

**TINJAUAN YURIDIS TERHADAP
TINDAK PIDANA PERETASAN KARTU
KREDIT MELALUI ONLINE BERDASARKAN
UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG
INFORMASI DAN TRANSASI ELEKTRONIK DI INDONESIA**

SKRIPSI



Diajukan Oleh :

RAUSYAN FIKRY

NIM : 190106107

Mahasiswa Fakultas Syari'ah dan Hukum

Prodi Ilmu Hukum

**UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
FAKULTAS SYARI'AH DAN HUKUM
PRODI ILMU HUKUM
2024 M/1445 H**

**TINJAUAN YURIDIS TERHADAP
TINDAK PIDANA PERETASAN KARTU
KREDIT MELALUI ONLINE BERDASARKAN
UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG
INFORMASI DAN TRANSASI ELEKTRONIK DI INDONESIA**

SKRIPSI

Diajukan kepada Fakultas Syari'ah dan Hukum
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
sebagai salah satu beban studi Program Sarjana (S1)
dalam Ilmu Hukum

Oleh:

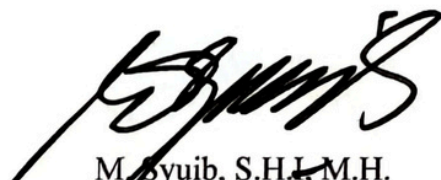
RAUSYAN FIKRY


Mahasiswa Fakultas Syari'ah dan Hukum
prodi Ilmu Hukum
NIM. 190106107

Disetujui dan Dimunaqasyahkan Oleh:

Pembimbing I,

Pembimbing II,


M. Syuib, S.H., M.H.
NIP. 198109292015031001


Muhammad Iqbal, M.M.
NIP. 19700512201411001

**TINJAUAN YURIDIS TERHADAP
TINDAK PIDANA PERETASAN KARTU
KREDIT MELALUI ONLINE BERDASARKAN
UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG
INFORMASI DAN TRANSASI ELEKTRONIK DI INDONESIA**

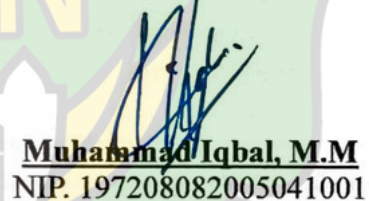
SKRIPSI

Telah diuji oleh Panitia Ujian Munaqasyah Skripsi
Fakultas Syari'ah dan Hukum UIN Ar-Raniry
dan dinyatakan lulus serta diterima
sebagai salah satu beban studi
Program Sarjana (S-1)
dalam Ilmu Hukum
pada hari/tanggal: Jum'at, 14 Juni 2024
7 Dzulhijjah 2024
di Darussalam, Banda Aceh
Panitia Ujian Munaqasyah Skripsi:

Ketua,


Sekretaris,

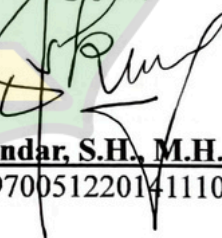

M. Syaib, S.H.I, M.H
NIP. 198109292015031001


Muhammad Iqbal, M.M
NIP. 197208082005041001

Penguji I,

Penguji II,


Yenny Sriwahyuni, M.H
NIP. 198101222014032001


Iskandar, S.H., M.H.
NIP. 197005122014111001





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

Jl. Sycikh Abdur Rauf Kopelma Darussalam Banda Aceh
Telepon : 0651-7557321, Email : uin@ar-raniry.ac.id

PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan di bawah ini

Nama : Rusyan Fikry
NIM : 190106107
Program Studi : Ilmu Hukum
Fakultas : Syari'ah dan Hukum

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 melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap untuk dicabut gelar akademik atau diberikan sanksi lain berdasarkan aturan yang berlaku di Fakultas Syari'ah dan Hukum UIN Ar-Raniry.

Demikian Pernyataan ini Saya buat dengan sesungguhnya.

Banda Aceh, 30 Desember
2024

Yang Menyatakan




(Rausyan Fikry)

ABSTRAK

Nama : Rausyan Fikry
NIM : 190106107
Fakultas/Prodi : Syariah dan Hukum/Ilmu Hukum
Judul : Tinjauan Yuridis Terhadap Tindak Pidana Peretasan Kartu Kredit Melalui Online Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik di Indonesia
Tanggal Sidang : Senin, 30, desember, 2024
Tebal Skripsi : 78 halaman
Pembimbing I : M. Syuib, S.H.I., M.H
Pembimbing II : Muhammad Iqbal, M.M
Kata Kunci : *peretasan kartu kredit, kejahatan siber, UU ITE, OJK, penegakan hukum, perlindungan konsumen*

Penelitian ini membahas tentang tindak pidana peretasan kartu kredit melalui online yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Meningkatnya transaksi elektronik dan penggunaan kartu kredit di era digital membawa dampak positif bagi perekonomian, namun juga menimbulkan risiko kejahatan siber, khususnya peretasan kartu kredit. Permasalahan utama dalam penelitian ini adalah bagaimana regulasi yang ada dapat melindungi korban peretasan kartu kredit serta efektivitas penegakan hukum dalam kasus ini. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan dan analisis teori hukum, serta memanfaatkan data sekunder dari literatur hukum, jurnal, dan laporan kasus. Berdasarkan analisis, ditemukan bahwa meskipun UU ITE telah memberikan dasar hukum yang kuat untuk menjerat pelaku peretasan kartu kredit, implementasinya masih menghadapi berbagai kendala, termasuk keterbatasan teknologi forensik dan ketergantungan pada kerja sama internasional. Selain itu, Otoritas Jasa Keuangan (OJK) dan Bank Indonesia memiliki peran penting dalam melindungi konsumen melalui berbagai regulasi yang mewajibkan lembaga keuangan untuk meningkatkan standar keamanan dan manajemen risiko. Hasil penelitian ini menunjukkan bahwa peningkatan efektivitas penegakan hukum terhadap tindak pidana peretasan kartu kredit memerlukan sinergi antara peningkatan sumber daya teknologi dan peningkatan kerja sama internasional. Diharapkan, penelitian ini dapat memberikan kontribusi dalam pengembangan kebijakan terkait keamanan data di sektor keuangan digital dan peningkatan perlindungan bagi konsumen di Indonesia.

KATA PENGANTAR



Puji syukur kepada Allah SWT berkat Rahmat, Hidayah, dan Karunianya kepada kita semua, shalawat dan salam tidak lupa pula kita curahkan kepada pangkuan Nabi Muhammad SAW, karena beliau telah mengubah pola pikir manusia di seluruh dunia dari alam kebodohan ke alam yang berilmu pengetahuan. Sehingga penulis dapat menyelesaikan proposal ini yang berjudul **“TINJAUAN YURIDIS TERHADAP TINDAK PIDANA PERETASAN KARTU KREDIT MELALUI ONLINE BERDASARKAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSASI ELEKTRONIK DI INDONESIA”**. Penelitian ini disusun untuk memenuhi salah satu syarat memperoleh gelar Sarjana Hukum pada Program Studi Ilmu Hukum Fakultas Syari’ah Dan Hukum, Universitas Islam Negeri Ar-Raniry Banda Aceh.

Tidak ada manusia yang sempurna, demikian pula dalam penyusunan karya ilmiah ini, penulis mendapat bimbingan, arahan dan bantuan dari banyak pihak sehingga skripsi dapat terselesaikan. Oleh karena itu, penulis menyampaikan ungkapan terima kasih kepada :

1. Bapak Prof. Dr. Mujiburrahman, M.Ag. selaku Rektor UIN AR-Raniry Banda Aceh.
2. Bapak Prof. Dr. Kamaruzzaman, M.Sh selaku Dekan Fakultas Syari’ah dan Hukum.
3. Ibu Sitti Mawar, S.Ag., M.H. selaku ketua prodi Ilmu Hukum dan Bapak Riza Afrian Mustaqim, M.H. selaku sekretaris prodi Ilmu Hukum, beserta seluruh staf prodi yang telah banyak membantu penulis selama mengerjakan skripsi ini.

4. Bapak Muhammad Syuaib, S.H.I., M.H selaku pembimbing pertama dan Bapak Muhammad Iqbal, S.E., M.M Selaku pembimbing kedua. Terima kasih telah senantiasa ikhlas memberikan bimbingan, arahan, masukan kepada penulis dalam menyelesaikan penelitian ini.
5. Ibu Yenny Sriwahyuni, M.H selaku dosen penguji pertama dan Bapak Iskandar, S.H., M.H selaku Dosen penguji kedua. Terima kasih sudah senantiasa memberikan masukan, arahan, dan perbaikan kepada penulis dalam menyelesaikan penelitian ini.
6. Orang tua tercinta Ayahanda Anhar dan Ibunda Habibah, dua orang hebat yang menjadi penyemangat dan alasan saya berada di titik ini, terimakasih sudah bersedia merawat saya sejak lahir hingga saat ini, memberikan kasih sayang penuh cinta, selalu memberikan semangat dan dukungan baik moral maupun materi dan juga doa yang tidak ada putusnya. Terimakasih selalu berjuang dan berkorban untuk kehidupan saya, semoga jerih payah terbalaskan berkali-kali lipat. Sehat dan bahagia selalu surga saya.

Semoga Allah SWT melimpahkan karunia-Nya serta membalas kebaikan kepada seluruh pihak yang membantu dalam menyelesaikan penelitian ini. Besar harapan saya agar penelitian ini dapat bermanfaat bagi pembaca, terutama penulis. Penulis berharap ada masukan yang membangun untuk kesempurnaan penelitian ini.

Banda Aceh, 15 Agustus 2024

Penulis,

Rusyan Fikry

PEDOMAN TRANSLITERASI

Keputusan Bersama Menteri Agama dan Menteri P dan K Nomor: 158 Tahun
1987 – Nomor: 0543 b/u/1987

1. Konsonan

Fonem konsonan bahasa Arab yang dalam sistem tulisan Arab dilambangkan dengan huruf. Dalam transliterasi ini sebagian dilambangkan dengan huruf dan sebagian dilambangkan dengan tanda, dan sebagian lagi dilambangkan dengan huruf dan tanda sekaligus.

No	Arab	Latin	No	Arab	Latin
1	ا	Tidak dilambangkan	16	ط	T
2	ب	B	17	ظ	Z̤
3	ث	T	18	ع	‘
4	ث	Ṣ	19	غ	G
5	ج	J	20	ف	F
6	ح	Ḥ	21	ق	Q
7	خ	Kh	22	ك	K
8	د	D	23	ل	L
9	ذ	Ḍ	24	م	M
10	ر	R	25	ن	N
11	ز	Z	26	و	W
12	ص	S	27	ه	H
13	ش	Sy	28	ء	‘
14	ص	Ṣ	29	ي	Y
15	ض	Ḍ			

2. Vokal

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:

kaifa : كيف

Haul : هول

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
أَ/إِ	<i>Fathah</i> dan <i>alif</i> atau <i>ya</i>	Ā
إِ	<i>Kasrah</i> dan <i>ya</i>	Ī
ئِ	<i>Dammah</i> dan <i>wau</i>	Ū

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 katanya 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:

رَوْضَةُ الْأَطْفَالِ : *Rauḍah al-atfāl/ raudatulatfāl*

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

طَلْحَةُ : *Talḥah*

Catatan:

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.

Kata-kata yang sudah dipakai (serapan) dalam kamus Bahasa Indonesia tidak ditransliterasi. Contoh: Tasauf, bukan Tasawuf.

5. *Syaddah (Tasydīd)*

Syaddah atau disebut dengan kata *tasydīd* yang dalam sistem tulisan Arab dilambangkan dengan satu tanda *tasydīd* (◌ْ) dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda *syaddah*, misalnya di dalam contoh berikut:

رَبَّنَا : *rabbānā*

نَجَّيْنَا : *najjainā*

الْحَقُّ : *al-ḥaqq*

الْحَجُّ : *al-ḥajj*

نُعَمُّ : *nu'ima*

عَدُوُّ : *'aduwwun*

Jika huruf *ع* memiliki *tasydīd* di akhir suatu kata, dan kemudian didahului oleh huruf berharakat kasrah (ـِ), maka ia ditransliterasi seperti huruf *maddah* (ī).

