahatan & Tindak Pidana Komputer*, Cet Ke- I, (Jakarta: Pustaka Utama Grafiti, 2009), hlm. 46-47.

³⁴Ibid, hlm. 6.

barang melalui pesanan lewat pos (*mail order*) untuk mendapatkan informasi kartu tanpa menunjukkan kartu tersebut. Pada masa itu pengguna internet seperti “*The Video Vindicator*” secara leluasa menulis tata cara pencurian kartu kredit melewati *American Online*, penipuan pesan fax, tata cara *phreaking*³⁵ serta berbagai teknik lainnya untuk mendapatkan keuntungan dari *carding*. Di antara para *hacker* yang tertangkap tersebut disebabkan oleh adanya aktivitas yang berhubungan dengan *carding*. Para *hacker* itu kebanyakan dijatuhi hukuman melalui peraturan keuangan yang berlaku dari pada peraturan mengenai komputer yang baru muncul kala itu.³⁶

Buku tentang *carding*, *100%internet credit card fraud protected* diterbitkan pertama kali pada tahun 1999. Buku ini menjelaskan tentang *spring hack1999* dan *credit card fraud on cybercash*, tingkatan keahlian para *carder*, serta skema dasar dari *phishing* untuk memperoleh data kartu kredit. Dalam buku tersebut juga menyatakan bahwa pada tahun 1999, Amerika Serikat telah mengalami kerugian antara 500 ribu hingga 2 juta dollar akibat *carding*. Beberapa situs jejaring seperti *Counterfeit Library*, *DiplomaMill* dan lain-lain berkembang pesat pada tahun 2000-an yang membentuk jaringan *cybercrime* dimana para anggota jaringan melakukan tindakan kriminal *carding*. Di Rusia tepatnya di Odessa juga terkenal dengan kumpulan *hacker* yang membentuk *Carder Planet*. Forum tersebut merupakan salah satu situs yang berbahaya untuk tindak kejahatan penipuan kartu kredit. Namun, karena tertangkapnya penemu

³⁵Phreaking merujuk kepada aktifitas hacking menggunakan telepon, atau mempergunakan media telepon atau peralatan telepon agar si pelaku bisa masuk ke sistem tersebut. Sifat dari phreaking ini sebenarnya akan sangat berhasil bila dikombinasikan dengan teknik social engineering yang bersifat menipu lewat percakapan ditelepon agar dia bisa diberikan izin akses langsung dari pemilik atau pengelola sistem yang dituju tersebut. <http://rikopn.blogspot.co.id/2016/05/pengertian-phreaking-cyber-crime-again.html> diakses pada tanggal 20 Januari 2020.

³⁶Credit Card for Profit, <http://textfiles.com/anarchy/CARDING/credit> diakses pada tanggal 20 Januari 2020.

Carder Planet yaitu Roman Vega maka situs jaringan tersebut ditutup pada akhir tahun 2004.³⁷

Dalam sebuah artikel berjudul “*Grand Theft Identity*” (S. Levy & Stone, 2005) menyebutkan bahwa 40,5 juta orang di Amerika Serikat diretas kartu kredit mereka; 800.000 mengalami kasus penjualan informasi kepada pelaku trik penipuan; dan ratusan ribu data pribadi milik mereka yang ikut terancam karena pencurian yang dilakukan oleh vendor yang sah seperti bank, sekolah, dan bisnis.³⁸

Di Indonesia kasus *cyberfraud* mulai bermunculan ketika terjadi *booming* internet di era tahun 2000-an. Adapun beberapa kota seperti Jakarta, Bandung dan Yogyakarta menjadi pusat *carder* dalam melaksanakan aksi pencurian data kartu kredit. Pada tahun 2004, aksi-aksi *cybercrime* ini mengakibatkan transaksi online yang berasal dari IP (*Internet Protocol*) Indonesia diblokir oleh dunia Internasional. Dari kasus-kasus yang termasuk ke dalam *cybercrime* khususnya *cyberfraud* tersebut yang benar-benar diproses oleh pengadilan di Indonesia dapat dihitung dengan jari. Karena para *carder* yang dijerat dengan hukum yang setimpal dengan perbuatannya sangat jarang muncul ke media massa.³⁹

Tindak pidana *cyberfraud* sudah beberapa kali terjadi di Indonesia dengan ini perlu adanya aturan dan/atau norma untuk mengatur tindak pidana tersebut. Keterbatasan untuk memenuhi ketersediaan aturan hukum di bidang telematika secara faktual mengharuskan aturan dan/atau norma di bidang ini penting untuk diadakan. Beberapa negara di dunia harus mengakui bahwasaat

³⁷Cyrus Farivar, *Ukrainan fraudster dan Carderplanet “Don” Finally Sentenced to 18 years*, <https://arstechnica.com/tech-policy/2013/12/ukrainian-fraudster-andcarderplanet-don-finallysentenced-to-18-years/> diakses pada hari Kamis tanggal 13 Februari Pukul 11:23 WIB.

³⁸Frank E.Hagan, *Pengantar Kriminologi: Teori, Metode, dan Perilaku Kriminal*, Edisi Ke-7, (Jakarta : Kencana Prenamedia Group, 2013), hlm. 391.

³⁹Leo T. Panjaitan, “Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008: IncomTech”. *Jurnal Telekomunikasi dan Komputer*, Vol. 3, No. 1, 2012, hlm. 13.

ini belum ada yang memiliki secara khusus aturan di bidang telematika. Indonesia sendiri telah memiliki Undang-Undang di bidang teknologi informasi yang dikenal dengan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang diundangkan pada tanggal 21 April 2008.⁴⁰

B. Unsur-Unsur Kriminal dalam Tindak Pidana *Cyberfraud*

Untuk menjatuhkan hukuman terhadap pelaku tindak pidana *cyberfraud* menggunakan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, terdapat 2 Pasal yang dapat digunakan untuk menjerat pelaku tindak pidana *cyberfraud* yaitu dalam Pasal 31 dan Pasal 35. Sementara itu untuk menuntut si pelaku tindak pidana *cyberfraud*, terlebih dahulu seorang hakim atau jaksa harus melihat apa saja unsur-unsur dari tindak pidana tersebut. Apabila si pelaku memenuhi unsur-unsur tersebut, maka baru si pelaku dapat ditahan dan dituntut sesuai dengan kesalahan yang dilakukannya.

Berdasarkan penjelasan dalam Pasal 31 ayat 1 UU Nomor 11 Tahun 2008, yang membahas tentang melakukan intersepsi atau penyadapan. Adapun yang dimaksud dengan intersepsi atau penyadapan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel seperti pancaran elektromagnetis atau radio frekuensi.⁴¹ Dalam tindak pidana *cyberfraud*, ada beberapa pelaku menggunakan alat *skimmer* untuk melakukan perekaman nomor kartu kredit atau data dari pemilik kartu kredit. Sehingga dalam hal ini pelaku tindak pidana *cyberfraud* dapat dijerat dengan Pasal 31 ayat 1 karena perbuatan si pelaku telah memenuhi unsur-unsur tersebut.

⁴⁰Maskun, *Kejahatan Siber...*, hlm. 13.

⁴¹Siswanto Sunarto, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, (Jakarta: Rineka Cipta, 2009), hlm. 70.

Sedangkan dalam Pasal 35 membahas tentang melakukan manipulasi, penciptaan, perubahan, penghilangan dan pengrusakan informasi elektronik dan atau dokumen elektronik yang mempunyai tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.⁴² Pada dasarnya pelaku tindak pidana *cyberfraud* ini melakukan penciptaan kartu kredit yang baru dan memanipulasi data seolah-olah kartu tersebut adalah asli merupakan milik pelaku. Sehingga si pelaku karena perbuatannya dapat dijerat dengan Pasal 35.

Pasal 31 merumuskan dua bentuk tindak pidana ITE, sebagaimana dalam Ayat (1) dan Ayat (2) adalah sebagai berikut:⁴³

1. Tindak Pidana Intersepsi Pasal 31 Ayat (1)

Tindak Pidana intersepsi yang pertama terdiri dari unsur-unsur sebagai berikut:

- a. Kesalahan: *dengan sengaja*;
- b. Melawan hukum: *tanpa hak atau melawan hukum*;
- c. Perbuatan: *intersepsi atau penyadapan*;
- d. Objek: *informasi elektronik dan/atau dokumen elektronik dalam komputer dan/atau sistem elektronik tertentu milik orang lain*.

Tulisan yang dicetak miring merupakan unsur formal yang membentuk tindak pidana Pasal 31 Ayat (1) UU ITE.

2. Tindak Pidana Intersepsi Pasal 31 Ayat (2)

- a. Kesalahan: *dengan sengaja*;
- b. Melawan hukum: *tanpa hak atau melawan hukum*;
- c. Perbuatan: *intersepsi*;

⁴²Ibid, hlm. 71-72.

⁴³Adami Ghazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik :Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, (Malang: Media Nusa Creative, 2015), hlm. 147-151.

- d. Objek: *Atas transmisi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam komputer dan/atau sistem elektronik tertentu milik orang lain;*
- e. *Baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik yang sedang ditransmisikan.*

Tulisan yang dicetak miring merupakan unsur formal yang membentuk tindak pidana Pasal 31 Ayat (2) UU ITE.

Berdasarkan unsur-unsur yang telah disebutkan di atas maka harus diketahui bahwa pengertian setiap orang di sini ialah selain ditafsirkan sebagai individu juga badan hukum yang berbadan hukum sesuai ketentuan perundang-undangan. Pengertian sengaja dan tanpa hak, juga dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang-undang dan berupa tindakan melalaikan yang diancam dengan hukuman. Adapun perbuatan yang dilarang oleh undang-undang (*wederrechtelijk*) seperti yang telah disebutkan di atas, ialah melakukan intersepsi atau penyadapan terhadap informasi elektronik dan/atau dokumen elektronik, transmisi informasi elektronik dan/atau elektronik yang tidak bersifat publik, dalam suatu komputer dan/atau sistem elektronik, milik orang lain, yang tidak atau menyebabkan perubahan, penghilangan, penghentian, informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan. Delik tersebut merupakan delik formil atau delik dengan perumusan formil, yaitu delik yang dianggap telah sepenuhnya terlaksana, dengan dilakukannya suatu perbuatan yang dilarang oleh undang-undang, dan tidak perlu dibuktikan akibat dari perbuatan yang dilarang tersebut.⁴⁴

Adapun tindak pidana *cyberfraud* dalam Pasal 35 tersebut terdiri dari beberapa unsur-unsur sebagai berikut:

⁴⁴Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik...*, hlm. 104-105.