Contoh:

عَلِيٍّ : 'Alī (bukan 'Aliyy atau 'Aly)

عَرَبِيٍّ : 'Arabī (bukan 'Arabiyy atau 'Araby)

Contoh:

عَلِيٍّ : 'Alī (bukan 'Aliyy atau 'Aly)

عَرَبِيٍّ : 'Arabī (bukan 'Arabiyy atau 'Araby)

6. Kata Sandang

Kata sandang dalam sistem tulisan Arab dilambangkan dengan huruf ال (*alif lam ma'arifah*). Pada pedoman transliterasi ini, kata sandang ditransliterasi seperti biasa yaitu (*al-*), baik ketika ia diikuti oleh huruf *syamsiah* maupun huruf *qamariah*. Kata sandang tersebut tidaklah mengikuti bunyi huruf langsung yang mengikutinya. Kata sandang itu ditulis terpisah dari kata yang mengikutinya dan dihubungkan dengan garis mendatar (-). Contohnya:

الشَّمْسُ : *al-syamsu* (bukan *asy-syamsu*)

الزَّلْزَلَةُ : *al-zalzalah* (bukan *az-zalzalah*)

الفَلْسَفَةُ : *al-falsafah*

الْبِلَادُ : *al-bilādu*

7. Hamzah

Aturan transliterasi huruf hamzah menjadi apostrof (') hanya berlaku bagi hamzah yang terletak di tengah dan akhir kata. Namun, bila hamzah terletak di awal kata, ia tidak dilambangkan, karena di dalam tulisan Arab ia berupa *alif*. Contohnya:

تَأْمُرُونَ : *ta'murūna*

النَّوْءُ : *al-nau'*

شَيْءٌ : *syai'un*

أُمِرْتُ : *umirtu*

8. Penulisan Kata Arab yang Lazim digunakan dalam Bahasa Indonesia

Kata, istilah, atau kalimat Arab yang ditransliterasikan adalah kata, istilah, atau kalimat yang belum dibakukan dalam bahasa Indonesia. Kata, istilah atau kalimat yang telah lazim dan menjadi bagian dari perbendaharaan dalam bahasa Indonesia, atau sudah sering ditulis di dalam tulisan bahasa Indonesia, tidak lagi ditulis menurut cara transliterasi di atas. Misalnya kata Alquran dari *al-Qur'ān*, sunnah, hadis, khusus dan juga umum. Namun, bila kata-kata tersebut menjadi bagian dari satu rangkaian teks Arab, maka mereka harus ditransliterasi secara utuh.

Contoh:

في ظلال القرآن	: <i>Fī ḡilāl al-Qur'ān</i>
السنة قبل التدوين	: <i>Al-Sunnah qabl al-tadwīn</i>
العبارات في عموم اللفظ لا بخصوص السبب	: <i>al-'ibārāt fī 'umūm al-lafḡ lā bi khusūṣ al-sabab</i>

9. *Lafḡ al-Jalālah* (الله)

Kata “Allah” yang didahului partikel seperti huruf *jarr* dan huruf lainnya atau berkedudukan sebagai *mudāfilaih* (frasa nominal), ditransliterasikan tanpa huruf hamzah. Contoh:

دِينُ اللَّهِ : *dīnullāh*

Adapun *ta marbūṭah* di akhir kata yang disandarkan pada *lafḡ al-jalālah*, ditransliterasi dengan huruf [t]. Contoh:

هُمْ فِي رَحْمَةِ اللَّهِ : *hum fī raḡmatillāh*

10. Huruf Kapital

Walau sistem tulisan Arab tidak mengenal huruf kapital (*All Caps*), dalam transliterasinya huruf-huruf tersebut dikenai ketentuan tentang

penggunaan huruf kapital berdasarkan pedoman ejaan Bahasa Indonesia yang berlaku atau Ejaah Yang Disempurnakan (EYD). Huruf kapital, misalnya, digunakan untuk menuliskan huruf awal nama diri (orang, tempat, bulan) dan huruf pertama pada permulaan kalimat. Bila nama diri didahului oleh kata sandang (*al-*), maka yang ditulis dengan huruf kapital tetap huruf awal nama diri tersebut, bukan huruf awal kata sandangnya. Jika terletak pada awal kalimat, maka huruf A dari kata sandang tersebut menggunakan huruf kapital (*Al-*). Ketentuan yang sama juga berlaku untuk huruf awal dari judul referensi yang didahului oleh kata sandang (*al-*), baik ketika ia ditulis dalam teks maupun dalam catatan rujukan (CK, DP, CDK, dan DR). Contoh:

Wa mā Muḥammadun illā rasūl

Inna awwala baitin wuḍi‘a linnāsi lallaḏī bi Bakkata mubārakan

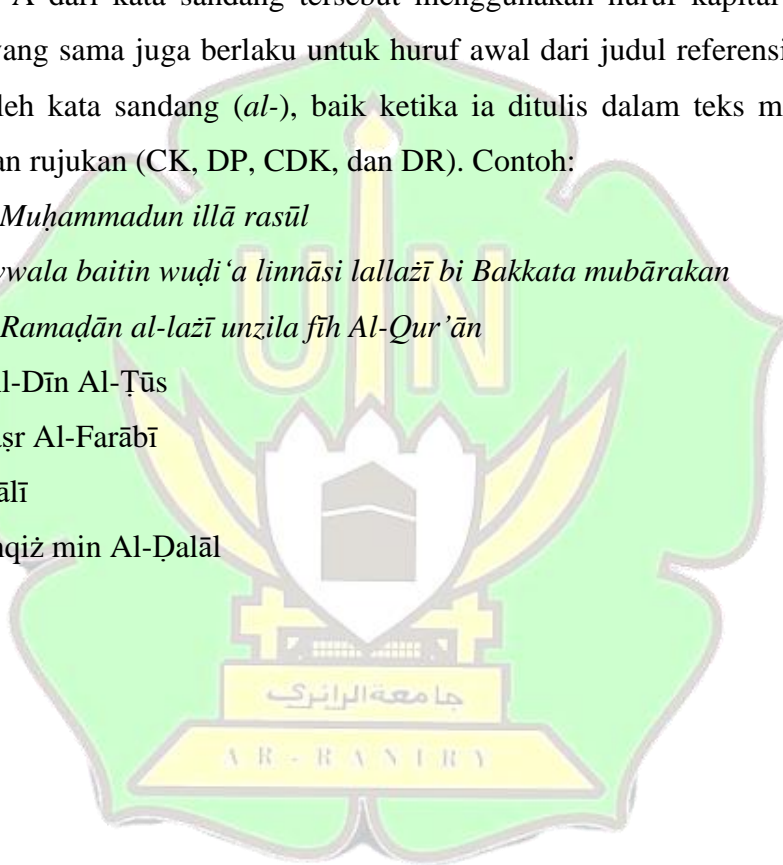
Syahru Ramaḏān al-laḏī unzila fīh Al-Qur‘ān

Naṣīr Al-Dīn Al-Ṭūs

Abū Naṣr Al-Farābī

Al-Gazālī

Al-Munqiz min Al-Ḍalāl



DAFTAR LAMPIRAN

Lampiran 1.1 UU No.11 Tahun 2008	57
Lampiran 1.2 UU No.19 Tahun 2016	67
Lampiran SK Pembimbing.....	77



DAFTAR ISI

LEMBAR JUDUL	i	
LEMBAR PENGESAHAN BIMBINGAN	ii	
LEMBAR PENGESAHAN SIDANG	iii	
PERNYATAAN KEASLIAN KARYA ILMIAH	iv	
ABSTRAK	v	
KATA PENGANTAR	vi	
PEDOMAN TRANSLITERASI	viii	
DAFTAR LAMPIRAN	xv	
DAFTAR ISI	xvi	
BAB SATU	PENDAHULUAN	1
	A. Latar Belakang Masalah.....	1
	B. Rumusan Masalah	7
	C. Tujuan Penelitian	7
	D. Kajian Pustaka.....	8
	E. Penjelasan Istilah.....	11
	F. Metode Penelitian.....	13
	G. Sistematika Pembahasan	15
BAB DUA	LANDASAN TEORI	16
	A. Kartu Kredit	16
	B. Teori Penegakan Hukum.....	19
	C. Ketentuan UU ITE tentang Tindak Pidana Peretasan Kartu Kredit.....	26
	D. Mekanisme Penegakan Hukum Terhadap Peretasan Kartu Kredit.....	29
	E. Perlindungan Hukum Bagi Korban Peretasan Kartu Kredit	33
	F. Peretasan Kartu Kredit Menurut Hukum Islam	35
BAB TIGA	HASIL PENELITIAN	38
	A. Kerangka Hukum Peretasan Kartu Kredit di Indonesia....	38
	B. Analisis Mekanisme Penegakan Hukum Tindak Pidana Peretasan Kartu Kredit dalam UU.....	44

	C. Perlindungan Hukum bagi Korban Berdasarkan Regulasi yang Ada	46
BAB LIMA	PENUTUP	51
	A. Kesimpulan	51
	B. Saran.....	53
	DAFTAR PUSTAKA	54
	DAFTAR RIWAYAT HIDUP.....	78



BAB SATU

PENDAHULUAN

A. Latar Belakang Masalah

Kemajuan teknologi informasi telah mengubah cara hidup dan meningkatkan efisiensi bisnis, namun juga memicu kejahatan siber yang mengancam keamanan. Teknologi berbasis online membawa perubahan sosial signifikan, mendukung kesejahteraan, namun juga menantang hak asasi manusia. Sebagai alat penegakan hukum, teknologi ini memerlukan adaptasi kerangka hukum agar tetap relevan.¹ Teknologi informasi telah menjadi alat yang penting, baik di masa kini maupun di masa depan. Pengertian "*Online*" adalah istilah yang digunakan untuk menggambarkan kondisi atau keadaan ketika perangkat atau sistem terhubung dan dapat berinteraksi dengan jaringan internet atau jaringan lainnya. Ketika seseorang atau suatu perangkat "*online*", Pernyataan tersebut menjelaskan bahwa saat seseorang terhubung secara "*online*," mereka sedang aktif menggunakan internet atau jaringan komputer untuk bertukar data, berkomunikasi, atau mengakses berbagai sumber daya digital. Internet, sebagai bagian penting dari revolusi teknologi informasi, menjadi saluran komunikasi dan informasi yang mempercepat penyebaran pengetahuan serta memfasilitasi berbagai aktivitas manusia.²

Kemajuan teknologi Internet yang pesat telah menyebabkan munculnya apa yang dikenal sebagai "*Cyber crime*" atau kejahatan dunia maya melalui jaringan Internet. Ada beberapa kasus "*cyber crime*" di Indonesia, termasuk peretasan kartu kredit, peretasan situs web, peretasan data dari orang lain (seperti email), dan manipulasi data melalui penggunaan kata sandi yang tidak aman

¹ Bambang Hartono, "Penerapan Sanksi Pidana Terhadap Tindak Pidana Carding," *Jurnal Universitas Bandar Lampung (UBL)*, Vol. 4, No. 1, 2016, hlm. 168.

² Alcianno G. Gani, "Cybercrime (Kejahatan Berbasis Komputer)," *Jurnal Sistem Informasi Universitas Suryadarma*, Vol. 5, No. 1, 2014, hlm. 16.

dalam program komputer. Oleh karena itu, dalam kejahatan komputer, baik delik materiil maupun formil itu dilarang. Delik materiil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain, sedangkan delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin.³

Internet adalah sistem jaringan komputer global yang saling terhubung menggunakan protokol *internet* (TCP/IP) untuk menghubungkan perangkat di komputer di seluruh dunia.⁴ Internet adalah ruang informasi dan komunikasi yang menembus batas-batas yurisdiksi antar negara. Media yang menawarkan berbagai kemudahan transaksional tanpa bertemu para pihak secara fisik atau material. Internet telah membawa kita ke dunia baru yang disebut dunia maya, yang dalam perkembangannya tidak hanya membawa efek positif tetapi juga penuh dengan dampak negatif.

Kejahatan dunia maya menjadi isu sulit ditangani pemerintah, yang berupaya memperkuat penanggulangan dengan teknologi komputer dan jaringan internet. Kemajuan teknologi informasi memiliki dampak positif dan negatif, dengan masyarakat menjadi korban dan pelaku. Maraknya kejahatan siber dipicu oleh penggunaan internet yang cepat berkembang dan masalah privasi online, yang mencerminkan menurunnya kualitas hidup, kondisi sosial, dan meningkatnya kriminalitas.⁵

Kartu kredit adalah alat pembayaran yang memungkinkan transaksi tanpa uang tunai, dikeluarkan oleh lembaga keuangan seperti Bank. Kartu kredit menjadi bagian penting dalam kehidupan modern sebagai pengganti uang tunai untuk pembelian barang dan jasa di merchant yang menerima kartu, didukung

³ Eliasta Ketaren, "Cybercrime, Cyber Space, dan Cyber Law," *Jurnal TIMES*, Vol. V, No. EJA (38), 2016, hlm. 35.

⁴ Fajar Hidayanto dan Mohammad Zidni Ilmi, "Pentingnya Internet Sehat," *Jurnal Inovasi dan Kewirausahaan*, Vol. 4, No. 1, 2015, hlm. 21.

⁵ Hardianto Djanggih dan Nurul Qamar, "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta: Research Law Journal*, Vol. 13, No. 1, 2018, hlm. 12..

oleh kemajuan teknologi *e-commerce*.⁶ Kejahatan siber yang sering terjadi saat ini adalah penipuan kartu kredit (*carding*), di mana pelaku (*carder*) menggunakan data kartu kredit untuk pembayaran. *Carding* dapat dilakukan melalui transaksi offline atau online. Meskipun populer di Indonesia, sistem hukum negara ini masih memiliki celah dan pengawasan yang lemah dalam menangani kasus tersebut. Indonesia tertinggal dalam pengembangan teknologi informasi, khususnya dalam penanggulangan kejahatan siber, terkait dengan regulasi dan aspek lainnya yang berdampak negatif terhadap penerapan hukum.⁷

Carding adalah kejahatan dunia maya yang dilakukan oleh *carder* dengan menggunakan kartu kredit yang dicuri atau dipalsukan untuk membeli produk atau menarik uang secara *illegal*. Transaksi ini dilakukan secara elektronik tanpa sepengetahuan pemilik kartu. *Carder* mendapatkan data nasabah melalui metode seperti *phishing* dan *hacking*, lalu memverifikasi kevalidan dan limit kartu untuk digunakan dalam transaksi. Meskipun mirip dengan pencurian, *carding* berbeda karena melibatkan penggunaan media elektronik yang lebih canggih.⁸ Kejahatan *carding* dapat terjadi di mana saja dan menimpa siapa saja, seperti yang terlihat dalam kasus-kasus *carding* yang sering dibicarakan publik. *Carder* dapat membeli data kartu kredit melalui *Facebook* atau *dark web*, yang sering kali berasal dari kebocoran data perbankan, *marketplace*, atau saat transaksi.

Penelitian terdahulu yang relevan dengan penelitian ini mengungkapkan bahwa terdapat dua upaya dalam menanggulangi kejahatan *carding*. Secara preventif dilakukan oleh pihak kepolisian berupa rekomendasi kepada Bank Indonesia seperti pengawasan, pembatasan terhadap peredaran, dan penerbitan kartu kredit. Adapun secara represif yaitu melakukan mediasi antara pihak bank,

⁶ Alex Yohanes Chandra, "Pertanggung Jawaban Bank Terhadap Nasabah Korban *Carding*," *Jurnal Universitas Sumatera Utara Medan*, 2019, hlm. 1.

⁷ Bambang Hartono, "Penerapan Sanksi Pidana Terhadap Tindak Pidana *Carding*," skripsi, Fakultas Hukum Universitas Bandar Lampung, halm. 169.

⁸ Alif Anas Ramadhan et al., "Tesis Upaya Penanggulangan Kejahatan Pembobolan Kartu Kredit Melalui Internet (Remedies in Combating Criminal Act of *Carding* Through the Internet)," 2022, hlm. 4.

pemegang kartu kredit, dan pelaku *carding*. Namun, apabila mediasi tidak efektif maka diserahkan ke pihak berwajib untuk ditangani seperti kejahatan pada umumnya.⁹

Proses hukum untuk mengatasi *carding* di Indonesia diatur dalam Pasal 27 sampai dengan Pasal 36 Undang-Undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008, yaitu pembuatan kartu kredit melalui berbagai macam cara oleh pengguna, termasuk pembobolan kartu kredit.¹⁰

Contoh kasus yang terjadi di Indonesia dan mengemparkan adalah ketika pada tanggal 18 Juni 2010– Direktorat Reserse Kriminal Khusus menangkap seorang karyawan cafe Starbucks Tebet, Jakarta Selatan, berinisial DDB, 26 tahun yang terbukti telah melakukan pembajakan kartu kredit para pelanggannya. Dengan barang bukti berupa 32 struk pembayaran di kasir Starbucks, di jalan Letjen MT. Haryono No. 9, Jakarta Selatan, lalu 7 kardus Ipod Nano, 1 kardus Ipod Touch dan 18 lembar invoice pengiriman barang. DDB melakukan transaksi lebih dari 50 kali untuk pembelian alat elektronik Ipod Nano dan Ipod Touch yang dilakukan sekitar bulan Maret hingga Juni 2010, Hal tersebut akhirnya terbongkar setelah lebih dari 41 nasabah melaporkan adanya transaksi ilegal pada kartu kreditnya.¹¹

Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa serangan siber di Indonesia meningkat sebesar 38,72%, dari 266,74 juta serangan

⁹ Gede Krisna Ginara, I Made Minggu Widyantara, dan Ni Komang Arini Styawati, “Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia,” *Jurnal Preferensi Hukum*, Vol. 3, No. 1, 2022, hlm. 169.

¹⁰ Siswanto Surnaso, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari* (Jakarta: Rineka Cipta, 2009), hlm. 39.

¹¹ Ryan Shack Syah dan Dahlan Ali, “Kebijakan Pidana Dalam Penanggulangan Tindak Pidana Carding Menurut Ketentuan Undang-Undang Nomor 11 Tahun 2008 Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik,” *JIM Bidang Hukum Pidana*, Vol. 3, No. 4, 2019, hlm. 614.

pada tahun 2021 menjadi 370,02 juta serangan pada tahun 2022.¹² Meskipun data spesifik mengenai jumlah korban peretasan kartu kredit tidak dipublikasikan secara terbuka, peningkatan signifikan dalam jumlah serangan siber ini mengindikasikan bahwa ancaman terhadap keamanan transaksi elektronik, termasuk peretasan kartu kredit, semakin serius. Selain itu, peningkatan jumlah kartu kredit yang beredar di Indonesia dari 12.259.295 pada tahun 2009 menjadi 17.487.057 pada tahun 2019 menunjukkan bahwa semakin banyak individu yang berpotensi menjadi target kejahatan ini.¹³

Penerapan sanksi pidana terhadap pelaku tindak pidana carding menggunakan perangkat hukum yang ada di KUHP, terutama Pasal 378 KUHP, yaitu penipuan karena tindak pidana carding. Berdasarkan fenomena tersebut, penelitian ini dilakukan dengan tujuan untuk memahami kriminalisasi carding dalam hukum di Indonesia, serta tantangan yang ditimbulkan oleh carding.

Sebelum UU ITE, Polri menggunakan prosedur KUHP seperti pemeriksaan dan pengeledahan untuk mengidentifikasi *carder*, namun tantangan muncul karena kejahatan siber bersifat non-fisik. Pasal 31 ayat (1) dan (2) UU ITE mengatur perilaku *carder*, namun meskipun diatur dalam KUHP dan UU ITE, kejahatan *carding* masih terus terjadi.

Carding sendiri dalam kacamata Islam, Al-Quran menegaskan prinsip-prinsip moral dan etika yang mengatur hubungan antarindividu dan masyarakat.¹⁴

Sebagaimana yang termaktub dalam Surah Al-Baqarah (2:188) yang berbunyi:

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

¹² Badan Siber dan Sandi Negara (BSSN), *Beragam Kejahatan Siber di Indonesia Tahun 2022*. Diakses dari: csirt.purwakartakab.go.id.

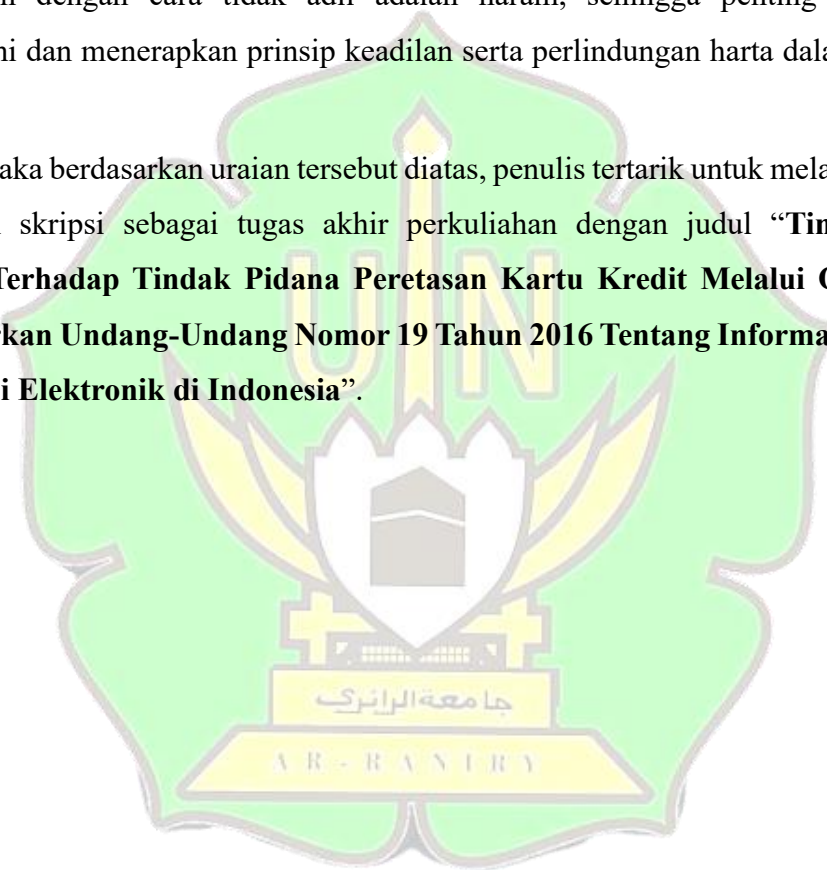
¹³ Analisis Perilaku Konsumen dan Keamanan Kartu Kredit Perbankan, *Jurnal Ekonomi dan Bisnis*. Diakses dari: download.garuda.kemdikbud.go.id.

¹⁴ QS. al-Baqarah [2]: 188.

Dan janganlah sebahagian kamu memakan harta sebahagian yang lain di antara kamu dengan jalan yang bathil dan (janganlah) kamu membawa (urusan) harta itu kepada hakim, supaya kamu dapat memakan sebahagian daripada harta benda orang lain itu dengan (jalan berbuat) dosa, padahal kamu mengetahui. (QS. Al-Baqarah [2] : 188)

Allah melarang umat-Nya saling memakan harta dengan cara batil, termasuk penipuan, pencurian, dan peretasan kartu kredit. Tindakan merugikan orang lain dengan cara tidak adil adalah haram, sehingga penting untuk memahami dan menerapkan prinsip keadilan serta perlindungan harta dalam Al-Quran.

Maka berdasarkan uraian tersebut diatas, penulis tertarik untuk melakukan penelitian skripsi sebagai tugas akhir perkuliahan dengan judul **“Tinjauan Yuridis Terhadap Tindak Pidana Peretasan Kartu Kredit Melalui Online Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik di Indonesia”**.



B. Rumusan Masalah

Mengacu pada pembahasan latar belakang yang telah diuraikan sebelumnya, maka rumusan masalah sebagai berikut :

1. Bagaimana ketentuan UU ITE mengatur tindak pidana peretasan kartu kredit secara online di Indonesia?
2. Bagaimana ketentuan regulasi mengatur mekanisme penegakan hukum terhadap tindak pidana peretasan kartu kredit secara online?
3. Bagaimana ketentuan regulasi mengatur perlindungan hukum bagi korban peretasan kartu kredit secara online?

C. Tujuan Penelitian

Mengacu pada rumusan masalah yang telah diuraikan sebelumnya, maka tujuan penelitian sebagai berikut :

1. Menganalisis kerangka hukum yang mengatur tindak pidana peretasan kartu kredit secara online di Indonesia, khususnya berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE).
2. Mengidentifikasi mekanisme penegakan hukum terhadap tindak pidana peretasan kartu kredit secara online sebagaimana diatur dalam regulasi yang ada.
3. Mengkaji perlindungan hukum yang diatur dalam regulasi bagi korban tindak pidana peretasan kartu kredit secara online di Indonesia.

D. Kajian Pustaka

Berikut beberapa penelitian sebelumnya yang penulis temukan dan berkaitan dengan penelitian ini.

1. Djanggih, Hardianto, and Nurul Qamar dengan judul “Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (*Cyber Crime*)”. jurnal ini membahas masalah penanggulangan kejahatan siber melalui pendekatan teori-teori kriminologi. Hal tersebut penting untuk memahami kejahatan siber dari segi karakteristik kejahatan dan penjahat. Metode penelitian yang digunakan yakni metode penelitian yang bersifat yuridis-empiris. Hasil penelitian menunjukkan bahwa terdapat empat teori yang dapat digunakan menganalisis kejahatan siber yaitu anomie, asosiasi diferensial, kontrol sosial, dan netralisasi. Teori tersebut dapat digunakan sebagai strategi pencegahan dan penindakan kejahatan siber sebagai kejahatan yang dihasilkan melalui interaksi anggota masyarakat memerlukan penanganan serius baik oleh masyarakat, penegak hukum dan perumusan perundang-undangan. Agar kebijakan memerangi kejahatan siber tepat guna dan berhasil guna, maka para pihak perlu memperhatikan hasil kajian dari perspektif kriminologi.¹⁵
2. Hartono, Bambang. dengan judul “Penerapan Sanksi Pidana Terhadap Tindak Pidana *Carding*” Jurnal ini membahas akibat dari perkembangan teknologi informatika berbasis internet, dengan sendirinya teknologi informatika juga telah mengubah perilaku masyarakat dan peradaban manusia secara global. Teknologi informatika menyebabkan perubahan sosial secara signifikan yang berlangsung dengan cepat. Teknologi informatika saat ini telah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan

¹⁵ Hardianto Djanggih dan Nurul Qamar, “Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (*Cyber Crime*),” *Jurnal Kriminologi Indonesia*, Vol. 7, No. 1, 2019, hlm. 23–34.

peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum, dengan kata lain terjadinya perbuatan-perbuatan melawan hukum tersebut maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut.¹⁶

3. Syah, Ryan Shack, and Dahlan Ali. dengan judul “Kebijakan Pidana Dalam Penanggulangan Tindak Pidana Carding Menurut Ketentuan Undang-Undang Nomor 11 Tahun 2008 Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik.” Jurnal ini membahas Perkembangan teknologi dan internet dewasa ini tidak selalu memberikan efek positif namun juga terdapat hal-hal negatif yang menyebabkan munculnya jenis kejahatan baru, yaitu kejahatan carding (pencurian data kartu kredit) yang merupakan salah satu jenis *cyber crime*. Seorang Carder dapat masuk ke sebuah server tanpa izin untuk mendapatkan dana yang tidak sah dari akun kartu kredit milik orang lain. Permasalahan yang muncul adalah faktor yang dapat menyebabkan seseorang menyalahgunakan komputer untuk melakukan kejahatan carding serta bagaimana kebijakan pidana dalam penanggulangan kejahatan carding, karena pada dasarnya peraturan perundang-undangan Indonesia belum mampu mengatasi persoalan tersebut.¹⁷
4. Ginara, I Gede Krisna, I Made Minggu Widyantara, and Ni Komang Arini Styawati dengan judul “Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia.” Jurnal ini membahas Kriminalisasi merupakan suatu tindakan yang awalnya bukan

¹⁶ Bambang Hartono, “Penerapan Sanksi Pidana Terhadap Tindak Pidana Carding,” *Jurnal Universitas Bandar Lampung (UBL)*, Vol. 4, No. 1, 2016, hlm. 168.