- a. Setiap orang;
- b. Dengan sengaja dan tanpa hak atau melawan hukum;
- c. Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik;
- d. Dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Adapun Pengertian dari kata “setiap orang” yang terdapat dalam Pasal 35, selain ditafsirkan sebagai individu juga badan hukum yang berbadan hukum sesuai ketentuan perundang-undangan. Pengertian dengan sengaja dan tanpa hak, dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang-undang dan tindakan melalaikan yang diancam hukuman. Sementara itu yang dilarang oleh undang-undang (*wederrechtelijk*) adalah melakukan suatu manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik; dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Delik yang dimaksud dalam Pasal 35 merupakan delik formil atau delik dengan perumusan formil, yaitu delik yang dianggap telah sepenuhnya terlaksana, dengan dilakukannya suatu perbuatan yang dilarang oleh undang-undang. Dengan demikian akibat dari perbuatan yang dilarang undang-undang sebagaimana dimaksud di atas, tidak perlu dibuktikan, yang penting bahwa tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.⁴⁵

⁴⁵*Ibid.*, hlm. 111-112.

C. Pihak Terkait Pelaku *Cyberfraud*

Tindakan kejahatan *cyberfraud* tentu tidak terlepas dari pihak-pihak yang terlibat atau ikut serta membantu dalam melancarkan aksinya. Pihak-pihak yang terlibat dalam tindak pidana *cyberfraud* adalah sebagai berikut:

1. *Carder*

Carder (pelaku dari kejahatan kartu kredit) yang dimaksud adalah nasabah dari bank yang sama dengan pemegang kartu kredit tersebut. *Carder* yang telah memperoleh nomor kartu kredit tersebut dapat menciptakan nomor kartu kredit yang lain dengan menggunakan bantuan program-program tertentu.⁴⁶ Teknik umum yang sering digunakan oleh para *carder* dalam aksi pencurian adalah membuat situs atau email palsu atau disebut juga *phishing* dengan tujuan memperoleh informasi nasabah seperti nomor rekening, PIN (*Personal Identification Number*), atau *password*.

Dalam penggunaan istilah “*phishing*” di dunia internet yang berasal dari olahraga “*fishing*” (memancing) yang merupakan analogi dari teknik olahraga memancing dalam melempar umpan pancing dengan umpan email yang menyakinkan agar berhasil dengan baik menangkap korban yang dituju.⁴⁷ Pelaku kemudian melakukan konfigurasi PIN atau *password* setelah memperoleh informasi dari nasabah, sehingga dapat mengambil dana dari nasabah tersebut.

Target *carder* yaitu para pengguna layanan internet *banking* atau situs-situs iklan, jejaring sosial, *online shopping* dan sejenisnya yang mana para pengguna layanan tersebut ceroboh dan tidak teliti dalam melakukan transaksi secara *online* melalui situs internet. Sehingga memberi peluang kepada *Carder* untuk mengirimkan sejumlah email ke target sasaran dengan tujuan untuk meng *up-date* atau mengubah *user ID* dan PIN nasabah melalui internet. Kemudian

⁴⁶Sutan Remy Sjahdeini, *Kejahatan & Tindak Pidana...*, hlm. 83.

⁴⁷*Ibid.*, hlm. 65.

email tersebut terlihat seperti dikirim dari pihak resmi, sehingga nasabah seringkali tidak menyadari kalau sebenarnya sedang ditipu.

2. *Netter*

Netter yaitu para pengguna internet yang melakukan kesalahan akibat lalai dalam menggunakan layanan internet sehingga memberi peluang kepada *carder* untuk menjalankan misinya. Dalam hal ini, *netter* adalah penerima email (nasabah sebuah bank) yang dikirimkan oleh para *carder*. Sehingga dapat disimpulkan bahwa *netter* merupakan korban atau target para *carder*.

3. *Cracker*

Cracker adalah sebutan untuk orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang dimasuki seperti pencurian data, penghapusan, penipuan, dan banyak yang lainnya. Sementara itu *cracker* juga memiliki cara-cara yang sama dengan *hacker* namun yang berbeda adalah motivasinya (*cracker* merusak dan mencuri) dan *cracker* memfokuskan sasarannya terhadap jaringan komputer serta peranti lunak.⁴⁸

4. Bank

Bank ialah badan hukum yang mengumpulkan dana dari masyarakat dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dengan tujuan meningkatkan taraf hidup rakyat seluruhnya. Bank juga merupakan pihak yang menerbitkan kartu kredit/debit, dan sebagai pihak yang menyelenggarakan transaksi *online*, *ecommerce*, *internet banking*, dan lain-lain.⁴⁹

Adapun pertanggung jawaban pihak bank terkait *cyberfraud* adalah sebagai berikut:

⁴⁸Maskun, *Kejahatan Siber...*, hlm. 67.

⁴⁹<https://needr005.wordpress.com/pihak-pihak-yang-terkait-dalam-carding/> Di akses pada tanggal 17 Februari 2020 pada Pukul 01:36 WIB.

1. Tahap pra transaksi

Pada tahap ini pihak bank sebagai penerbit wajib memberikan informasi kepada nasabah mengenai produk kartu kredit yang berisi informasi mengenai syarat-syarat yang harus dipenuhi, jenis kartu kredit yang ditawarkan, hak dan kewajiban sebagai pemegang kartu, resiko yang akan timbul dari penggunaan kartu kredit serta informasi mengenai penyampaian keluhan kerugian yang diharapkan dapat mengurangi kerugian yang timbul akibat dari penggunaan kartu kredit bank penerbit yang bersangkutan sebagai bentuk pertanggung jawaban bank penerbit dalam melindungi nasabahnya dari kerugian yang tidak diinginkan.

2. Transaksi konsumen

Dalam tahap transaksi ini, konsumen dan pelaku usaha telah melakukan suatu perikatan atau perjanjian dalam penerbitan dan penggunaan kartu kredit. Pada tahap ini terdapat pertanggung jawaban dari pelaku usaha yang berupa bentuk tanggung jawab kontraktual karena dalam hal ini pihak bank penerbit sebelumnya sudah melakukan perikatan dengan konsumen sehingga pihak bank harus memenuhi kontraktual yang mana bank selaku pelaku usaha.

3. Tahap sesudah transaksi

Tahap ini merupakan tahap penyelesaian masalah antara pihak bank dengan nasabah apabila terjadi pengaduan, sengketa atau masalah. Penyelesaian pengaduan nasabah merupakan salah satu bentuk peningkatan terhadap perlindungan nasabah dalam rangka menjamin hak-hak nasabah dalam berhubungan dengan bank. Ada dua cara yang dapat digunakan dalam menyelesaikan masalah tersebut. Cara pertama adalah cara damai yaitu bank akan menyelesaikan sendiri masalahnya dengan nasabah yang mengalami kerugian baik dengan cara ganti rugi maupun memberikan kompensasi. Cara kedua adalah menggunakan jalur apabila nasabah merasa dengan jalan damai masalahnya belum dapat diselesaikan maka nasabah dapat mengajukan gugatan perdata maupun pidana ke Pengadilan Negeri yang ditujukan kepada pelaku

usaha. Adapun cara lain yang dapat digunakan nasabah melalui jalur luar pengadilan yaitu melalui Badan Penyelesaian Sengketa Konsumen (BPSK).⁵⁰

D. Dampak Negatif Tindak Pidana *Cyberfraud*

Kejahatan *cyberfraud* biasanya ditujukan terhadap data atau dokumen pribadi seseorang yang tersimpan pada formulir data pribadi melalui sistem komputer, yang apabila diketahui oleh orang lain, maka dapat menimbulkan kerugian terhadap orang tersebut secara materil maupun imateril.⁵¹ Tindak pidana *cyberfraud* merupakan suatu perbuatan yang melanggar hukum yang bisa menimbulkan berbagai dampak negatif. Banyak dampak negatif yang bisa ditimbulkan dengan melakukan kegiatan *cyberfraud*. Beberapa dampak negatif *cyberfraud* adalah sebagai berikut:⁵²

1. Kehilangan uang atau pencurian secara ilegal

Bagi pemilik kartu kredit, akan memperoleh dampak negatif secara nyata. Pemilik kartu kredit akan mendapatkan pencurian atau penggunaan kartu kredit secara ilegal yang digunakan untuk melakukan segala jenis transaksi yang dilakukan oleh *carder*. Dengan adanya hal tersebut, pemilik kartu kredit akan mengalami kerugian yang sangat dominan.

2. Adanya kasus penipuan

Banyak kasus penipuan yang dapat terjadi dengan adanya sistem *cyberfraud*. Dengan adanya *cyberfraud* tingkat penipuan yang dilakukan dalam dunia maya akan mengalami peningkatan. Oleh karena itu, *cyberfraud* merupakan kegiatan yang sangat dilarang oleh banyak negara.

3. Hilangnya kepercayaan pada negara

⁵⁰ Annisa Aprilia, Paramita Prananingtyas dan Budiharto, *Tanggung Jawab Bank Penerbit Terhadap Kerugian Nasabah Kartu Kredit Akibat Pencurian Data Dalam Kegiatan Transaksi*, <http://www.ejournal-s1.undip.ac.id/index.php/dlr/> Di akses pada tanggal 14 Agustus 2020 pada Pukul 22:30 WIB.

⁵¹ Maskun, *Kejahatan Siber...*, hlm. 54

⁵² <https://www.nesabamedia.com/pengertian-carding/> Di akses pada tanggal 4 Maret 2020 pada Pukul 14:18 WIB.

Banyaknya *carder* dari suatu negara akan membuat negara tersebut kehilangan kepercayaan dari negara-negara yang dijadikan tujuan *cyberfraud*. Dengan adanya hal tersebut akan mempengaruhi adanya konflik sosial antar negara dan bisa berakhir pada tidak adanya perdamaian dunia.

4. Adanya keresahan atas kurang amannya bertransaksi menggunakan kartu kredit

Dengan banyaknya kasus *cyberfraud* yang menggunakan berbagai jenis kartu kredit, akan meningkatkan keresahan pada pengguna kartu kredit. Dengan adanya *cyberfraud*, keresahan pemilik kartu kredit akan mengalami peningkatan karena dirasa menggunakan kartu kredit akan menimbulkan banyak kasus penipuan. Selain itu, pemilik kartu kredit akan merasa bahwa tidak harus menggunakan kartu kredit guna untuk mengurangi adanya tindak kejahatan seperti *cyberfraud*.

5. Merugikan orang lain yang tidak melakukan *cyberfraud*

Cyberfraud merupakan kegiatan yang tidak hanya merugikan orang yang menjadi target *cyberfraud* (pemilik kartu kredit yang digunakan sebagai target *cyberfraud*). Namun, orang lain yang tidak melakukan *cyberfraud* akan terkena dampaknya. Banyak orang yang mungkin trauma akan adanya *cyberfraud* dan akan menyebabkan adanya pengurangan transaksi online. Sehingga bisa menurunkan adanya kerjasama antar negara.