¹⁷ Ryan Shack Syah dan Dahlan Ali, “Kebijakan Pidana Dalam Penanggulangan Tindak Pidana Carding Menurut Ketentuan Undang-Undang Nomor 11 Tahun 2008 Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik,” *JIM Bidang Hukum Pidana*, Vol. 3, No. 4, 2019, hlm. 614.

dianggap sebuah peristiwa pidana, lalu digolongkan menjadi sebuah peristiwa pidana bagi masyarakat. Pada era globalisasi seperti sekarang banyak sekali kejahatan jagat maya yang timbul di Indonesia, merupakan perbuatan ilegal yang dilakukan oleh pelaku kejahatan dengan memanfaatkan teknologi dan sistem informasi jaringan komputer. Salah satu yang terjadi di Indonesia dan tergolong awam di masyarakat yaitu kejahatan carding yang berupa perbuatan jahat dalam memakai teknologi internet menjadi alat dalam membuka dengan cara ilegal sebuah sistem pada website untuk memperoleh informasi kartu kredit dimiliki nasabah. Tujuan journal ini yaitu untuk mengungkap kriminalisasi terhadap kejahatan carding dalam hukum pidana Indonesia serta upaya penanggulangan terhadap kejahatan carding.¹⁸

5. Eliasta Ketaren dengan judul “*Cybercrime, Cyber Space, Dan Cyber Law.*” Jurnal ini membahas Pemanfaatan dalam bidang teknologi Informasi, media, dan komunikasi telah membuat perilaku seseorang menjadi lebih baik dalam berperilaku dalam sebuah masyarakat. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tidak terhalang dengan batas dan norma yang ada sehingga dapat menimbulkan suatu perubahan dalam seluruh bidang missal bidang sosial, ekonomi, dan budaya secara cepat dan luas. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi factor penting dalam perbuatan melawan hukum.¹⁹

¹⁸ Gede Krisna Ginara, I Made Minggu Widyantara, dan Ni Komang Arini Styawati, “Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia,” *Jurnal Preferensi Hukum*, Vol. 3, No. 1, 2022, hlm. 169.

¹⁹ Eliasta Ketaren, “Cybercrime, Cyber Space, Dan Cyber Law,” *Jurnal TIMES*, Vol. 5, No. EJA, 2016, hlm. 35.

E. Penjelasan Istilah

Berikut ini adalah frase-frase yang membentuk judul penelitian "Tinjauan Yuridis terhadap Tindak Pidana Peretasan Kartu Kredit melalui Internet berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia," yang telah penulis format, yaitu sebagai berikut:

1. *Cyber crime*

Kejahatan Siber atau *cybercrime* adalah pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif criminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung.²⁰

2. *Carding*

Carding, yaitu peretasan nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet.²¹ Data kartu kredit biasanya diperoleh melalui peretasan, atau pembelian di pasar gelap. Dalam hukum Indonesia, carding diatur dalam *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)*, khususnya Pasal 30 tentang akses ilegal dan Pasal 32 tentang manipulasi data elektronik.

3. Internet

Internet adalah sistem jaringan komputer global yang saling terhubung menggunakan protokol internet (TCP/IP) untuk menghubungkan perangkat di komputer di seluruh dunia.²²

²⁰ Debarati Halder dan K. Jaishankar, *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations* (Hershey, PA, USA: IGI Global, 2012), ISBN 978-1-60960-830-9.

²¹ Eliasta Ketaren, "Cybercrime, Cyber Space, Dan Cyber Law," *Jurnal TIMES*, Vol. 5, No. EJA, 2016, hlm. 37.

²² Fajar Hidayanto dan Mohammad Zidni Ilmi, "Pentingnya Internet Sehat," *Jurnal Inovasi dan Kewirausahaan*, Vol. 4, No. 1, 2015, hlm. 21.

4. Serangan Siber

Serangan siber adalah serangan yang dilakukan oleh network komputer atau telekomunikasi terhadap network komputer atau telekomunikasi yang lain seperti website, sistem komputer, dan komputer individu. Serangan siber merupakan sebuah usaha sistematis operasional yang dilakukan oleh perseorangan dan organisasi yang melakukan penyerangan dengan maksud-maksud tertentu misalnya untuk meretas, merusak dan menghancurkan target spesifik dengan cara masuk kedalam sistem atau network komputer.²³

5. Pemegang Kartu Kredit (*Cardholder*)

Pemegang Kartu Kredit (*Cardholder*) Merupakan individu atau entitas yang menggunakan kartu kredit untuk melakukan transaksi jual beli barang atau jasa. Dalam konteks carding, pemegang kartu kredit menjadi korban karena informasi kartunya digunakan secara ilegal oleh pihak lain.²⁴

²³ Diny Luthfah, “Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata Dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law),” *Jurnal Keamanan Nasional*, Vol. 3, 2021, hlm. 12.

²⁴ Della Rahmi Pratiwi, “Legal Standing,” *Jurnal Hukum*, Vol. 4, No. 2, 2020, hlm. 206–223.

F. Metode Penelitian

Dalam penelitian ini peneliti menggunakan metode penelitian:

1. Jenis Penelitian

Dalam penelitian ini, penulis menggunakan jenis penelitian hukum normatif, yaitu penelitian studi pustaka atau studi dokumen, karena penelitian ini berpusat pada bahan pustaka atau bahan-bahan hukum lainnya serta bahan non-hukum.

2. Sifat Penelitians

Penelitian hukum ini bersifat preskriptif, yang menyatakan penelitian hukum dilakukan untuk menghasilkan argumentasi sebagai konsep baru dalam menyelesaikan bentuk isu hukum yang dihadapi. Dalam penelitian diharapkan dapat menghasilkan argumentasi untuk memberikan preskriptif baru mengenai pertanggungjawaban tindak pidana Peretasan Kartu Kredit Melalui Internet Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (UU ITE) Di Indonesia.

3. Pendekatan Penelitian

Penelitian ini berfokus pada pendekatan undang-undang (*statue approach*) dan pendekatan konseptual (*conseptual approach*). Dengan dasar ini peneliti mengkaji isu hukum untuk mencari pemecahan terhadap Tinjauan Yuridis Terhadap Ketentuan Hukum Tindak Pidana Peretasan Kartu Kredit Melalui Internet Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia

4. Sumber Data

Sumber data yang digunakan pada penelitian ini, berupa :

- a. Bahan Hukum Primer : Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- b. Bahan Hukum Sekunder : Buku yang ditulis oleh para ahli hukum, jurnal yang terkait dengan penelitian ini yang sedang ditulis dan contoh kasus kejahatan Peretasan Kartu Kredit Melalui Internet.

5. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah teknik studi kepustakaan atau studi dokumen (library research). Dengan cara mengkaji, mempelajari, dan memberi catatan terhadap buku-buku, peraturan perundang-undangan, dokumen, laporan, arsip, dan hasil penelitian lain.

6. Teknik Analisis Data

Teknik analisis data dalam penelitian ini menggunakan metode berpikir deduktif. Dalam metode ini, analisis dilakukan dengan dua premis, yaitu premis mayor yang merupakan aturan hukum yang berlaku, dan premis minor yang berisi fakta hukum terkait aturan tersebut. Dari kedua premis ini, kemudian ditarik sebuah kesimpulan yang relevan untuk menganalisis isu hukum yang ada.

G. Sistematika Pembahasan

Agar proposal ini lebih tepat sasaran, maka sistematika pembahasan proposal terdiri dari 4 (empat) bab, yaitu :

BAB SATU PENDAHULUAN

Pada bab pertama ini meliputi latar belakang masalah kemudian dilanjutkan rumusan masalah, tujuan penelitian, kajian pustaka, penjelasan istilah, metode penelitian, dan sistematika pembahasan.

BAB DUA LANDASAN TEORI

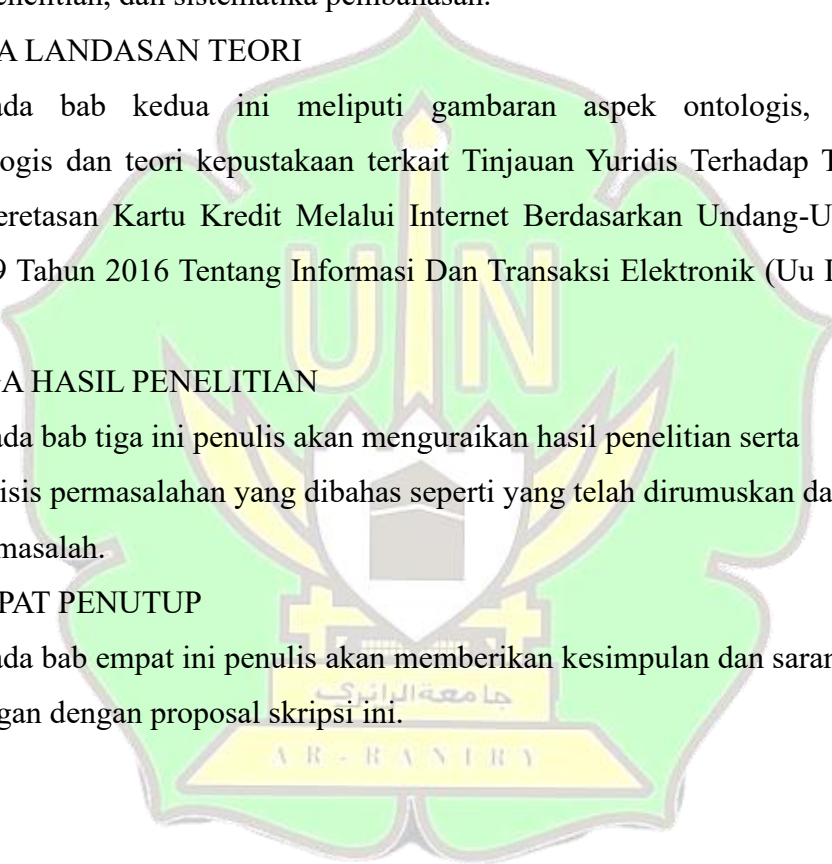
Pada bab kedua ini meliputi gambaran aspek ontologis, aspek epistemologis dan teori kepustakaan terkait Tinjauan Yuridis Terhadap Tindak Pidana Peretasan Kartu Kredit Melalui Internet Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Uu Ite) Di Indonesia

BAB TIGA HASIL PENELITIAN

Pada bab tiga ini penulis akan menguraikan hasil penelitian serta menganalisis permasalahan yang dibahas seperti yang telah dirumuskan dalam rumusan masalah.

BAB EMPAT PENUTUP

Pada bab empat ini penulis akan memberikan kesimpulan dan saran yang berhubungan dengan proposal skripsi ini.



BAB DUA

LANDASAN TEORI

A. Kartu Kredit

Secara terminologi, kamus *Oxford* mendefinisikan kartu kredit sebagai kartu yang dikeluarkan oleh pihak bank dan sejenisnya yang dapat digunakan oleh pembawanya untuk membeli segala keperluan dan barang-barang serta pelayanan tertentu secara kredit.²⁵ Penggunaan kartu kredit di era digital ini semakin luas, dan bersamaan dengan itu muncul juga ancaman yang terkait dengan penyalahgunaan data, seperti tindak pidana peretasan. Kartu kredit pertama kali digunakan di Amerika Serikat pada tahun 1920-an oleh department store besar untuk memudahkan pelanggan berbelanja dengan pembayaran bulanan. Pada 1950-an, bank-bank di AS mulai menerbitkan kartu kredit lokal bagi nasabah untuk memberikan jalur kredit tanpa jaminan. Di Indonesia, kartu kredit diatur dalam Undang-Undang Nomor 7 Tahun 1972, sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, sebagai salah satu alat pembayaran nontunai.²⁶

Kartu kredit terbuat dari plastik dengan ukuran standar, dilengkapi dengan data nomor kartu yang terekam pada magnetic stripe di bagian belakang. Bagian depan kartu memuat nama, nomor pemegang kartu (biasanya terdiri dari 12-16 digit), dan tanggal kedaluwarsa. Kartu kredit diatur oleh Undang-Undang Perbankan di Indonesia, karena bank merupakan penerbit utama kartu ini.²⁷ Pengertian bank berdasarkan Pasal 1 angka 2 Undang-Undang Nomor 7 Tahun 1992 sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998

²⁵Oxford English Dictionary (OED) Online, "Definition of Credit Card," diakses melalui <https://www.oed.com>, tanggal 4 Desember 2024.

²⁶ Republik Indonesia, Undang-Undang Nomor 7 Tahun 1972 sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Lembaran Negara Tahun 1972 No. 50, Tambahan Lembaran Negara No. 2992.

²⁷ Bank Indonesia, Peraturan Bank Indonesia Nomor 11/11/PBI/2009 tentang Alat Pembayaran dengan Menggunakan Kartu (APMK), Lembaran Negara Republik Indonesia Tahun 2009 No. 11.

tentang Perbankan, bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak.²⁸ Sedangkan pengertian kartu kredit dapat dijelaskan sebagai berikut:

- 1) Peraturan Bank Indonesia Nomor 11/11/PBI/2009 Menurut Peraturan Bank Indonesia Nomor 11/11/PBI/2009, kartu kredit adalah Alat Pembayaran dengan Menggunakan Kartu (APMK) yang dapat digunakan untuk melakukan pembayaran atas kewajiban yang timbul dari suatu kegiatan ekonomi, termasuk transaksi pembelian dan/atau untuk melakukan penarikan tunai, dimana kewajiban pembayaran pemegang kartu dipenuhi terlebih dahulu oleh acquirer atau penerbit, dan pemegang kartu berkewajiban untuk melakukan pembayaran pada waktu yang disepakati baik dengan pelunasan secara sekaligus (charge card) ataupun dengan pembayaran secara angsuran.²⁹
- 2) Undang-undang Nomor 7 Tahun 1972 sebagaimana telah diubah dengan Undang-undang Nomor 10 Tahun 1998 tentang Perbankan. Menurut Undang-undang Nomor 7 Tahun 1972 sebagaimana telah diubah dengan Undang-undang Nomor 10 Tahun 1998 tentang Perbankan, kartu kredit merupakan salah satu alat pembayaran terbaru setelah giro dan giro non tunai. Kartu kredit terbuat dari plastik dengan ukuran standar tertentu dan berisi data nomor kartu yang direkam pada garis magnet di bagian belakang kartu. Di bagian depan kartu adalah nama dan nomor pemegang kartu, tercetak dan tercetak, serta tanggal kedaluwarsa kartu. Nomor pemegang

²⁸ Republik Indonesia, Undang-Undang Nomor 7 Tahun 1972 tentang Perbankan, sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998, Lembaran Negara Republik Indonesia Tahun 1972 No. 7, Tambahan Lembaran Negara No. 2946.

²⁹ Bank Indonesia, Peraturan Bank Indonesia Nomor 11/11/PBI/2009 tentang Alat Pembayaran Menggunakan Kartu (APMK), Lembaran Negara Republik Indonesia Tahun 2009 No. 11.

kartu biasanya terdiri dari 12-16 digit dan unik untuk setiap bank dan pemegang kartu.

- 3) Bunga Ayu Lestari, Budi Suharjo, dan Istiqlaliyah Muflikhat (2016, 144). Menurut Bunga Ayu Lestari, Budi Suharjo, dan Istiqlaliyah Muflikhat (2016, 144), kartu kredit adalah kartu yang diterbitkan oleh bank tertentu kepada pengguna sebagai alat pembayaran dengan menggunakan kartu tersebut. Kartu kredit menawarkan dua fungsi yang berbeda kepada konsumen, yaitu sebagai alat pembayaran dan sumber kredit, memungkinkan pengguna untuk membeli barang dan jasa dari perusahaan yang menerima kartu tanpa membayar tunai. Menurut Peter Salam dalam bukunya yang berjudul "*The Contemporaray English-Indonesia Dictionary*" (1986, 438), kartu kredit adalah kartu yang dikeluarkan oleh bank atau lembaga keuangan bagi langganan-langganannya untuk membeli barang dan jasa dari perusahaan yang menerima kartu tersebut tanpa pembayaran tunai.³⁰

Dalam konteks peretasan yang menjadi fokus utama skripsi ini, kelemahan sistem kartu kredit dan infrastruktur digital yang mendukungnya sering menjadi target para peretas. Peretasan kartu kredit merupakan salah satu bentuk kejahatan siber yang dapat dilakukan melalui berbagai metode, seperti phishing, malware, atau peretasan data melalui jaringan yang tidak aman. Oleh karena itu, UU ITE (Undang-Undang Nomor 19 Tahun 2016) memainkan peran penting dalam memberikan dasar hukum untuk melindungi korban dan menindak pelaku kejahatan siber, termasuk peretasan kartu kredit. Perlindungan hukum ini menjadi sangat krusial karena selain aspek perbankan, aspek siber juga menjadi tantangan besar di era digital.

³⁰ Bunga Ayu Lestari, Budi Suharjo, dan Istiqlaliyah Muflikhat, "Penggunaan Kartu Kredit dalam Era Digital," dalam *Hukum Perbankan Indonesia*, (Jakarta: Sinar Grafika, 2016), hlm. 144.

B. Teori Penegakan Hukum

Penegakan hukum merupakan proses yang mencakup penerapan aturan-aturan hukum oleh institusi-institusi yang berwenang dengan tujuan untuk menjaga ketertiban dan keadilan dalam masyarakat. Dalam konteks tindak pidana peretasan kartu kredit melalui internet, penegakan hukum menjadi sangat penting karena kejahatan siber sering kali memiliki dampak yang luas dan sulit untuk dideteksi dan ditindak secara efektif. Oleh karena itu, pemahaman tentang teori penegakan hukum sangat diperlukan untuk melihat bagaimana hukum diterapkan dalam konteks siber.

1. Teori Penegakan Hukum Menurut Soerjono Soekanto

Soerjono Soekanto mendefinisikan penegakan hukum sebagai kegiatan yang bertujuan untuk mewujudkan ketentuan-ketentuan hukum dalam kenyataan. Menurutnya, penegakan hukum tidak hanya melibatkan aparat penegak hukum (seperti polisi, jaksa, dan hakim), tetapi juga melibatkan seluruh komponen masyarakat yang mematuhi hukum. Penegakan hukum yang efektif memerlukan sinergi antara masyarakat yang sadar hukum dan aparat penegak hukum yang bekerja dengan integritas dan kompetensi.³¹

Dalam konteks tindak pidana peretasan kartu kredit, teori Soekanto ini relevan karena penegakan hukum siber membutuhkan kolaborasi yang erat antara aparat penegak hukum, penyedia layanan internet, lembaga keuangan, dan pengguna internet itu sendiri. Tanpa kerjasama ini, upaya penegakan hukum akan mengalami banyak hambatan.

Soerjono Soekanto mengidentifikasi lima faktor utama yang mempengaruhi efektivitas penegakan hukum, yang juga dapat diterapkan dalam konteks penanganan peretasan kartu kredit. Faktor efektivitasnya sebagai berikut:

³¹ Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum* (Jakarta: Rajawali Pers, 2004), hlm. 5.

a) Faktor hukum itu sendiri (undang-undang)

Hukum yang berlaku harus memberikan keadilan, kepastian, dan kemanfaatan dalam masyarakat. Dalam konteks kejahatan siber, hukum yang diterapkan sering kali harus mengikuti perkembangan teknologi. Misalnya, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi dasar hukum dalam menangani kasus-kasus siber, termasuk peretasan kartu kredit. Namun, masih ada tantangan dalam penerapannya, seperti celah hukum atau perbedaan penafsiran dalam berbagai kasus siber.

b) Faktor penegak hukum

Penegakan hukum siber memerlukan aparat penegak hukum yang kompeten dan berintegritas. Hal ini meliputi kemampuan teknis dalam memahami aspek-aspek digital serta pemahaman hukum yang menyeluruh tentang tindak pidana siber. Koordinasi antar lembaga seperti polisi siber, kejaksaan, dan lembaga peradilan sangat penting agar proses hukum berjalan efektif dan menghasilkan kepastian hukum.

c) Faktor sarana atau fasilitas yang mendukung penegak hukum

Sarana dan prasarana yang mendukung penegakan hukum, seperti teknologi informasi, perangkat investigasi digital, serta infrastruktur keamanan siber, sangat penting dalam menangani kejahatan peretasan kartu kredit. Apabila sarana tersebut tidak memadai, upaya penegakan hukum akan terhambat dan kejahatan siber akan sulit diungkap.

d) Faktor masyarakat

Masyarakat yang memiliki kesadaran hukum dan pemahaman mengenai risiko keamanan siber sangat berperan dalam mencegah peretasan. Misalnya, masyarakat diharapkan lebih berhati-hati dalam penggunaan kartu kredit di internet dan memahami pentingnya menjaga keamanan data pribadi.

e) Faktor kebudayaan

Kebiasaan atau budaya masyarakat dalam memandang teknologi dan keamanan siber juga turut mempengaruhi efektivitas penegakan hukum. Di Indonesia, budaya keterbukaan terhadap informasi digital dan pemahaman keamanan siber masih perlu ditingkatkan untuk membantu pencegahan peretasan kartu kredit.

Secara keseluruhan, teori penegakan hukum Soerjono Soekanto sangat relevan dalam konteks kejahatan peretasan kartu kredit. Selain hukum yang jelas, penegakan hukum memerlukan dukungan dari berbagai elemen masyarakat, institusi, dan teknologi. UU ITE menjadi instrumen utama dalam menindak kejahatan siber di Indonesia, tetapi penerapannya harus didukung oleh aparat penegak hukum yang memiliki keahlian teknis serta infrastruktur yang memadai agar hukum dapat ditegakkan secara efektif.

2. Teori Kepatuhan Hukum

Teori kepatuhan hukum menekankan pentingnya kesadaran hukum di masyarakat sebagai prasyarat utama bagi penegakan hukum yang efektif. Kepatuhan terhadap hukum tidak hanya didorong oleh ancaman sanksi hukum, tetapi juga melalui internalisasi nilai-nilai hukum dalam masyarakat. Soerjono Soekanto menekankan bahwa kepatuhan hukum dapat terjadi apabila masyarakat secara sadar menerima dan menghormati hukum sebagai bagian dari kehidupan sosialnya, bukan semata-mata karena takut akan hukuman.³²

Di era digital, kepatuhan terhadap hukum siber menjadi krusial dalam konteks peretasan kartu kredit. Semua pihak yang terlibat pengguna kartu kredit, penyedia layanan internet, bank, dan penegak hokum harus mematuhi

³² Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum* (Jakarta: Rajawali Pers, 2004), hlm. 13.

regulasi dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) untuk menangani kejahatan digital. Kepatuhan terhadap UU ITE dan aturan perbankan sangat mempengaruhi efektivitas penegakan hukum dalam kasus peretasan kartu kredit. Kurangnya kesadaran hukum dari pengguna, penyedia layanan, atau bank dapat menghambat penanganan kasus ini, misalnya melalui penggunaan perangkat lunak yang tidak aman atau ketidakpatuhan dalam menjaga keamanan data transaksi.

Penyedia layanan internet dan bank harus mematuhi regulasi keamanan data yang ketat untuk mengurangi risiko peretasan. Internalisasi nilai-nilai hukum dalam sistem digital penting untuk menciptakan lingkungan yang aman dari kejahatan siber. Tanpa kepatuhan tinggi, penegakan hukum akan terhambat dan memberi ruang bagi pelaku kejahatan.

Kepatuhan terhadap hukum dalam kejahatan siber memerlukan regulasi yang jelas serta edukasi dan kesadaran masyarakat. Pengguna kartu kredit harus melindungi data pribadi dan menggunakan sistem transaksi yang aman, sedangkan bank dan penyedia layanan harus terus meningkatkan keamanan mereka. Teori kepatuhan hukum menjadi relevan dalam mengatasi peretasan kartu kredit dan menjaga kepercayaan publik terhadap sistem perbankan digital.