E. Ketentuan Sanksi Pidana *Cyberfraud*

- a) Dari segi unsur-unsurnya

Tindak pidana *cyberfraud* dalam Undang-undang No. 11 tentang Informasi dan Transaksi Elektronik dapat digolongkan sebagai intersepsi atau penyadapan sebagaimana yang telah diatur dalam pasal 31 ayat (1) dan (2) serta pasal 35 tentang melakukan suatu manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik. Karena dalam modus operandi *cyberfraud* terdapat unsur-unsur intersepsi atau

penyadapan dan penciptaan kartu baru serta memanipulasi data. Adapun unsur-unsur dari pada *cyberfraud* yang terdapat dalam pasal 31 dan 35 adalah sebagai berikut:

1) Kesalahan yaitu dengan sengaja dan tanpa hak

Perbuatan *cyberfraud* merupakan suatu perbuatan yang bertentangan dengan undang-undang dan tindakan melalaikan yang diancam hukuman. Maksudnya apabila seseorang yang berniat hendak mencuri atau mengambil sesuatu barang kepunyaan orang lain harus disertai dengan niat sengaja untuk mengambil barang tersebut, bukan karena kekeliruan. Dalam hal ini *carder* sengaja melakukan tindak pidana *cyberfraud* yang pada awalnya untuk bermain-main, akan tetapi pada akhirnya menjadi gaya hidup dengan tujuan mendapatkan uang untuk memenuhi kebutuhan hidup mereka.

2) Perbuatan yaitu intersepsi atau penyadapan

Dalam transaksi *cyberfraud*, nomor-nomor kartu kredit didapatkan dari hasil hack, dengan melakukan penyadapan pada setiap transaksi *on-line* melalui jaringan telekomunikasi, memasuki suatu *website* yang belum diamankan atau sistem pengamanannya yang belum bagus, dan lain-lain. Dengan mendapatkan nomor-nomor kartu kredit dan *exp.datanya*, *carder* dapat melakukan transaksi *on-line* baik itu transaksi pembelian ataupun transfer tunai. Para *carder* juga melakukan transaksi pembelian melalui internet kemudian memasukkan jenis pembayaran.

3) Objek yaitu informasi elektronik dan/atau dokumen elektronik dalam komputer dan/atau sistem elektronik tertentu milik orang lain

Tujuan *carder* ialah melakukan intersepsi atau penyadapan untuk memperoleh nomor kartu kredit milik korban yang kemudian nomor tersebut digunakan untuk kepentingan pribadinya atau si pelaku dapat memperoleh keuntungan dari perbuatannya tersebut yang mengakibatkan kerugian terhadap korban yaitu pemilik dari nomor kartu kredit itu.

4) Secara melawan hukum

Apabila perbuatan tersebut memenuhi semua unsur yang terdapat di dalam rumusan suatu delik. Delik ialah delik formil atau delik dengan perumusan formil, yaitu delik yang dianggap telah sepenuhnya terlaksana, dengan dilakukannya suatu perbuatan yang dilarang oleh undang-undang dan tidak perlu dibuktikan akibat dari perbuatan yang dilarang tersebut. Sedangkan "melawan hukum" dalam arti materil adalah suatu perbuatan yang dapat dipandang sebagai bersifat melawan hukum apabila perbuatan melanggar hukum bukan hanya ditinjau sesuai dengan ketentuan-ketentuan hukum yang tertulis saja melainkan juga harus ditinjau menurut asas-asas hukum umum dari hukum yang tidak tertulis.

Dalam hal ini tindakan *cyberfraud* sudah jelas merupakan perbuatan yang melanggar hukum, karena tindakannya telah merugikan orang lain, yakni korban yang merupakan pemilik kartu kredit. Kemudian cara mendapatkan kartu kredit tersebut juga melawan hukum, karena mencuri data orang lain tanpa izin ataupun sepengetahuan pemiliknya. Hal ini bisa dijerat dengan pasal 31 ayat (2) dan pasal 35 UU ITE Tahun 2008.

b) Dari segi sanksi hukumannya

Cyberfraud dapat dapat digolongkan kedalam intersepsi atau penyadapan serta pemalsuan atau memanipulasi kartu kredit karena terdapat unsur-unsur intersepsi di dalamnya sebagaimana penjelasan diatas. Intersepsi atau penyadapan diatur dalam pasal 31 ayat (1) dan ayat (2) serta pemalsuan dan manipulasi juga terdapat dalam pasal 35.

Ketentuan sanksi pidana terhadap pelaku *cyberfraud* terdapat pada Pasal 31 yang ancaman pidananya dirumuskan dalam Pasal 47 tentang tindak pidana intersepsi atau penyadapan informasi elektronik secara melawan hukum. Sanksi pidana terhadap pelaku *cyberfraud* juga terdapat dalam pasal 35 yang ancaman

pidananya dirumuskan pada Pasal 51 tentang melakukan suatu manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik.

Rumusan tindak pidana Pasal 31 yang dimaksud dirumuskan dalam satu naskah dengan Pasal 47 selengkapnya sebagai berikut:⁵³

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).
- (2) Dipidana yang sama seperti ayat pertama, setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.
- (3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
- (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Ketika tindak pidana Pasal 35 juncto Pasal 51 Ayat (1) dirumuskan dalam satu naskah, maka rumusan selengkapnya adalah sebagai berikut.

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang autentik, dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).⁵⁴

⁵³Adami Ghazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik...*, hlm. 147.

⁵⁴*Ibid.*, hlm. 150.

BAB TIGA

TINJAUAN HUKUM PIDANA ISLAM TERHADAP SANKSI PIDANA *CYBERFRAUD* DALAM UU NO. 11 TAHUN 2008

A. Pendekatan pada *Cyberfraud*

Berbagai masalah *cyberfraud* biasanya menggunakan sarana internet. Dalam pembelanjaan yang ditawarkan melalui sistem dalam internet, untuk pembelanjaan dan pembayaran dapat menggunakan kartu kredit dengan menyebutkan atau menuliskan, menginput nomor kartu kredit pada kolom pembayaran yang telah tersedia dan pihak penjual akan melakukan pengecekan atau otorisasi kepada penyelenggara kartu kredit atau bank. Setelah otorisasi serta nomor dan pemiliknya dinyatakan maka barang akan dikirim ke alamat pembeli.⁵⁵ Namun dengan segala kecanggihan yang diberikan juga terdapat kelemahan dalam sistem keamanannya, oleh karena itu perlu adanya pendekatan untuk mempertahankan keamanan tersebut. Melalui Kementerian Komunikasi dan Informatika RI, terdapat tiga pendekatan untuk mempertahankan keamanan agar terhindar dari *cyberfraud*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika, dan ketiga pendekatan hukum. Untuk mengatasi gangguan keamanan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, dintersepsi, atau diakses secara ilegal dan tanpa hak.

Pertama, pendekatan tata kelola dan teknologi keamanan informasi, yang dalam hal ini pendekatan dilakukan melalui sistem manajemen keamanan informasi serta melalui pendekatan teknologi yang cermat dan akurat serta *up to date* agar dapat menutup setiap lubang atau celah yang dapat digunakan untuk melakukan penyerangan-penyerangan dalam dunia siber. Kemudian yang kedua, pendekatan sosial budaya, dalam arti memberikan pemahaman dari sudut sosial

⁵⁵Irman, *Anatomi Kejahatan Perbankan (banking crime anatomy)*, (Bandung: MQS Publishing dan AYYCCS GROUP, 2006), Hlm. 161.

budaya agar masyarakat memahami secara benar tentang kepedulian akan keamanan informasi khususnya fenomena dalam dunia siber yang bersifat global dan lintas batas (*borderless*). Ketiga, pendekatan hukum yaitu tersedianya instrumen hukum positif nasional yang terkait dengan pemanfaatan teknologi informasi seperti UU No. 11 Tahun 2008 tentang ITE dan PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) yang salah satunya adalah kebijakan dan regulasi di bidang keamanan informasi.⁵⁶

Dalam tindak pidana *cyberfraud* pelanggaran seringkali menjadi sulit dijerat karena hukum dan pengadilan Indonesia tidak memiliki yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi, mengingat pelanggaran hukum bersifat transnasional tetapi akibatnya justru memiliki implikasi hukum di Indonesia. Masaki Hamano mengemukakan pada awalnya ada yurisdiksi yang didasarkan pada prinsip-prinsip tradisional.

Menurutnya ada tiga kategori yurisdiksi tradisional, yaitu yurisdiksi legislatif (*legislative jurisdiction* atau *jurisdiction to prescribe*), yurisdiksi yudisial (*judicial jurisdiction* atau *jurisdiction to adjudicate*), dan yurisdiksi eksekutif (*executive jurisdiction* atau *jurisdiction to enforce*). Mengacu pada pengertian ketiga yurisdiksi di atas, maka dapat dikatakan bahwa yurisdiksi tradisional berkaitan dengan batas-batas kewenangan negara di tiga bidang penegakan hukum. Pertama, kewenangan pembuatan hukum substantif (oleh karena itu, disebut yurisdiksi legislatif, atau dapat juga disebut yurisdiksi formulatif). Kedua, kewenangan mengadili atau menerapkan hukum (oleh karena itu, disebut yurisdiksi yudisial atau aplikasi). Ketiga, kewenangan melaksanakan/memaksakan kepatuhan hukum yang dibuatnya (oleh karena itu, disebut yurisdiksi eksekutif).⁵⁷

⁵⁶https://www.kominfo.go.id/content/detail/7479/tiga-jurus-tangani-penyalahgunaan-tik/0/berita_satker Di Akses pada 7 Maret Pukul 06:55.

⁵⁷Barda Nawawi Arief, *Tindak Pidana Mayantara...*, hlm.27-28.

Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu : pertama, *subjective territoriality*, yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain. Kedua, *objectiveterritoriality*, yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan. Ketiga, *nationality* yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku. Keempat, *passive nationality* yang menekankan yurisdiksi berdasarkan kewarganegaraan korban. Kelima, *protective principle* yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah, dan keenam, asas *Universality*. Asas *Universality* selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus *cyber*. Asas ini disebut juga sebagai “*universalinterest jurisdiction*”. Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (*crimes againsthumanity*), misalnya penyiksaan, genosida, pembajakan udara dan lain-lain. Meskipun di masa mendatang asas yurisdiksi universal ini mungkin dikembangkan untuk *internet piracy*, seperti *computer*, *cracking*, *carding*, *hacking and viruses*, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.⁵⁸

⁵⁸https://prastowo.staff.ugm.ac.id/files/130M-09-final2.0laws_investigations_and_ethics.pdf Di Akses pada 6 Maret 2020 Pukul 15:16.