3. Teori Penegakan Hukum Progresif

Teori penegakan hukum progresif diperkenalkan oleh Satjipto Rahardjo pertama kali dalam artikelnya yang dimuat harian Kompas 15 Juni 2002 dengan judul "Indonesia Butuhkan Penegakan Hukum Progresif".³³ Dalam teori ini, Rahardjo mengkritisi kondisi hukum di Indonesia yang menurutnya tidak berorientasi pada kesejahteraan dan kebahagiaan masyarakat. Rahardjo menilai bahwa hukum sering kali stagnan dan tidak mencerminkan keadilan

³³ M. Zulfa Aulia, "Hukum Progresif Dari Satjipto Rahardjo," *Undang: Jurnal Hukum*, Vol. 1, No. 1, 2018, hlm. 164.

sosial yang sesungguhnya. Penegakan hukum yang kaku dan tidak adaptif terhadap perubahan sosial menjadi salah satu penyebab lemahnya sistem hukum di Indonesia, terutama dalam menghadapi tantangan baru, seperti kejahatan siber.³⁴

Dalam konteks tindak pidana peretasan kartu kredit melalui internet, teori ini sangat relevan. Satjipto Rahardjo berpendapat bahwa penegakan hukum harus bersifat fleksibel dan adaptif terhadap perkembangan sosial dan teknologi. Penegakan hukum yang progresif menuntut agar Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tidak hanya diterapkan secara kaku, tetapi juga dinamis, sehingga mampu menyesuaikan diri dengan perkembangan modus operasi peretasan kartu kredit yang semakin canggih dan sulit diatasi hanya dengan pendekatan konvensional.

Penegakan hukum progresif mengharuskan aparat, seperti polisi, jaksa, dan hakim, untuk meningkatkan kemampuan dalam teknologi informasi dan *cyber forensics* guna menghadapi kejahatan siber yang semakin rumit dan sering melibatkan jaringan internasional. Selain itu, penegakan hukum progresif membutuhkan kerjasama antara pemerintah, lembaga keuangan, dan penyedia layanan internet untuk menciptakan keamanan siber yang terpadu

Dalam kasus peretasan kartu kredit, pendekatan ini tidak hanya fokus pada pemberian sanksi, tetapi juga pada pemulihan hak korban, pencegahan kejahatan di masa depan, serta penyesuaian hukum dengan perkembangan teknologi. UU ITE dan peraturan terkait perlu diperbarui agar relevan dengan tantangan baru, menjaga keseimbangan antara perlindungan masyarakat dan hak individu di era digital.³⁵

³⁴ Satjipto Rahardjo, *Hukum Progresif: Sebuah Sintesa Hukum Indonesia* (Yogyakarta: Genta Publishing, 2009), hlm. 15-16.

³⁵ Eko Haryanto, "Penegakan Hukum Siber di Indonesia," *Jurnal Hukum & Teknologi* Vol. 5, No. 1 (2020): hlm. 89-91.

4. Teori Hukum Responsif

Teori hukum responsif, yang dikembangkan oleh Philippe Nonet dan Philip Selznick, menekankan bahwa hukum harus merespons kebutuhan dan aspirasi masyarakat. Hukum yang responsif tidak hanya berfungsi untuk mengontrol, tetapi juga untuk memfasilitasi kehidupan sosial. Dalam konteks penegakan hukum terhadap peretasan kartu kredit, teori ini menekankan pentingnya hukum yang dapat merespons ancaman baru di dunia siber dan memberikan perlindungan yang memadai bagi korban.³⁶

Penerapan teori hukum responsif terhadap UU ITE dalam kasus kejahatan siber berarti bahwa regulasi harus selalu diperbarui dan disesuaikan dengan perkembangan teknologi dan modus operandi kejahatan yang terus berubah. Hukum harus mampu memberikan perlindungan yang efektif bagi korban peretasan, serta mendorong kolaborasi antar berbagai pihak, termasuk pemerintah, lembaga keuangan, dan penyedia layanan internet, dalam membangun ekosistem keamanan digital yang kuat. Pendekatan ini penting untuk memastikan bahwa penegakan hukum selalu relevan dan mampu merespons kejahatan di era digital dengan cepat dan tepat.³⁷

5. Peran Otoritas Jasa Keuangan dalam Penegakan Hukum Siber

Otoritas Jasa Keuangan (OJK) memiliki peran penting dalam penegakan hukum di sektor keuangan, terutama dalam melindungi konsumen dan mengawasi keamanan transaksi elektronik. Berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, OJK bertanggung jawab untuk mengatur dan mengawasi kegiatan jasa keuangan di Indonesia,

³⁶ Philippe Nonet & Philip Selznick, *Law and Society in Transition: Toward Responsive Law* (Harper & Row: 2001), hlm. 14.

³⁷ Satjipto Rahardjo, *Hukum Progresif: Sebuah Sintesa Hukum di Tengah Kehidupan Masyarakat Modern* (Yogyakarta: Genta Publishing, 2012), hlm. 31.

termasuk perbankan, pasar modal, dan sektor jasa keuangan lainnya.³⁸ Dalam konteks kejahatan siber seperti peretasan kartu kredit, peran OJK menjadi sangat relevan dalam melindungi data nasabah dan mendorong penerapan standar keamanan yang ketat oleh lembaga keuangan.

OJK menetapkan aturan dan pedoman yang harus diikuti oleh bank dan institusi keuangan lainnya untuk menjaga kerahasiaan dan keamanan data konsumen. Salah satu regulasi penting adalah Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yang mencakup kewajiban lembaga keuangan untuk menerapkan tindakan pengamanan data dan memberikan informasi yang jelas kepada konsumen mengenai risiko yang mungkin terjadi dalam transaksi elektronik.³⁹

Selain itu, OJK bekerja sama dengan Bank Indonesia dalam mengawasi penerapan manajemen risiko di sektor keuangan, yang bertujuan untuk meminimalkan kemungkinan terjadinya kejahatan siber, termasuk peretasan data kartu kredit. Pengawasan ini mencakup audit sistem keamanan dan penilaian kepatuhan terhadap standar keamanan data, sehingga memungkinkan lembaga keuangan untuk mengidentifikasi dan menutup celah keamanan sebelum terjadi pelanggaran.⁴⁰

Secara keseluruhan, OJK tidak hanya berfungsi sebagai pengawas regulasi, tetapi juga sebagai pelaksana teori penegakan hukum yang berupaya menjaga stabilitas sektor keuangan dan memastikan bahwa konsumen terlindungi dari potensi kerugian akibat kejahatan siber, seperti peretasan kartu kredit. Dalam kasus kejahatan yang terjadi lintas batas, OJK turut berperan

³⁸ Republik Indonesia, Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Jakarta: Lembaran Negara Republik Indonesia, 2011).

³⁹ Otoritas Jasa Keuangan, Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan (Jakarta: Otoritas Jasa Keuangan, 2013).

⁴⁰ Bank Indonesia, Peraturan Bank Indonesia No. 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran (Jakarta: Bank Indonesia, 2016).

dalam membangun kerja sama internasional dengan otoritas jasa keuangan negara lain, guna mendukung penegakan hukum yang efektif di era digital.

C. Ketentuan UU ITE tentang Tindak Pidana Peretasan Kartu Kredit

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan regulasi utama yang mengatur tentang kejahatan siber di Indonesia, termasuk tindak pidana peretasan kartu kredit. Peretasan kartu kredit melalui internet merupakan salah satu bentuk kejahatan siber yang kian marak seiring dengan perkembangan teknologi dan penggunaan transaksi elektronik.

UU ITE menyediakan landasan hukum untuk menindak pelaku kejahatan ini, serta memberikan perlindungan kepada korban. Ketentuan hukum dalam UU ITE telah dipraktikkan di lapangan oleh aparat penegak hukum, seperti dalam penyelesaian kasus-kasus kejahatan siber, termasuk kasus peretasan kartu kredit. Sebagai contoh, Kepolisian Republik Indonesia melalui Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri secara aktif menggunakan UU ITE untuk menyelidiki dan menangani kasus-kasus peretasan kartu kredit. Beberapa kasus konkret menunjukkan implementasi UU ITE, misalnya penangkapan sindikat internasional peretasan kartu kredit yang diungkap pada tahun 2020 dengan kerugian miliaran rupiah.⁴¹

Dengan implementasi ini, UU ITE menjadi alat penting dalam memerangi kejahatan siber, meskipun masih terdapat tantangan dalam pelaksanaannya, seperti keterbatasan teknologi forensik digital dan perlunya peningkatan kapasitas aparat penegak hukum.⁴²

⁴¹ Laporan Kepolisian Republik Indonesia, *Kasus Sindikat Peretasan Kartu Kredit Internasional 2020* (Jakarta: Dittipidsiber Bareskrim Polri, 2020), hlm. 45.

⁴² Romli Atmasasmita, *Cybercrime: Problematika dan Solusi* (Jakarta: Sinar Grafika, 2017), hlm. 104.

1. Definisi dan Lingkup Tindak Pidana Peretasan

Menurut UU ITE, tindak pidana peretasan atau akses ilegal diatur dalam Pasal 30. Pasal ini menjelaskan bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun, merupakan tindakan yang melanggar hukum.⁴³

Peretasan kartu kredit termasuk dalam kategori ini karena pelaku secara ilegal mengakses informasi kartu kredit, baik dengan tujuan meretas data, menggunakannya untuk transaksi tanpa izin, atau menjual informasi tersebut kepada pihak lain. Lingkup tindak pidana ini meliputi akses ke sistem elektronik perbankan, *e-commerce*, atau sistem lainnya yang menyimpan data kartu kredit.

2. Ketentuan Pidana Terkait Peretasan Kartu Kredit

UU ITE secara spesifik mengatur sanksi pidana bagi pelaku peretasan dalam Pasal 46, yang merupakan kelanjutan dari Pasal 30. Pasal 46 UU ITE menyebutkan bahwa:⁴⁴

- a) Ayat (1): Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).
- b) Ayat (2): Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).

⁴³ Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), Lembaran Negara Tahun 2016 No. 251, Tambahan Lembaran Negara No. 5952, diakses melalui JDIH (Jaringan Dokumentasi dan Informasi Hukum), Pasal 30..

⁴⁴ Republik Indonesia, *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)*, Lembaran Negara Tahun 2016 No. 251, Tambahan Lembaran Negara No. 5952, Pasal 46.,

- c) Ayat (3): Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Dalam konteks peretasan kartu kredit, pelaku yang secara sengaja mengakses, mengubah, atau menyebarkan data kartu kredit tanpa izin dapat dikenai sanksi sesuai dengan ketentuan di atas, tergantung pada tingkat keparahan dan dampak dari perbuatan yang dilakukan.

3. Tindak Pidana Tambahan: Pemalsuan dan Penyalahgunaan Data

Selain peretasan itu sendiri, UU ITE juga mengatur tindak pidana terkait lainnya, seperti pemalsuan data elektronik dan penyalahgunaan informasi yang diakses secara ilegal. Pasal 35 UU ITE mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan pemalsuan data dengan tujuan agar data elektronik tersebut dianggap sebagai data yang otentik, dapat 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).⁴⁵ Pemalsuan atau penyalahgunaan data kartu kredit, seperti membuat kartu kredit palsu atau melakukan transaksi dengan data curian, juga dapat dikenai sanksi berdasarkan pasal ini.

4. Perlindungan Hukum bagi Korban

UU ITE tidak hanya fokus pada sanksi bagi pelaku, tetapi juga memberikan perlindungan hukum bagi korban peretasan. Pasal 26 UU ITE mengatur tentang hak-hak individu untuk mengajukan penghapusan informasi pribadi dari sistem elektronik yang dikuasai oleh penyelenggara sistem elektronik, jika informasi tersebut terbukti melanggar privasi atau digunakan tanpa izin.⁴⁶

⁴⁵ UU ITE, Pasal 35,

⁴⁶ UU ITE, Pasal 26

Korban peretasan kartu kredit berhak untuk meminta penghapusan data pribadi mereka dari sistem yang telah diakses secara ilegal dan digunakan untuk tujuan kriminal. Selain itu, korban juga berhak mengajukan gugatan perdata untuk mendapatkan ganti rugi atas kerugian yang diderita akibat tindakan peretasan tersebut.

5. Penegakan Hukum dan Tantangan yang Dihadapi

Penegakan hukum terhadap tindak pidana peretasan kartu kredit melalui internet di Indonesia masih menghadapi berbagai tantangan, termasuk keterbatasan teknologi dan sumber daya di kalangan aparat penegak hukum. Meskipun UU ITE telah memberikan dasar hukum yang kuat, implementasinya sering kali terkendala oleh kurangnya pemahaman teknis dan infrastruktur yang memadai.

Upaya penegakan hukum juga membutuhkan kerjasama internasional, mengingat banyaknya kasus peretasan yang melibatkan pelaku atau infrastruktur teknologi dari luar negeri. Oleh karena itu, penguatan kapasitas penegak hukum dan peningkatan kerjasama antarnegara menjadi sangat penting untuk menghadapi tantangan ini.

D. Mekanisme Penegakan Hukum Terhadap Peretasan Kartu Kredit

Penegakan hukum terhadap tindak pidana peretasan kartu kredit di Indonesia diatur oleh beberapa perangkat hukum, dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai landasan utamanya. Penegakan hukum terhadap kejahatan siber, termasuk peretasan kartu kredit, melibatkan berbagai tahap dan institusi, mulai dari deteksi, investigasi, penuntutan, hingga pemidanaan..