Oleh karena itu, untuk menghindari terjadinya *cyberfraud* dibutuhkan suatu hukum baru yang menggunakan pendekatan yang berbeda dengan hukum yang dibuat berdasarkan batas-batas wilayah. *Cyberfraud* dapat diibaratkan sebagai suatu tempat yang hanya dibatasi oleh *screens and passwords*. Secara radikal, *cyberfraud* telah mengubah hubungan antara *legally significant (online) phenomena and physical location*. Berdasarkan karakteristik khusus yang terdapat dalam *cyberfraud* dimana pengaturan dan penegakan hukumnya tidak dapat menggunakan cara-cara tradisional, beberapa ahli berpandangan bahwa sebaiknya kegiatan-kegiatan dalam *cyberfraud* diatur oleh hukum tersendiri, dengan mengambil contoh tentang tumbuhnya *the law of merchant (lex mercatoria)* pada abad pertengahan. Asas kebiasaan dan norma yang mengatur *cyberfraud* ini yang tumbuh dalam praktek dan diakui secara umum disebut sebagai *Lex Informatica*.⁵⁹

Menurut Khyati Chaundhary dan Bhawna Mallick, Transaksi berbasis kartu kredit dapat diklasifikasikan menjadi dua jenis. Pertama, transaksi menggunakan kartu kredit dalam bentuk fisik, dan kedua transaksi kartu jarak jauh. Pada transaksi menggunakan kartu kredit dalam bentuk fisik, pemegang kartu memberikan kartunya secara fisik ke pedagang (*merchant*) untuk melakukan pembayaran. *Credit card fraud* dengan menggunakan metode ini, pelaku harus memiliki kartu kredit dalam bentuk fisik. Kedua, transaksi kartu jarak jauh (biasa disebut transaksi online), pada transaksi jenis ini, hanya membutuhkan beberapa informasi penting tentang kartu, seperti nama pemegang kartu kredit, nomor kartu kredit, tanggal kadaluarsa, kode pengaman, nomor verifikasi kartu kredit (CVV/*Card Verification Value*) untuk melakukan pembayaran.

⁵⁹https://prastowo.staff.ugm.ac.id/files/130M-09-final2.0laws_investigations_and_ethics.pdf Di Akses pada 6 Maret 2020 Pukul 15:16.

Untuk melakukan penipuan dalam jenis transaksi ini, pelaku perlu mengetahui rincian informasi penting tentang kartu. Rincian data itulah yang diberikan kepada pedagang (*merchant*) sebagai alat pembayaran. Dengan informasi itulah pedagang akan membebankan beban pembayaran kepada *account* (rekening) kartu kredit milik pemegang yang sah.⁶⁰

Adapun modus kejahatan *cyberfraud* ialah dengan melaksanakan pembelanjaan melalui internet tetapi dengan menggunakan nomor kartu kredit orang lain, sehingga yang dirugikan adalah pemilik kartu kredit yang asli. Pada saat ini banyak dari pelaku modus kejahatan *cyberfraud* dilakukan oleh pelaku antar negara, misalnya, pemilik kartu kredit asli adalah warga negara Eropa dan penjual barang berada di Jepang. Kemudian barang dikirim ke alamat di Jakarta (Indonesia), tetapi pembeli yang juga pelaku *cyberfraud* berada di kota lain, di luar Jakarta. Secara fisik kartu kreditnya tidak dipakai atau tidak digesek pada terminal POS (*Point of Sale*/ mesin gesek kartu kredit), tetapi hanya nomornya saja yang dipakai untuk pembelanjaan.⁶¹

B. Bentuk-Bentuk *Cyberfraud*

Dilansir dari situs hukum online yang mewawancarai Ketua Asosiasi Kartu Kredit Indonesia (AKKI) Baskoro Widyopranoto saat usai seminar sosialisasi RUU Informasi dan Transaksi Elektronik (ITE) di Fakultas Hukum UI. Menurut Baskoro, kejahatan *cyberfraud* banyak jenisnya yaitu *misuse* (*compromise*) of card data, *Counterfeiting*, *Wire Tapping* dan *Phishing*.⁶²

⁶⁰Said Noor Prasetyo, *Rumusan Pengaturan Credit Card Fraud dalam Hukum Pidana Indonesia Ditinjau dari Asas Legalitas*, Legality, Vol.24, No.1, Maret 2016-Agustus 2016, hlm.110. <http://ejournal.umm.ac.id/index.php/legality/article/download/4260/4627> Di Akses pada 6 Maret 2020 Pukul 13:00.

⁶¹Irman, *Anatomi Kejahatan Perbankan ...*, Hlm. 161-162.

⁶²<https://www.hukumonline.com/berita/baca/hol15453/bisakah-ruu-ite-mengantisipasi-kejahatan-icardingi/> Di Akses pada 7 Maret 2020 Pukul 13:45.

Adapun bentuk-bentuk dari *cyberfraud* adalah sebagai berikut:⁶³

- a. *Misuse (compromise) of card data*, yaitu berupa penyalahgunaan kartu kredit yang tidak dipresentasikan.
- b. *Counterfeiting*, yaitu pemalsuan kartu kredit. Kartu palsu tersebut sudah diubah sehingga menyerupai kartu asli. *Cyberfraud* jenis ini dilakukan oleh perorangan atau sindikat pemalsu kartu kredit yang memiliki jaringan luas, mempunyai dana yang besar dan didukung oleh keahlian tertentu. Perkembangan *counterfeiting* saat ini telah menggunakan software tertentu yang tersedia secara umum di situs-situs tertentu (*creditmaster, credit probe*) untuk menghasilkan nomor-nomor kartu kredit serta dengan menggunakan mesin atau terminal yang dicuri dan telepon genggam untuk mengecek keabsahan nomor-nomor tersebut. Selain itu, *counterfeiting* juga menggunakan *skimming device* yang berukuran kecil untuk menyamai data yang tertera di *magnetic stripe* (sebagai media penyimpanan data) kartu kredit asli dan menggunakan peralatan-peralatan untuk *meng-intercept* jaringan telekomunikasi serta menggunakan terminal *implants*.
- c. *Wire Tapping*, yaitu penyadapan transaksi kartu kredit melalui jaringan komunikasi. Dengan sistem ini jumlah data yang didapat sangat banyak, jumlah kerugian yang tinggi dan sampai saat ini belum ada buktinya di Indonesia.
- d. *Pishing* adalah pengiriman email palsu kepada seseorang atau suatu perusahaan atau suatu organisasi dengan menyatakan bahwa pengirim adalah suatu entitas bisnis yang sah. Pengiriman email palsu tersebut dimaksudkan untuk menipu penerima agar memberitahu informasi mengenai penerima. *Phishing* juga merupakan salah satu bentuk dari kejahatan Internet yang

⁶³Sylviani, Studi Komparasi Hukum Pidana Islam dan Pasal 362 Tentang Tindak Pidana Carding, Skripsi Sarjana Hukum, (Surabaya: Universitas Islam Negeri Sunan Ampel, 2010). Di Akses melalui <http://digilib.uinsby.ac.id/8765/6/bab3.pdf> pada 7 Maret 2020 Pukul 12:53.

disebut *Identity theft* (penyalahgunaan identitas orang lain).⁶⁴ *Phising* juga bisa didefinisikan sebagai bentuk penyadapan melalui situs *website* agar personal data nasabah dapat dicuri.

C. Ketentuan Sanksi Pidana *Cyberfraud* di Indonesia

Tindak pidana *cyberfraud* merupakan jenis perbuatan pencurian dan dalam hukum Islam diqiyaskan dengan *jarīmah* penipuan. Karena *cyberfraud* berdasarkan bentuk-bentuknya yang telah disebutkan dan diuraikan di atas, maka *cyberfraud* digolongkan dalam pencurian dengan berbagai trik penipuan seperti menggunakan nomor kartu atm seseorang dalam berbelanja online.

Hukuman dalam istilah Arab sering disebut '*uqūbah*, yaitu bentuk balasan bagi seseorang yang atas perbuatannya melanggar ketentuan syara' yang ditetapkan Allah dan Rasul-Nya untuk kemaslahatan manusia.⁶⁵ Dengan balasan yang diterima oleh pelaku kejahatan maka kemaslahatan antar sesama manusia akan tetap berlangsung dengan baik dan tidak hanya itu dengan hukuman yang mereka dapatkan maka akan timbul rasa penyesalan dalam jiwa mereka.

Hukuman atau sanksi pidana yang dijatuhkan pada perbuatan yang diancam pidana harus tercantum dalam nash Al-quran atau As-sunnah, atau dalam kitab Undang-undang pidana. Suatu asas disebut dengan *mullum Crime Ine Lange (Ia huma qabla wūrudinnas)*. Dalam hukum di Indonesia tercantum dalam pasal 1 ayat (1) KUHP. Letak perbedaan antara istilah hukuman atau pidana harus berdasarkan nash yang legal dan formal atau ketentuan Undang-undang.⁶⁶ Dengan penjelasan ini jelaslah bahwa dalam menjatuhkan hukuman pada seorang pidana harus berdasarkan ketentuan-ketentuan yang telah

⁶⁴Sutan Remy Syahdeini, *Kejahatan dan Tindak Pidana...*, hlm. 63-64.

⁶⁵ Teguh Prasetyo, *Hukum Pidana*, (Depok: Raja Grafindo Persada, 2017), hlm. 111.

⁶⁶ Mustofa Hasan, *Hukum Pidana Islam Fiqh Jinayah*, ..., hlm. 85.

ditetapkan baik dalam Al-quran, Hadits atau berdasarkan Undang-undang yang formal, kita tidak dapat memberikan hukuman dengan kehendak sendiri.

Hukum Pidana Islam, sebagai realisasi dari hukum Islam itu sendiri, menerapkan hukuman dengan tujuan untuk menciptakan hidup rukun antar individu, individu antar masyarakat serta mencegah perbuatan-perbuatan yang dapat menimbulkan kerugian terhadap anggota masyarakat baik yang berkenaan dengan fisik, jiwa, harta maupun kehormatan. Tujuan memberi hukuman dalam Islam sesuai dengan konsep tujuan umum disyariatkan hukum, yaitu untuk merealisasi kemaslahatan umat sekaligus untuk menegakkan keadilan antar sesama manusia.

Perbuatan *cyberfraud* termasuk dalam kejahatan pencurian, pencurian dalam Islam sudah Allah tetapkan sebagai perbuatan yang tidak boleh dilakukan, perbuatan ini adalah perbuatan yang haram dilakukan, tentang kasus pencurian Allah telah menjelaskan dalam Al-quran Surah Al-baqarah ayat 188:

وَلَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوا بِهَا إِلَى الْحُكَّامِ
لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنْتُمْ تَعْلَمُونَ

Artinya: “Dan janganlah kamu memakan harta orang lain diantaranya dengan jalan yang bathil dan janganlah kamu membawa (urusan) hartamu itu kepada hakim supaya kamu dapat memakan sebagian dari harta benda orang lain dengan jalan berbuat dosa, padahal kalian mengetahui”.⁶⁷ (Q.S Al-Baqarah:188).

Dari ayat di atas dapat kita pahami bahwa *cyberfraud* adalah perbuatan yang tidak boleh dilakukan, memperoleh harta benda orang lain dengan cara yang bathil adalah termasuk dalam kejahatan pencurian baik dengan cara

⁶⁷Departemen Agama RI, *AL-Qur'an dan Terjemahan, Special For Women* (Bandung: Syamil AL-Qur'an, 2005), Hlm. 114.

menipu, mengambil secara diam-diam ataupun dengan cara merampas (kekerasan).

Dalam hukum pidana Islam kejahatan dapat dirujuk pada istilah *jināyah*. Istilah lain hukum kepidanaan atau disebut dengan *jarimah* adalah perbuatan-perbuatan yang dilarang oleh syara' yang diancam oleh Allah dengan hukuman *ḥad* atau *ta'zīr*.⁶⁸ Menurut istilah jarimah adalah perbuatan-perbuatan yang dilarang oleh *syara'*, *syara'* sendiri mengandung pengertian yang pertama yaitu larangan berbuat, larangan mengerjakan perbuatan yang dilarang. Dan yang kedua larangan tidak berbuat, larangan meninggalkan perbuatan yang diperintahkan yang diancam dengan hukuman *ḥad* atau *ta'zīr*.⁶⁹ Dengan demikian perbuatan-perbuatan yang dilarang untuk melakukannya dalam syara' diancam dengan hukuman *ḥad* atau *ta'zīr*.

Pidana *ta'zīr* merupakan hukuman yang bentuk dan ukurannya tidak ditentukan oleh *syara'*, akan tetapi *syara'* menyerahkan kepada kebijakan negara untuk menjatuhkan bentuk hukuman yang menurut negara sesuai dengan kejahatan yang dilakukan dan bisa memberikan efek jera, dengan memperhatikan dan mempertimbangkan keadaan individu yang bersangkutan, ruang, waktu dan perkembangan yang ada, sehingga bisa berbeda-beda sesuai dengan tingkat kemajuan dan peradaban masyarakat serta situasi dan kondisi manusia pada berbagai ruang dan waktu.⁷⁰

Ruang lingkup dalam *ta'zīr*, yaitu sebagai berikut:

1. *Jarimah ḥudūd* atau *qisās-diyat* yang terdapat syubhat, dialihkan ke sanksi *ta'zīr*, seperti:
 - b. Orangtua yang mencuri harta anaknya
 - c. Orangtua yang membunuh anaknya.

⁶⁸ Ahmad Wardi Muslich, *Hukum Pidana Islam*, (Jakarta: Sinar Grafika, 2005), hlm. ix.

⁶⁹ Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam, Cet.2*, (Jakarta: Sinar Grafika, 2006), hlm. 9.

⁷⁰ Wahbah Az- Zuhaili, *Fiqih Islam Wa Adilatuhu*, Darulfikir, Jakarta, Jilid 7, hlm. 259.

2. *Jarīmah ḥudūd* atau *qisās-diyat* yang tidak memenuhi syarat akan dijatuhi sanksi *ta'zīr*, contohnya percobaan pencurian, percobaan pembunuhan, dan percobaan zina.
3. *Jarīmah* yang ditentukan Al- qur'an dan Hadis, namun tidak ditentukan sanksinya. Misalnya penghinaan, tidak melaksanakan amanah, sanksi palsu, riba, suap, dan pembalakan liar.
4. *Jarīmah* yang ditentukan *ulil amri* untuk kemaslahatan umat, seperti penipuan, pencopetan, pornografi dan pornoaksi, penyeludupan, pembajakan, *human trafficking*, dan *money laundering*.⁷¹

Jarīmah ta'zīr apabila dilihat dari hak yang dilanggar dibagi menjadi dua, yaitu sebagai berikut:

- a. *Jarīmah ta'zīr* yang menyinggung hak Allah, yaitu semua perbuatan yang berkaitan dengan kemaslahatan umum. Misalnya, berbuat kerusakan di muka bumi, pencurian yang tidak memenuhi syarat, mencium wanita yang bukan istrinya, penimbunan bahan-bahan pokok, dan penyeludupan.
- b. *Jarīmah ta'zīr* yang menyinggung hak perorangan (individu), yaitu setiap perbuatan yang mengakibatkan kerugian pada orang tertentu, bukan orang banyak. Contohnya penghinaan, penipuan, dan pemukulan.⁷²

Sebagian ulama mengartikan bahwa *jarīmah ta'zīr* merupakan hukuman yang berkaitan dengan hak Allah dan hak hamba yang tidak ditentukan dalam Al-quran dan Hadis. Sebagian ulama yang lain mengatakan bahwa hukuman terhadap perbuatan maksiat yang tidak dihukum dengan hukuman *ḥad/kafarah*.⁷³ Dalam *jarīmah ta'zīr* tidak diperlukan asas legalitas secara khusus, artinya bahwa setiap tindak pidana tidak memerlukan ketentuan yang khusus, satu

⁷¹ M. Nurul Irfan dan Masyrofah, *Fiqh Jināyah...*, hlm. 144.

⁷² *Ibid.*, hlm. 144.

⁷³ *Ibid.*, hlm. 138.

persatu. Hal tersebut dikarenakan bukan banyaknya *jarīmah ta'zīr*, melainkan sifat *jarīmah* itu sendiri yang lebih dan fluktuatif, yang bisa berkurang dan bisa tambah sesuai dengan keperluan.⁷⁴

Kebanyakan bentuk-bentuk hukuman yang terdapat dalam undang-undang hukum positif adalah masuk kategori hukuman *ta'zīr*. Karena undang-undang hukum positif tersebut hanya semata-mata sebagai sebuah bentuk pengaturan dan rumusan yang di dalamnya dipertimbangkan hal-hal yang sesuai dengan bentuk dan tingkat kejahatan serta kondisi pelaku kejahatan, dengan tujuan untuk memberi efek jera dan perehabilitasian serta menciptakan suasana yang aman, nyaman, dan tenteram.⁷⁵

Macam-macam sanksi *ta'zīr*, yaitu sebagai berikut:⁷⁶

1. Sanksi *ta'zīr* yang berkaitan dengan badan

Adapun sanksi *ta'zīr* yang berkaitan dengan badan, dibedakan menjadi dua, yaitu:

a. Hukuman mati

Hukuman mati sebagai sanksi *ta'zīr* tertinggi hanya diberikan kepada pelaku *jarīmah* yang berbahaya sekali; berkaitan dengan jiwa, keamanan, ketertiban masyarakat; di samping sanksi *hudūd* tidak lagi memberi pengaruh baginya.

Mazhab Hanafi membolehkan sanksi *ta'zīr* dengan hukuman mati dengan syarat perbuatan itu dilakukan dengan berulang-ulang dan akan membawa kemaslahatan bagi masyarakat.⁷⁷ Contohnya, hukuman mati bagi residivis dan jenis lain yang dianggap sangat berbahaya bagi kemaslahatan masyarakat.

⁷⁴ Rahmat Hakim, *Hukum Pidana Islam*, (Bandung: Pustaka Setia, 2010), hlm. 141.

⁷⁵ Wahbah Az- Zuhaili, *Fiqh Islam*..., hlm. 259.

⁷⁶ M. Nurul Irfan dan Masyrofah, *Fiqh Jināyah*..., hlm. 147-159.

⁷⁷ M. Nurul Irfani, *Hukum Pidana Islam*, (Jakarta: Amzah, 2016), hlm. 96.

Mazhab Maliki dan sebagian mazhab Hanabillah juga memperbolehkan hukuman mati sebagai yang tertinggi. Contohnya sanksi bagi mata-mata dan orang yang melakukan perusakan di muka bumi. Sebagian ulama Syafi'iyah yang membolehkan hukuman mati, seperti hal kasus homoseks.⁷⁸

Untuk alat yang digunakan dalam melakukan hukuman mati pada sanksi *ta'zīr* sebagian ulama menggunakan pedang dikarenakan pedang mudah digunakan dan tidak menganiaya pelaku, serta bila menggunakan pedang lebih cepat kematiannya. Sebagian ulama menggunakan alat bantu seperti korsi listrik.

Dalam penerapan hukuman bagi pelaku *ta'zīr* dengan hukuman mati yang tertinggi hanya diberikan kepada pelaku yang sangat berbahaya sekali bagi kemaslahatan masyarakat, seperti yang berkaitan dengan jiwa, keamanan dan ketertiban atau apabila sanksi-sanksi yang sebelumnya telah melakukan kejahatan tersebut secara berulang-ulang.

b. Hukuman cambuk

Dalam *jarīmah ta'zīr*, hakim diberikan kewenangan untuk menetapkan jumlah cambukan disesuaikan dengan kondisi pelaku, situasi, dan tempat kejahatan.

Menurut pendapat kalangan mazhab Maliki dalam memberikan hukuman cambuk bahwa *jarīmah ta'zīr* adalah hak penguasa, maka batasan jumlah hukuman *ta'zīr* harus diserahkan kepada yang mempunyai hak, yaitu *ulil amri*. Dalam memberikan hukuman cambuk hakim harus mempertimbangkan situasi dan kondisi. Menurut Hanafiah, cambukan itu harus dilakukan lebih keras, dengan harapan si pelaku menjadi jera apabila jumlah cambukan lebih sedikit dari pada jumlah cambukan dari pada jumlah cambukan dalam *jarīmah ḥudūd*. Berapapun batas-batas terendah hukuman cambukan harus dapat menimbulkan dampak *preventif* dan *represif*.⁷⁹

⁷⁸ M. Nurul Irfani, *Hukum Pidana...*, 96.