Dalam Pasal 30 hingga Pasal 36 UU ITE, terdapat ketentuan yang secara spesifik mengatur larangan akses ilegal dan penggunaan sistem elektronik tanpa izin, termasuk akses terhadap data kartu kredit. Namun, dalam pelaksanaannya, efektivitas penegakan hukum ini belum sepenuhnya optimal. Berdasarkan

laporan yang dikeluarkan oleh Bareskrim Polri, tingkat keberhasilan penegakan hukum terhadap kejahatan siber, termasuk peretasan kartu kredit, berkisar di angka 60-70% dari kasus yang dilaporkan.⁴⁷

Beberapa kendala yang memengaruhi pelaksanaan ini meliputi:

- 1) Kurangnya Kapasitas Teknologi dan Sumber Daya Aparat, yaitu tidak semua unit di tingkat kepolisian daerah memiliki kemampuan forensik digital yang memadai.
- 2) Kerumitan Bukti Digital, maksudnya Bukti elektronik memerlukan prosedur tertentu untuk dijadikan alat bukti sah di pengadilan, sehingga memengaruhi kecepatan penyelesaian kasus
- 3) Kolaborasi Internasional yang Terbatas, yaitu karena sebagian besar peretasan kartu kredit melibatkan jaringan internasional, kolaborasi lintas negara sering menjadi tantangan tersendiri.

Meskipun demikian, beberapa kasus besar menunjukkan keberhasilan mekanisme ini, seperti pengungkapan sindikat kejahatan siber pada tahun 2021 yang melibatkan kerjasama antara Polri dan Interpol.⁴⁸ Dengan terus meningkatnya kapasitas aparat dan kerjasama antar-institusi, diharapkan efektivitas penegakan hukum ini dapat lebih ditingkatkan ke depannya.

1. Deteksi dan Pelaporan Tindak Pidana Peretasan

Mekanisme penegakan hukum terhadap peretasan kartu kredit dimulai dari deteksi dan pelaporan. Tindak pidana peretasan sering kali terdeteksi oleh institusi keuangan, perusahaan penyedia layanan online, atau oleh korban secara langsung. Ketika aktivitas yang mencurigakan atau ilegal terdeteksi, langkah pertama yang diambil adalah melaporkan kejadian tersebut kepada pihak yang berwenang, seperti kepolisian siber (*Cyber Crime Unit*) di bawah

⁴⁷ Kepolisian Republik Indonesia, *Laporan Tahunan Penanganan Kejahatan Siber 2023* (Jakarta: Bareskrim Polri, 2023), hlm. 67.

⁴⁸ Laporan Interpol, *Cooperation on Cybercrime in Southeast Asia* (Singapore: Interpol Cybercrime Unit, 2021), hlm. 45.

Direktorat Tindak Pidana Siber Bareskrim Polri. Dalam konteks ini, pelaporan dari korban atau institusi terkait menjadi sangat penting. Laporan ini kemudian akan menjadi dasar bagi pihak berwenang untuk melakukan penyelidikan awal dan mengumpulkan bukti-bukti yang diperlukan.⁴⁹

2. Investigasi oleh Aparat Penegak Hukum

Setelah laporan diterima, aparat penegak hukum, terutama dari unit siber, akan melakukan investigasi mendalam. Investigasi terhadap tindak pidana peretasan kartu kredit melibatkan pengumpulan dan analisis data elektronik yang terkait dengan aktivitas peretasan. Teknologi forensik digital digunakan untuk melacak jejak digital pelaku, mengidentifikasi metode yang digunakan untuk meretas, dan mengumpulkan bukti-bukti yang dapat dihadirkan di pengadilan. Selama investigasi, kerja sama dengan penyedia layanan internet, perusahaan kartu kredit, dan institusi keuangan sangat diperlukan. Data log aktivitas, catatan transaksi, dan bukti elektronik lainnya menjadi kunci dalam mengungkap identitas pelaku dan modus operandi yang digunakan.⁵⁰

3. Penahanan dan Penyitaan Barang Bukti

Jika hasil investigasi menunjukkan adanya bukti yang cukup, aparat penegak hukum dapat melakukan penahanan terhadap tersangka pelaku peretasan kartu kredit. Selain itu, barang bukti yang terkait dengan tindak pidana, seperti perangkat komputer, server, perangkat penyimpanan data, dan dokumen digital, dapat disita untuk keperluan penyidikan lebih lanjut. Proses penahanan dan penyitaan ini harus dilakukan sesuai dengan prosedur hukum

⁴⁹ Republik Indonesia, *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)*, Lembaran Negara Tahun 2016 No. 251, Tambahan Lembaran Negara No. 5952, Pasal 30, Pasal 35, dan Pasal 46

⁵⁰ M. Edy Susilo, *Hukum Siber: Perlindungan Privasi, Tindakan Penipuan dan Keamanan Informasi* (Bogor: Ghalia Indonesia, 2016).

yang berlaku, untuk memastikan bahwa bukti-bukti yang diperoleh dapat diterima di pengadilan dan tidak melanggar hak-hak tersangka.⁵¹

4. Penuntutan oleh Jaksa Penuntut Umum

Setelah penyidikan selesai dan berkas perkara dinyatakan lengkap (P-21), kasus tersebut akan diserahkan kepada jaksa penuntut umum untuk proses penuntutan. Jaksa penuntut umum berperan dalam menyusun dakwaan berdasarkan bukti-bukti yang telah dikumpulkan selama penyidikan. Dalam konteks peretasan kartu kredit, jaksa akan mendakwa pelaku berdasarkan ketentuan yang ada dalam UU ITE, khususnya Pasal 30 dan Pasal 46. Pada tahap ini, jaksa juga dapat menambahkan dakwaan lain jika ditemukan bukti adanya tindak pidana tambahan seperti pencucian uang, penipuan, atau pemalsuan data elektronik, yang semuanya juga diatur dalam UU ITE dan undang-undang terkait lainnya.⁵²

5. Proses Persidangan dan Pemidanaan

Setelah dakwaan disusun, kasus akan dibawa ke pengadilan untuk diproses lebih lanjut. Dalam persidangan, hakim akan mempertimbangkan semua bukti yang diajukan oleh jaksa penuntut umum dan pembelaan dari pihak terdakwa. Bukti-bukti elektronik, kesaksian ahli, dan hasil analisis forensik digital akan menjadi bagian penting dalam proses pembuktian.

Jika terdakwa dinyatakan bersalah, hakim akan menjatuhkan hukuman sesuai dengan ketentuan yang diatur dalam UU ITE. Hukuman ini bisa berupa pidana penjara, denda, atau kombinasi keduanya, tergantung pada tingkat keseriusan tindak pidana yang dilakukan.⁵³

6. Pemantauan dan Evaluasi Penegakan Hukum

⁵¹ Romli Atmasasmita, *Penegakan Hukum di Indonesia: Problematika dan Solusi* (Jakarta: Sinar Grafika, 2017).

⁵² Kavita Verma, *Digital Forensics: Concepts and Applications* (Boca Raton: CRC Press, 2021).

⁵³ Ahmad Faisal, "Penegakan Hukum Terhadap Kejahatan Siber di Indonesia," *Jurnal Hukum & Pembangunan*, Vol. 49, No. 2 (2019).

Setelah putusan pengadilan, mekanisme penegakan hukum tidak berhenti di situ. Penting untuk melakukan pemantauan terhadap pelaksanaan hukuman yang dijatuhkan dan melakukan evaluasi terhadap efektivitas penegakan hukum dalam kasus-kasus peretasan kartu kredit. Evaluasi ini dapat memberikan masukan bagi pemerintah dan aparat penegak hukum untuk memperbaiki kebijakan dan strategi penanggulangan kejahatan siber di masa depan. Pemantauan juga mencakup upaya untuk mencegah terulangnya kejahatan serupa, misalnya dengan memperketat regulasi keamanan siber, meningkatkan kesadaran masyarakat tentang pentingnya keamanan data, dan memperkuat koordinasi antara berbagai institusi terkait.

E. Perlindungan Hukum Bagi Korban Peretasan Kartu Kredit

Perlindungan hukum bagi korban peretasan kartu kredit di Indonesia menjadi penting, mengingat dampak yang ditimbulkan oleh tindak pidana ini. Kejahatan siber, terutama peretasan kartu kredit, tidak hanya menimbulkan kerugian finansial bagi korban, tetapi juga merusak rasa aman dan kepercayaan terhadap penggunaan sistem elektronik dalam bertransaksi. Oleh karena itu, pemerintah Indonesia, melalui berbagai regulasi, terutama Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), memberikan landasan bagi perlindungan hukum terhadap korban kejahatan siber.

1. Perlindungan Hukum Berdasarkan UU ITE

Pasal 26 UU ITE memberikan perlindungan hak-hak pribadi individu, termasuk hak atas informasi pribadi. Pasal ini menyatakan bahwa setiap penyelenggara sistem elektronik harus menjamin perlindungan data pribadi pengguna. Dalam kasus peretasan kartu kredit, korban berhak atas perlindungan terhadap data pribadi mereka yang telah disalahgunakan.

Selain itu, Pasal 30 UU ITE mengatur tentang akses ilegal ke sistem elektronik. Ketika data kartu kredit seseorang diakses secara ilegal tanpa izin, korban dapat melaporkan tindakan tersebut dan meminta perlindungan hukum

melalui proses pidana yang diatur oleh UU ITE. Dalam konteks peretasan, pelaku dapat dikenai sanksi pidana yang diatur dalam Pasal 46 UU ITE.⁵⁴

2. Hak Restitusi dan Ganti Rugi bagi Korban

UU ITE juga memberikan hak kepada korban peretasan untuk mendapatkan restitusi atau ganti rugi atas kerugian yang diderita. Dalam Pasal 38 UU ITE, dijelaskan bahwa setiap orang yang merasa dirugikan akibat adanya tindak pidana siber berhak untuk mengajukan gugatan perdata guna mendapatkan kompensasi. Pengaturan ini memberikan jalan bagi korban untuk menuntut ganti rugi dari pelaku kejahatan maupun dari pihak lain yang dianggap lalai dalam menjaga data pribadi pengguna, seperti bank atau penyedia layanan kartu kredit.⁵⁵

3. Peran OJK dalam Perlindungan Konsumen

Selain UU ITE, korban peretasan kartu kredit juga mendapatkan perlindungan melalui regulasi keuangan yang diawasi oleh Otoritas Jasa Keuangan (OJK). OJK memiliki peran penting dalam memastikan perlindungan konsumen terhadap praktik penyalahgunaan data keuangan. Bank atau lembaga keuangan lainnya harus mematuhi standar keamanan siber yang ketat, dan jika terjadi pelanggaran, konsumen berhak untuk mengajukan keluhan kepada OJK yang kemudian dapat memproses masalah ini lebih lanjut.⁵⁶

4. Upaya Perlindungan Hukum Lainnya

Sebagai bagian dari perlindungan hukum, aparat penegak hukum dan lembaga terkait terus mengembangkan mekanisme pencegahan dan mitigasi terhadap kejahatan siber, termasuk edukasi kepada masyarakat mengenai pentingnya menjaga kerahasiaan data pribadi. Selain itu, penyedia layanan kartu

⁵⁴ M. Edy Susilo, *Hukum Siber: Perlindungan Privasi, Tindakan Penipuan dan Keamanan Informasi* (Ghalia Indonesia, 2016).

⁵⁵ Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Jakarta: Lembaran Negara Republik Indonesia, 2016)

⁵⁶Otoritas Jasa Keuangan (OJK), Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen di Bidang Jasa Keuangan (Jakarta: Otoritas Jasa Keuangan, 2013)

kredit juga diharapkan untuk terus memperbarui sistem keamanan mereka untuk mencegah peretasan.

Kesimpulannya, perlindungan hukum bagi korban peretasan kartu kredit di Indonesia diatur dalam beberapa regulasi utama, terutama UU ITE dan peraturan yang diawasi oleh OJK. Korban peretasan memiliki hak untuk melaporkan kejahatan, meminta restitusi, serta menuntut ganti rugi melalui gugatan perdata. Meskipun regulasi yang ada sudah cukup komprehensif, masih terdapat tantangan dalam penegakan hukum dan implementasi perlindungan ini secara optimal, terutama karena kejahatan siber terus berkembang seiring dengan kemajuan teknologi.

F. Peretasan Kartu Kredit Menurut Hukum Islam

Sekarang ini dunia sudah terbagi menjadi dua, yakni dunia nyata dan dunia maya. Di dunia nyata kita ketahui ada yang namanya rumah, toko, tempat menyimpan uang atau yang kita sebut dengan bank, dan tempat bermain. Begitu juga dengan dunia maya, hampir setiap orang memiliki yang namanya website, home page, e-mail, dan blog-blog. Di sana banyak sekali beredar informasi-informasi pribadi yang bersifat individu maupun lembaga. Dimana data-data atau informasi tersebut dibutuhkan oleh orang lain. Baik untuk kepentingan bersifat positif bisa juga dalam hal negatif. Untuk meretas informasi tersebut merupakan aktivitas dari individu ataupun sekelompok yang disebut *hacker*.