2. Sanksi *ta'zīr* yang berkaitan dengan kemerdekaan seseorang

Mengenai hal ini ada dua jenis hukuman, yaitu hukuman penjara dan hukuman pengasingan. Penjelasannya sebagai berikut:

a. Hukuman penjara

Hukuman penjara dapat menjadi hukuman pokok dan dapat menjadi hukuman tambahan, apabila hukuman pokok berupa hukuman cambuk tidak membawa dampak bagi terhukum. Kemudian, hukuman ini dibedakan menjadi dua, yaitu sebagai berikut:

1). Hukuman penjara terbatas

Hukuman penjara terbatas ialah hukuman yang lama waktunya dibatasi secara tegas. Hukuman ini diterapkan untuk *jarīmah* penghinaan, menjual *khamr*, memakan riba, berbuka puasa pada siang hari di bulan Ramadhan tanpa uzur, mengairi ladang dengan air milik orang lain tanpa izin, dan bersaksi palsu.

Dalam pelaksanaan hukuman cambuk harus memperhatikan alat yang dipakai, tidak terlalu besar dalam mempergunakan cambuk untuk mencegah kerusakan yang berlebihan terhadap pelaku. Ulama sepakat bahwa hukuman cambuk tidak ditujukan kepada vital tubuh manusia si pelaku seperti ditujukan di mata, kemaluan atau kepala.⁸⁰ Untuk terhukum adalah laki-laki maka baju dibuka sedangkan bila perempuan maka baju tidak boleh dibuka dan pukulan diarahkan ke punggung.

2). Hukuman penjara tidak terbatas

Hukuman penjara tidak terbatas tidak dibatasi waktunya dan berlangsung terus sampai si terhukum meninggal dunia atau bertaubat. Hukuman ini disebut juga hukuman penjara seumur hidup.

⁷⁹ M. Nurul Irfani, *Hukum Pidana...*, hlm. 98.

⁸⁰ Ibid. 98.

b. Hukuman pengasingan

Hukuman pengasingan merupakan hukuman *ḥad*, namun dalam prakteknya hukuman tersebut diterapkan juga sebagai hukuman *ta'zīr*. Hukuman pengasingan ini dijatuhkan kepada pelaku jarimah yang dikhawatirkan dapat memberikan pengaruh buruk terhadap masyarakat. Dengan diasingkannya pelaku, diharapkan mereka akan terhindar dari pengaruh tersebut.

3. Hukuman *ta'zīr* yang berkaitan dengan harta

Hukuman *ta'zīr* dengan mengambil harta bukan berarti mengambil harta pelaku untuk diri hakim atau untuk kas negara, melainkan menahannya untuk sementara waktu. Adapun jika pelaku tidak dihadapkan untuk bertaubat, hakim dapat menyerakan harta tersebut untuk kepentingan yang mengandung maslahat.

Imam Ibnu Taimiyah membagi hukuman *ta'zīr* berupa harta ini menjadi tiga bagian, yaitu sebagai berikut:

a. Menghancurkannya (*Al-Itlāf*)

Penghancuran terhadap barang sebagai hukuman *ta'zīr* berlaku untuk barang-barang yang mengandung kemungkaran.

b. Mengubahnya (*Al-Ghayīr*)

Hukuman *ta'zīr* yang berupa mengubah harta pelaku, antara lain mengubah patung yang disembah oleh orang muslim dengan cara memotong bagian kepalanya sehingga mirip pohon atau vas bunga.

c. Memilikinya (*Al-Tamlīk*)

Hukuman *ta'zīr* berupa pemilikan harta pelaku. Hukuman denda dapat merupakan hukuman pokok yang berdiri sendiri. Ibnu Al-Qayyim menjelaskan bahwa ada dua macam denda yaitu denda yang dipastikan kesempurnaan dan denda yang tidak dipastikan kesempurnaannya.

- 1). Denda yang dipastikan kesempurnaannya ialah denda yang mengharuskan lenyapnya harta karena berhubungan dengan hak Allah.
- 2). Denda yang tidak pasti kesempurnaannya ialah denda yang ditetapkan melalui ijtihad hakim dan disesuaikan dengan pelanggaran yang dilakukan.

4. Sanksi *ta'zīr* lainnya

Adapun beberapa sanksi *ta'zīr* lainnya, selain hukuman-hukuman *ta'zīr* yang telah disebutkan yaitu sebagai berikut:

- a. Peringatan keras
- b. Dihadirkan di hadapan sidang
- c. Nasehat
- d. Celaan
- e. Pengucilan
- f. Pemecatan
- g. Pengumuman kesalahan secara terbuka, seperti diberitakan di media cetak atau elektronik.⁸¹

Di Indonesia suatu perbuatan pidana diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) namun untuk tindak pidana khusus ada Undang-Undang khusus yang dibuat oleh pemerintah untuk mengatur tindak pidana di luar KUHP. Untuk mengatur tindak pidana *cyberfraud* di Indonesia menggunakan Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dengan hukuman seperti dalam Pasal 47 dan Pasal 51. Pidana *ta'zīr* bagi pelaku *cyberfraud* di Indonesia sudah ada. Bentuk peraturan yang dibuat oleh pemerintah seperti adanya Undang-Undang ITE sudah memenuhi ketentuan dalam pidana *ta'zīr* yang dibuat oleh *ulil amri*.

⁸¹ *Ibid*, hlm. 157-160.

Penerapan dan peberlakuan bentuk-bentuk hukuman tersebut secara benar tanpa memberi ruang sedikitpun kepada praktek-praktek rekayasa, perantara untuk meminta pembatalan hukuman (*syafa'at*), dan praktek-praktek suap, akan bisa menekan angka kriminalitas atau mencegahnya. Penerapan bentuk-bentuk hukuman *had* dan *ta'zīr* secara benar, tegas dan sungguh-sungguh dengan memperhatikan aturan, ketentuan dan syarat-syarat yang ada, serta memperhatikan dan mempertimbangkan secara seksama keterpautan dan perbedaan antara faktor-faktor yang mengharuskan hukuman *had* dan faktor-faktor-faktor yang mengharuskan hukuman *ta'zīr*, semua itu bisa membawa kepada terciptanya masyarakat yang baik, aman, tenteram dan kondusif, serta mampu mengatasi fenomena kriminalitas.⁸²

Cyberfraud adalah suatu bentuk pencurian dan kecurangan yang dilakukan oleh pelakunya melalui dunia internet dengan menggunakan kartu kredit (*credit card*) dari hasil curian atau kartu kredit palsu yang dibuat menyerupai aslinya. Artinya para pelaku *cyberfraud* terlebih dahulu mencuri nomor-nomor kartu kredit sehingga dapat menciptakan nomor kartu kredit yang lain dengan bantuan program-program tertentu.

Bagaimanapun metode yang dilakukan dan modus operandi yang digunakan oleh pelaku *cyberfraud*, *cyberfraud* tetap merupakan suatu tindakan yang melanggar hukum. Dalam hal ini *cyberfraud* juga termasuk dalam kategori Jinayat yang disebut juga dengan hukum pidana Islam. Karena pada dasarnya *cyberfraud* merupakan aktivitas pencurian (mengambil dan memanfaatkan uang orang lain melalui kartu kredit tanpa izin orang tersebut).

Walaupun sudah ada peraturan yang membicarakan tentang data elektronik atau disebut juga hukum dunia maya (*cyberlaw*). Permasalahan *cyberfraud* di Indonesia belum disebut secara jelas dalam peraturan perundang-

⁸² Wahbah Az- Zuhaili, Fiqih Islam..., hlm. 260.

undangan yang sudah ada. Penegakan hukum terhadap tindak pidana *cyberfraud* dirasa masih terlalu prematur apabila menggunakan perangkat hukum yang sudah ada. Kendati demikian tindak pidana ini harus tetap diproses secara hukum karena perbuatan tersebut telah menimbulkan kerugian bagi banyak pihak, baik di dalam negeri maupun di luar negeri. Oleh sebab itu, kita dapat menggunakan perangkat hukum yang telah ada untuk menangani tindak pidana *cyberfraud*.

Tindak pidana *cyberfraud* apabila dikaji menggunakan pendekatan kontekstual dengan memperluas maknanya dari kata mengambil (*akhaḏa*) yang ada dalam rumusan definisi *sariqah* dan memperluas arti penyimpanan (*al-hirz*), maka *cyberfraud* bisa digolongkan kedalam *sariqah*. Namun dalam hal ini apabila tindak pidana dikaji dengan menggunakan pendekatan tekstual maka tidak dapat digolongkan ke dalam *sariqah* seperti yang dimaksudkan dalam surah Al- Mā'idah ayat 38 sebagai berikut :

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءُ بِمَا كَسَبَا نَكَالًا مِّنَ اللَّهِ
وَاللَّهُ عَزِيزٌ حَكِيمٌ

Artinya: “Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya (sebagai) pembalasan bagi apa yang mereka kerjakan dan sebagai siksaan dari Allah. dan Allah Maha Perkasa lagi Maha Bijaksana” (QS. Al- Mā'idah: 38).⁸³

Faktor yang dapat mencegah dimasukkannya *cyberfraud* ke dalam *sariqah* adalah keterkaitan antara keduanya menjadi sangat penting dalam pembicaraan mengenai *sariqah* karena proses pengambilan yang berbeda-beda akan menghasilkan konsekuensi hukum yang berbeda pula. Kalau kita cermati perbedaan konsekuensi hukum masing-masing variasi bentuk pencurian

⁸³DepagRI, *Al-Qur'an dan Terjemahnya*, hlm.165.

yang diungkapkan oleh para *fuqaha'*, maka akan terlihat jelas bahwa yang mendasari perbedaan tersebut tidak lain dan tidak bukan adalah terkait dengan bagaimana proses pengambilan dalam pencurian dilakukan.

Bahkan posisi pelaku dan tangan pelaku ketika melakukan pengambilanpun akan menghasilkan berbagai konsekuensi hukum. Pengaturan hukum Islam mengenai “proses pengambilan” ternyata sangat ketat, rinci dan tegas, sehingga sampai dalam hal *sariqahal-naqbī*, sahabat Ali berkomentar:

اذكن الث لسرف ليقط

Artinya: *Jika pencurinya pintar maka tidak dipotong.*

Maksudnya bila seorang pencuri bisa “menyiasati” ketentuan hukum yang ada dan ketat tersebut, maka ia bisa lepas dari jerat hukum *had*.⁸⁴ Oleh karena itu, apabila melihat bagaimana modus pengambilan harta dalam praktek *cyberfraud*, jelas tidak dapat disamakan dengan *sariqah*. Dalam *cyberfraud*, sang *carder* hanya menghadap komputer dan menekan tombol-tombol keyboard untuk “membobol” kartu kredit seseorang. Kemudian dengan kartu yang telah dibobol, dia mentrasfer sebagian atau semua yang tersimpan dalam kartu tersebut ke rekening lain untuk keperluan tertentu ataupun rekening sendiri. Dari penjelasan tersebut, jelas dikatakan bahwa *carder* secara kasat mata tidak melakukan kejahatan, dia hanya “bermain-main” dengan komputer.

Cyberfraud termasuk dalam jenis kejahatan pencurian. Pencurian dalam hukum Islam adalah mengambil harta orang lain dengan cara sembunyi-sembunyi (tidak terang-terangan) terhadap harta yang seharusnya dijaga dengan baik.

Dalam Islam pencurian biasa disebut *sirqoh* yaitu mengambil sesuatu dengan cara sembunyi, sedangkan menurut istilah *sirqoh* adalah mengambil sesuatu (barang) hak milik orang lain secara sembunyi-sembunyi dan ditempat

⁸⁴Wahbah Az- Zuhaili, *al-Fiqhu al- Islamy wa adilatuhu*, Juz 6, hlm. 111.

penyimpanan yang pantas.⁸⁵ Pencurian bila ditinjau dari syariat Islam ada dua macam, diantaranya: pencurian yang hukumnya *ḥad* dan pencurian yang hukumnya *ta'zīr*.⁸⁶ Pencurian yang hukumnya *ḥad* terbagi menjadi dua bagian yaitu:

a. Pencurian ringan

Pencurian ringan adalah pengambilan harta yang dilakukan secara sembunyi-sembunyi tanpa kekerasan dengan cara yang mereka rencanakan.

b. Pencurian berat

Pencurian berat adalah pengambilan harta orang lain secara terang-terangan dengan kekerasan.

Perbedaan antara pencurian ringan dengan pencurian berat adalah bahwa dalam pencurian ringan pengambilan harta dilakukan tanpa sepengetahuan pemilik dan tanpa persetujuannya, sedangkan dalam pencurian berat pengambilan harta dilakukan dengan sepengetahuan pemilik harta tapi tanpa kerelaannya dan diikuti dengan adanya unsur kekerasan.

Untuk memberikan suatu sanksi pidana *cyberfraud* tidak hanya menggunakan Al- Qur'an dan Hadis saja. Al- Qur'an dan Hadis juga menyerahkan kepada *Ulil Amri* untuk urusan-urusan hukum pidana, sanksi pidana, perbuatan yang dinilai pidana yang belum ada ketentuan di dalam nas untuk diatur dan diberikan hukuman *ta'zīr*. Hukuman *ta'zīr* hukuman yang belum ditetapkan oleh *syara'*, melaikan diserahkan kepada hakim, baik penentuannya maupun pelaksanaannya.

Dalam pidana Islam, sumber hukum pidana tidak hanya berasal dari *ḥudūd*, *qīṣaṣ-diyat*, tetapi juga yang bersumber dari *ta'zīr* yang mana ketentuan perbuatan apa yang dikelompokkan ke dalam pidana dan seperti apa bentuk

⁸⁵Sudarsono, *Pokok-pokok Hukum Islam*, (Jakarta: Rineka Cipta, Cet Ke-2, 2001), hlm. 545.

⁸⁶Djazuli, *Fiqh Jināyah*, (Jakarta: PT Raja Grafindo Persada, 1997), hlm. 71.

sanksinya, *syari'at* memberikan keluasaan kepada *Ulil Amri*. Saat ini pemerintah Indonesia sudah membuat Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menjerat pelaku *cyberfraud*. Sehingga hukum yang telah dibuat pemerintah dapat dikatakan sebagai hukuman *ta'zīr* sebagaimana ketentuannya di dalam hukum pidana Islam.

Tindakan *cyberfraud* sudah jelas merupakan perbuatan yang melanggar hukum, karena tindakannya telah merugikan orang lain, yakni korban yang merupakan pemilik kartu kredit. Kemudian cara mendapatkan kartu kredit tersebut juga melawan hukum, karena mencuri data orang lain tanpa izin ataupun sepengetahuan pemiliknya. Hal ini bisa dijerat dengan pasal 31 ayat (2) dan pasal 35 UU ITE Tahun 2008.

Adapun mengenai sanksi hukumannya terdapat pada pasal 47, yaitu “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)”. Kemudian tindak pidana *cyberfraud* juga dapat dipidana dengan menggunakan pasal 51, yaitu “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)”.

D. Analisis Sanksi Pidana *Cyberfraud* pada UU No. 11 Tahun 2008 Perspektif Hukum Pidana Islam

Dalam hukum pidana Islam untuk menjerat pelaku *cyberfraud* dapat diancam dengan hukuman *ta'zīr*. Karena hukuman *ta'zīr* ini merupakan hukuman yang belum ditentukan oleh *syara'*, melainkan diserahkan kepada *ulil amri*, baik penentuannya maupun pelaksanaannya. Sehingga untuk menentukan hukumannya, penguasa hanya menetapkan hukuman secara global. Maksudnya ialah pembuatan Undang-Undang tidak menetapkan hukuman untuk masing-

masing jarīmah *ta'zīr*, melainkan hanya menetapkan keseluruhan hukumannya, dari yang paling ringan hingga yang sangat berat. Sehingga dalam hal ini pelaku *cyberfraud* akan mendapatkan hukuman yang setimpal dengan perbuatannya.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan peraturan yang dibuat oleh pemerintah di Indonesia yang mana dalam hukum pidana Islam peraturan tersebut dapat dikatakan sebagai hukuman *ta'zīr*.

Dalam hukum pidana Islam tidak hanya menggunakan Al-Qur'an dan hadis sebagai dasar hukum yang di dalamnya terdapat hukuman *ḥudūd*, *qisās-diyat* akan tetapi dalam hal apabila suatu tindak pidana tidak diatur di dalam *syara'*, maka dapat menggunakan sumber hukum yang berasal dari hukuman *ta'zīr*.

Persamaan dan Perbedaan Tindak Pidana *Cyberfraud* dalam Hukum Pidana Islam dan UU No. 11 Tahun 2008 Tentang ITE yaitu sebagai berikut:

a. Persamaannya

1. Tidak disebutkan secara jelas dalam Perundang-undangan maupun Al-Qur'an dan Hadis
2. Sama-sama merupakan tindakan kejahatan
3. Akibat yang ditimbulkan dapat merugikan orang lain, yang dimaksud adalah pemilik kartu kredit
4. Merupakan perbuatan yang dilarang

b. Perbedaannya

Adapun perbedaannya terdapat pada sanksi atau hukuman yang diberikan kepada pelaku *cyberfraud* atau *carder*. Dalam Hukum Pidana Islam, *carder* dapat diancam dengan hukuman *ta'zīr*. Sedangkan menurut undang-undang hukum pidana yang juga merupakan produk hukum yang dibuat oleh pemerintah/penguasa yaitu Undang-undang No.11 tahun 2008 tentang ITE, *carder* dapat dipidana dengan pidana penjara paling lama 10 tahun dan atau

denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)". Kemudian tindak pidana *cyberfraud* juga dapat dipidana dengan menggunakan pasal 51, yaitu "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)".



BAB EMPAT PENUTUP

A. Kesimpulan

Berdasarkan permasalahan yang dipaparkan dalam penelitian ini, maka hasil pembahasan yang telah diuraikan dapat disimpulkan sebagai berikut:

1. Bentuk-Bentuk *Cyberfraud*

- a. *Misuse (compromise) of card data*
- b. *Counterfeiting*
- c. *Wire Tapping*
- d. *Pishing*

2. Tinjauan Hukum Pidana Islam Terhadap Sanksi Pidana *Cyberfraud* yang Ditentukan Dalam UU No.11 Tahun 2008

a. Sanksi Pidana *Cyberfraud* dalam UU No.11 Tahun 2008

Sanksi bagi pelaku tindak pidana *cyberfraud* yaitu dengan ancaman pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). Hal ini tertera dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 35 dan Pasal 51 ayat 1.

b. Dalam Hukum Pidana Islam

Dalam *cyberfraud* dapat dikategorikan pencurian ringan karena aktivitas *cyberfraud* sama sekali tidak melukai fisik korban, pelaku seolah-olah hanya mengotak-atik komputer menggunakan jaringan internet untuk menipu korban. Kemudian pencurian dengan hukuman *ta'zīr* juga terbagi dua yakni semua jenis pencurian yang dikenai *ḥad*, tetapi syarat-syaratnya tidak terpenuhi atau ada syubhat dan pengambilan harta milik orang lain dengan sepengetahuan pemilik tanpa kerelaannya dan tanpa kekerasan. Dalam hal ini *cyberfraud* dapat dikategorikan tindak pidana yang bisa juga dikenai hukuman *ta'zīr* berdasarkan cara pelaku *cyberfraud* dalam mengelabui korban.

- c. Analisi sanksi pidana *cyberfraud* dalam UU No. 11 Tahun 2008 perspektif hukum pidana Islam

Dalam pidana Islam, sumber hukum pidana tidak hanya berasal dari *ḥudūd*, *qisās-diyat*, tetapi juga yang bersumber dari *ta'zīr* yang mana ketentuan perbuatan apa yang dikelompokkan ke dalam pidana dan seperti apa bentuk sanksinya, *syari'at* memberikan keluasaan kepada *Ulil Amri*. Saat ini pemerintah Indonesia sudah membuat Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menjerat pelaku *cyberfraud*. Sehingga hukum yang telah dibuat pemerintah dapat dikatakan sebagai hukuman *ta'zīr* sebagaimana ketentuannya di dalam hukum pidana Islam.

B. Saran

Berdasarkan permasalahan yang penulis uraikan pada bab-bab sebelumnya, maka dapat diberikan beberapa saran, yaitu sebagai berikut:

1. Untuk para pelajar atau akademisi dan para peneliti selanjutnya diharapkan dapat lebih baik dalam mengembangkan teori yang lebih relevan dengan saat ini berdasarkan kasus dan gejala sosial yang terjadi di lingkungan masyarakat agar lebih peduli terhadap perkembangan zaman yang semakin maju yang mengakibatkan banyaknya tindakan kejahatan yang terjadi melalui dunia maya atau *online* khususnya kejahatan *cyberfraud*, sehingga dapat melakukan pencegahan ataupun pengamanan serta solusi untuk menangani para pelaku tindak pidana *cyberfraud* ini secara lebih tepat.
2. Untuk masyarakat diharapkan lebih berhati-hati dalam melakukan transaksi *online* baik dalam kegiatan berbelanja ataupun transfer uang serta melakukan tindakan pengamanan terkait data kartu kredit.
3. Untuk Kementerian Komunikasi dan Informatika serta lembaga-lembaga yang berwenang sebaiknya lebih teliti dalam melacak dan mengidentifikasi para pelaku kejahatan ini dikarenakan kejahatan jenis ini

cukup sulit untuk dilacak serta memberikan hukuman yang tegas kepada siapapun juga yang mencoba atau melakukan kejahatan *cyberfraud* agar tidak menimbulkan efek yang besar dalam masyarakat.



DAFTAR PUSTAKA

Buku-Buku

- Abdul Manaf, *Pembaruan hukum Islam Di Indonesia*, Depok: Kencana, 2017.
- Abdul Wahab Ibrahim Abu Sulaiman, *Banking Cards Syariah (Kartu Kredit dan Debit Dalam Perspektif Fiqih)*, Jakarta: PT Raja Grafindo Persada, 2006.
- Abu Zakaria Yahya ibn SyarafAl-Nawawiy, *Shahih Muslim bi Syarh al-Nawawiy*, Beirut: Dar al –Fikr, 1983.
- Adami Ghazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik :Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, Malang: Media Nusa Creative, 2015.
- Ahmad Wardi Muslich, *Hukum Pidana Islam*, Jakarta: Sinar Grafika, 2016.
- Ahmad Wardi Muslich, *Hukum Pidana Islam*, Jakarta: Sinar Grafika, 2005.
- Ahmad Wardi Muslich, *Pengantar Dan Asas Hukum Pidana Islam Fikih Jinayah*, Jakarta: Sinar Grafika, 2006.
- Andi Hamzah, *Hukum Acara Pidana Indonesia*, Jakarta: Sinar Grafika, 2004.
- Asmuni A. Rahman, *Qaidah-Qaidah Fiqih*, Jakarta: Bulan Bintang, 1976.
- Aziz Syamsuddin, *Tindak Pidana Khusus*, Jakarta: Sinar Grafika, 2016.
- Bambang Sunggono, *Pengantar Metodologi Penelitian Hukum*, Jakarta: PT. Raja Grafindo Persada, 2007.
- Barda Nawawi Arief, *Tindak Pidana Mayantara*, Jakarta: PT Raja Grafindo Persada, 2006.
- Dedy Sumardi, dkk. *Hukum Pidana Islam*, Banda Aceh: Fakultas Syariah UIN Ar-Raniry, 2014.
- Departemen Agama RI, *AL-Qur'an dan Terjemahan, Special For Women* Bandung: Syamil AL-Qur'an, 2005.

- Djazuli, *Fiqh Jinayah*, Jakarta: PT Raja Grafindo Persada, 1997.
- Frank E. Hagan, *Pengantar Kriminologi: Teori, Metode, dan Perilaku Kriminal*, Edisi Ke-7, Jakarta : Kencana Prenamedia Group, 2013.
- Hassan Saleh, *Kajian Fiqh Nabawi dan Fiqh kontemporer*, Jakarta: PT Raja Grafindo Persada, 2008.
- Husni Mubarrak A. Latief, *Fiqh Islam Dan Problematika Kontemporer*, Banda Aceh: Arraniry Press dan Lembaga Naskah Aceh (NASA), 2012.
- Irman, *Anatomi Kejahatan Perbankan (banking crime anatomy)*, Bandung: MQS Publishing dan AYYCCS GROUP, 2006.
- M. Nurul Irfan dan Masyrofah, *Fiqh Jinayah*, Jakarta: Amzah, 2018.
- Mahrus Ali, *Dasar-Dasar Hukum Pidana*, Jakarta: Sinar Grafika, 2015.
- Maskun, *Kejahatan Siber (Cyber Crime)*, Kencana, Jakarta, 2013.
- Mohammad Daud Ali, *Hukum Islam*, Jakarta: PT Raja Grafindo Persada, 2011.
- Muslim bin al-Haj Ibn Muslim al-Qusyiriy al-Naisaburiy (al-Muslim), *Shahih al Muslim* Bairut : Dar al-Fikr, t.th, Juz 8.
- Mustofa dan Abdul Wahid, *Hukum Islam Kontemporer*, Jakarta: Sinar Grafika, 2013.
- Mustofa Hasan, *Hukum Pidana Islam Fiqh Jinayah*.
- Niniek Suparni, *Eksistensi Pidana Denda Dalam Sistem Pidana Dan Pemidanaan*, Jakarta: Sinar Grafika, 2007.
- Nurul Irfani, *Hukum Pidana Islam*, Jakarta: Amzah, 2016.
- Rahman, *Penjelasan Lengkap Hukum-hukum Allah (Syariah)*, Jakarta: Raja Grafindo Persada, 2002.
- Rahmat Hakim, *Hukum Pidana Islam*, Bandung: Pustaka Setia, 2010.
- Siswanto Sunarto, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, Jakarta: Rineka Cipta, 2009.
- Sudarsono, *Pokok-pokok Hukum Islam*, Jakarta: Rineka Cipta, Cet Ke-2, 2001.

Sutan Remy Sjahdeini, *Kejahatan & Tindak Pidana Komputer*, Cet Ke- I, Jakarta: Pustaka Utama Grafiti, 2009.

Teguh Prasetyo, *Hukum Pidana*, Depok: Raja Grafindo Persada, 2017.

Wahbah Az- Zuhaili, *Fiqh Islam Wa Adilatuhu*, Terj. Abdul Hayyie al- Kattani, dkk. Cet 1, Jilid 7, Jakarta: Gema Insani, 2011.

Zainuddin Ali, *Hukum Pidana Islam*, Jakarta: Sinar Grafika, 2012.

Zulkarnain Lubis dan Bakti Ritonga, *Dasar-Dasar Hukum Acara Jinayah*, Jakarta: Kencana, 2016.

Jurnal Ilmiah

Leo T. Panjaitan, “Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008: IncomTech”. *Jurnal Telekomunikasi dan Komputer*, Vol. 3, No. 1, 2012, hlm. 13.

Sumber lain

<https://kejahatanduniacyber.wordpress.com/pembahasan/cyber-crime/> diakses pada hari Senin 20 Mei 2019 Pukul 00:02 WIB

<https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi/> diakses pada hari senin 20 Mei 2019 Pukul 01:47 WIB

<https://news.detik.com/berita/d-3810769/total-ada-68-wna-yang-ditangkap-terkait-cyber-fraud-di-bali> diakses pada hari Kamis 19 September Pukul 11.00 WIB

Credit Card for Profit, <http://textfiles.com/anarchy/CARDING/credit> diakses pada tanggal 20 Januari 2020.

Cyrus Farivar, *Ukrainian fraudster dan Carderplanet “Don” Finally Sentenced to 18 years*, <https://arstechnica.com/tech-policy/2013/12/ukrainian-fraudster-andcarderplanet-don-finallysentenced-to-18-years/> diakses pada hari Kamis tanggal 13 Februari Pukul 11:23 WIB.

<https://needr005.wordpress.com/pihak-pihak-yang-terkait-dalam-carding/> Di akses pada tanggal 17 Februari 2020 pada Pukul 01:36 WIB



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
FAKULTAS SYARI'AH DAN HUKUM

Jl. Syekh Abdur Rauf Kopelma Darussalam Banda Aceh
Telp. 0651-7557442 Email: fsh@ar-raniry.ac.id

SURAT KEPUTUSAN DEKAN FAKULTAS SYARI'AH DAN HUKUM
UIN AR-RANIRY BANDA ACEH
Nomor: 3894/Un.08/FSH/PP.009/07/2019

T E N T A N G
PENETAPAN PEMBIMBING SKRIPSI MAHASISWA

DEKAN FAKULTAS SYARI'AH DAN HUKUM

Menimbang : a. Bahwa untuk kelancaran bimbingan KKU Skripsi pada Fakultas Syari'ah dan Hukum, maka dipandang perlu menunjuk pembimbing KKU Skripsi tersebut;
b. Bahwa yang namanya dalam Surat Keputusan ini dipandang mampu dan cakap serta memenuhi syarat untuk diangkat dalam jabatan sebagai pembimbing KKU Skripsi.

Mengingat : 1. Undang-undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
2. Undang-undang Nomor 14 Tahun 2005 tentang Guru dan Dosen;
3. Undang-undang Nomor 12 Tahun 2012 Tentang Pendidikan Tinggi;
4. Peraturan Pemerintah Nomor 19 Tahun 2005 tentang Standar Nasional Pendidikan;
5. Peraturan Pemerintah Nomor 04 Tahun 2014 tentang penyelenggaraan Pendidikan Tinggi dari Pengelolaan Perguruan Tinggi;
6. Peraturan Presiden RI Nomor 64 Tahun 2013 tentang Perubahan Institut Agama Islam Negeri IAIN Ar-Raniry Banda Aceh Menjadi Universitas Islam Negeri;
7. Keputusan Menteri Agama 492 Tahun 2003 tentang Pendelegasian Wewenang Pengangkatan, Pemindahan dan Pemberhentian PNS di lingkungan Agama RI;
8. Peraturan Menteri Agama Republik Indonesia Nomor 12 Tahun 2014 tentang Organisasi dan Tata Kerja Universitas Islam Negeri Ar-Raniry Banda Aceh;
9. Peraturan Menteri Agama Republik Indonesia Nomor 21 Tahun 2015 Tentang Statuta Universitas Islam Negeri Ar-Raniry;
10. Surat Keputusan Rektor UIN Ar-Raniry Nomor 01 Tahun 2015 tentang Pemberi Kuasa dan Pendelegasian Wewenang Kepada Para Dekan dan Direktur Program Pascasarjana dalam Lingkungan UIN Ar-Raniry Banda Aceh;

M E M U T U S K A N

Menetapkan :

Pertama :

- Menunjuk Saudara (i) :
a. Dr. Abdul Jalil Salam, S.Ag., M.Ag.
b. Syarifah Rahmatillah, S.H.I., M.H.

Sebagai Pembimbing I
Sebagai Pembimbing II

untuk membimbing KKU Skripsi Mahasiswa (i) :

Nama : Al-Viratun
NIM : 160104003
Prodi : Hukum Pidana Islam
Judul : Tindak Pidana Cyberfraud dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Menurut Tinjauan Hukum Islam

Kedua : Kepada pembimbing yang tercantum namanya di atas diberikan honorarium sesuai dengan peraturan perundang-undangan yang berlaku;

Ketiga : Pembiayaan akibat keputusan ini dibebankan pada DIPA UIN Ar-Raniry Tahun 2019;

Keempat : Surat Keputusan ini mulai berlaku sejak tanggal ditetapkan dengan ketentuan bahwa segala sesuatu akan diubah dan diperbaiki kembali sebagaimana mestinya apabila ternyata terdapat kekeliruan dalam keputusan ini.

Kutipan Surat Keputusan ini diberikan kepada yang bersangkutan untuk dilaksanakan sebagaimana mestinya.



Ditetapkan di : Banda Aceh
Pada tanggal : 1 Oktober 2019
Dekan,

Muhammad Siddiq

Tembusan :

1. Rektor UIN Ar-Raniry;
2. Ketua Prodi HPI;
3. Mahasiswa yang bersangkutan;
4. Arsip.