Hacker atau peretas tidak bisa lepas dari informasi. Seorang peretas tidak bisa melakukan peretasan tanpa mengetahui informasi tentang target yang akan diretas. Ibarat seperti orang yang ingin melakukan tindakan peretasan, si peretas tentunya terlebih dahulu mencari informasi tentang targetnya. Rumah mana yang akan menjadi target, siapa pemilik rumah tersebut, celah mana yang mudah untuk dimasuki, kapan waktu yang tepat untuk melakukan aksinya. Begitu pula dengan seorang peretas, dia terlebih dahulu mencari-cari informasi tentang targetnya. Seperti apa keamanan websitenya, siapa yang akan menjadi targetnya, dan lain

sebagainya. Informasi memiliki hubungan yang sangat erat dengan peretas. Karena kata *hacker* atau peretas baru muncul ketika dunia teknologi informasi berkembang. Ayat-ayat AlQur'an yang memiliki korelasi dan kaitan dengan *hacker*⁵⁷ terdapat pada Al-Qur'an Surah An-Nur ayat 27, yang berbunyi:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَتَذَكَّرُونَ

Wahai orang-orang yang beriman, janganlah memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Demikian itu lebih baik bagimu agar kamu mengambil pelajaran. (QS. An-Nur [24]: 27).

Menurut Ibnu Katsir, ayat ini menekankan pentingnya meminta izin sebelum memasuki rumah orang lain, yang menunjukkan penghormatan terhadap privasi orang lain. Prinsip ini berlaku juga dalam konteks dunia maya; tindakan peretasan, yang mirip dengan memasuki rumah tanpa izin, merupakan pelanggaran terhadap hak privasi individu. Dalam konteks ini, hacker dapat dianggap sebagai pelanggar etika yang tidak menghormati privasi dan hak orang lain.⁵⁸

Ibnu Katsir mengatakan bahwa meminta izin dan mengucapkan salam merupakan adab dari Allah yang diajarkan kepada hamba-hambanya. Allah mengajarkan hamba-hambanya untuk memasuki rumah orang lain sebelum meminta izin kepada si pemilik rumah, setelah mendapatkan izin barulah mengucapkan salam. Hendaklah ia meminta izin sebanyak tiga kali, jika tidak mendapatkan izin, maka dia harus kembali atau pergi sebagaimana ketika Abu Musa minta izin kepada Umar bin Khattab untuk masuk sebanyak tiga kali, namun tidak ada jawaban, maka Abu Musa pun kembali.

Prinsip keadilan dalam Islam juga menekankan perlunya menghormati hak orang lain dan menjaga integritas. Tindakan peretasan dapat merugikan

⁵⁷ QS. an-Nur [24]: 27.

⁵⁸ Ibnu Katsir, *Tafsir Al-Qur'an Al-Azim*.

korban secara finansial dan emosional, serta menciptakan ketidakpercayaan dalam interaksi digital. Oleh karena itu, tindakan tersebut tidak hanya melanggar hukum positif, tetapi juga bertentangan dengan ajaran Islam yang mengedepankan etika dan moralitas.



BAB TIGA

HASIL PENELITIAN

A. Kerangka Hukum Peretasan Kartu Kredit di Indonesia

Di Indonesia, tindakan peretasan kartu kredit dikategorikan sebagai tindak pidana di bidang siber. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi landasan hukum utama yang mengatur tindak pidana siber ini. UU ITE berfungsi untuk melindungi masyarakat dari berbagai bentuk kejahatan elektronik, termasuk akses ilegal, penyalahgunaan data pribadi, serta transaksi elektronik yang tidak sah. Beberapa pasal dalam UU ITE memberikan ketentuan yang spesifik terkait dengan tindakan peretasan kartu kredit, terutama Pasal 30, Pasal 32, dan Pasal 46 UU ITE, yang menjelaskan konsekuensi hukum bagi individu yang mengakses sistem elektronik tanpa izin serta menyalahgunakan data digital.

1. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)

UU ITE merupakan landasan hukum yang komprehensif untuk mengatur berbagai aspek terkait informasi dan transaksi elektronik di Indonesia. Dalam konteks peretasan kartu kredit, UU ITE secara khusus mengatur tentang akses ilegal terhadap sistem elektronik, yang mencakup tindakan peretasan.

- a) Pasal 30 UU ITE mengatur tentang larangan akses ilegal ke sistem elektronik milik orang lain. Pasal ini melarang tindakan masuk ke dalam sistem elektronik tanpa izin, yang mencakup tindakan peretasan atau hacking yang dilakukan untuk memperoleh informasi yang bukan haknya. Dalam konteks peretasan kartu kredit, tindakan mengakses data kartu

- b) kredit tanpa izin merupakan tindakan yang dapat dikenakan pidana berdasarkan pasal ini.⁵⁹
- c) Pasal 32 UU ITE mengatur tentang penyalahgunaan atau perusakan data. Dalam kasus peretasan kartu kredit, apabila pelaku merusak, mengubah, atau menyalahgunakan data kartu kredit korban, maka pelaku dapat dikenakan pidana berdasarkan pasal ini. Tindakan meretas dan menggunakan data kartu kredit orang lain untuk kepentingan pribadi atau untuk keuntungan finansial dianggap sebagai penyalahgunaan data yang melanggar ketentuan dalam Pasal 32.⁶⁰
- d) Pasal 46 UU ITE mengatur sanksi pidana untuk pelanggaran terhadap Pasal 30 dan Pasal 32. Pelaku yang terbukti melakukan peretasan kartu kredit dapat dijatuhi hukuman pidana berupa kurungan penjara dan/atau denda yang cukup signifikan sebagai upaya penegakan hukum siber.⁶¹

UU ITE juga mencakup ketentuan mengenai perlindungan data pribadi yang relevan untuk kasus peretasan kartu kredit, di mana informasi pribadi yang disalahgunakan merupakan salah satu bentuk pelanggaran yang diatur dalam UU ini.

2. Kitab Undang-Undang Hukum Pidana (KUHP)

Selain UU ITE, KUHP juga memberikan dasar hukum dalam penanganan tindak pidana terkait peretasan kartu kredit. Beberapa pasal dalam KUHP dapat digunakan untuk menjerat pelaku kejahatan siber, khususnya dalam konteks penipuan dan peretasan data.

- a) Pasal 362 KUHP mengatur mengenai pencurian, yang dalam konteks kejahatan siber dapat diaplikasikan jika pelaku mengambil atau mengakses data kartu kredit korban tanpa izin dan memanfaatkannya

⁵⁹ Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Tahun 2016 No. 251, Tambahan Lembaran Negara No. 5942, Pasal 30

⁶⁰ *Ibid.*, Pasal 32.

⁶¹ *Ibid.*, Pasal 46.

untuk kepentingan pribadi atau dengan tujuan merugikan pemilik data tersebut. Tindakan ini dapat dianggap sebagai bentuk pencurian yang menimbulkan kerugian materiel pada korban.⁶²

- b) Pasal 378 KUHP mengatur tentang penipuan, yang dapat diterapkan jika pelaku menggunakan data kartu kredit yang diperoleh secara ilegal untuk melakukan transaksi atau memperoleh keuntungan dari pihak ketiga, seperti bank atau merchant, dengan cara yang menipu atau merugikan pihak tersebut. Penggunaan data kartu kredit hasil peretasan untuk transaksi ilegal dianggap sebagai penipuan yang memiliki konsekuensi hukum pidana.⁶³

Penerapan pasal-pasal dalam KUHP ini memberikan tambahan dasar hukum dalam menangani kasus peretasan kartu kredit, terutama dalam hal di mana pelaku melakukan pencurian data untuk tujuan menipu atau memperoleh keuntungan secara tidak sah. Dengan mengombinasikan KUHP dan UU ITE, aparat penegak hukum dapat menjerat pelaku tindak pidana siber ini secara lebih komprehensif, memastikan bahwa aspek peretasan dan penipuan dalam peretasan kartu kredit dapat dikenai sanksi yang sesuai.

3. Peraturan Otoritas Jasa Keuangan (OJK) dan Bank Indonesia

Sebagai lembaga yang mengatur sektor keuangan di Indonesia, Otoritas Jasa Keuangan (OJK) dan Bank Indonesia juga mengeluarkan peraturan yang relevan dalam penanganan peretasan kartu kredit, khususnya untuk menjaga keamanan data nasabah dan mencegah risiko kejahatan siber. Peraturan-peraturan ini mengatur kewajiban bank dan institusi keuangan lainnya untuk memastikan perlindungan data pribadi nasabah dan melaporkan insiden keamanan yang berpotensi merugikan.

⁶² Republik Indonesia, Kitab Undang-Undang Hukum Pidana (KUHP), Lembaran Negara Tahun 1982 No. 77, Tambahan Lembaran Negara No. 3646, Pasal 362.

⁶³ Ibid., Pasal 378 tentang Penipuan.

- a) Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen di Sektor Jasa Keuangan memberikan kerangka perlindungan konsumen, termasuk dalam hal perlindungan data pribadi yang mungkin disalahgunakan akibat peretasan kartu kredit. Peraturan ini mewajibkan institusi keuangan untuk memastikan perlindungan data nasabah dan menyediakan mekanisme pengaduan konsumen jika terjadi insiden yang merugikan mereka.⁶⁴
- b) Peraturan Bank Indonesia No. 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran mengatur penyelenggaraan transaksi pembayaran, termasuk kartu kredit, dengan menekankan pentingnya aspek keamanan dalam pemrosesan data dan transaksi elektronik. Bank dan institusi keuangan diwajibkan menerapkan standar keamanan yang ketat untuk melindungi data nasabah dari ancaman peretasan serta menjaga integritas sistem pembayaran.⁶⁵

Kombinasi kedua peraturan ini memperkuat kerangka hukum dalam melindungi konsumen dari risiko peretasan kartu kredit. Dengan adanya peraturan dari OJK dan Bank Indonesia, diharapkan bank dan penyedia layanan keuangan dapat meningkatkan sistem keamanan mereka guna mencegah insiden kejahatan siber yang merugikan konsumen.

4. Konvensi Internasional dan Kerjasama Internasional

Selain regulasi domestik, kerangka hukum dalam menangani peretasan kartu kredit juga mencakup konvensi internasional dan kolaborasi antarnegara. Dengan semakin meningkatnya kejahatan siber lintas batas, termasuk kasus peretasan kartu kredit, penting bagi Indonesia untuk mengikuti standar

⁶⁴ Otoritas Jasa Keuangan, Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen di Sektor Jasa Keuangan.

⁶⁵ Bank Indonesia, Peraturan Bank Indonesia No. 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.

internasional guna memudahkan penegakan hukum yang melibatkan yurisdiksi lebih dari satu negara.

Salah satu konvensi utama adalah *Budapest Convention on Cybercrime*, yang diadopsi oleh Dewan Eropa pada tahun 2001. Konvensi ini bertujuan untuk menyelaraskan legislasi negara anggota dalam menangani tindak pidana siber, memfasilitasi kerja sama internasional dalam investigasi, dan menetapkan prosedur standar pengumpulan bukti digital lintas negara. Meskipun Indonesia belum meratifikasi konvensi ini, beberapa prinsipnya telah diadopsi dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), seperti pengaturan terkait tindak pidana akses ilegal dan penyalahgunaan data elektronik. Namun, absennya ratifikasi menyebabkan tantangan dalam kerja sama internasional formal, terutama dalam kasus lintas yurisdiksi.⁶⁶

Cakupan *Budapest Convention* mencakup berbagai tindak pidana, seperti akses ilegal ke sistem komputer, pengawasan komunikasi tanpa izin, perubahan data secara ilegal, dan penyalahgunaan perangkat. Selain itu, konvensi ini juga mengatur prosedur penegakan hukum, termasuk pengawasan data lalu lintas dan pengumpulan bukti elektronik. Dengan cakupan yang luas, konvensi ini menjadi rujukan utama bagi banyak negara dalam menyusun regulasi terkait kejahatan siber.

Namun, hingga saat ini, Indonesia belum meratifikasi *Budapest Convention*. Ada beberapa alasan yang menjadi kendala, antara lain:

- 1) Kendala hukum dan regulasi yaitu, meratifikasi konvensi ini berarti Indonesia harus menyesuaikan beberapa undang-undang domestik, yang dapat memakan waktu dan proses politik yang panjang.

⁶⁶ *Budapest Convention on Cybercrime*, Council of Europe, diakses pada 31 Oktober 2024, dari <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

- 2) Kerja sama internasional yang intensif dalam konvensi ini melibatkan berbagi data sensitif, yang dianggap berpotensi mengancam kedaulatan negara.
- 3) Fokus Indonesia masih pada penguatan regulasi domestik, seperti melalui UU ITE, sehingga ratifikasi konvensi internasional belum menjadi prioritas utama

Relevansi *Budapest Convention* dalam kasus peretasan kartu kredit di Indonesia sangat signifikan. Sebagai contoh, banyak kasus peretasan melibatkan pelaku yang berada di negara lain atau menggunakan infrastruktur teknologi di luar negeri. Tanpa adanya kerangka kerja internasional yang formal, seperti yang disediakan oleh konvensi ini, Indonesia menghadapi kesulitan dalam mengakses bukti digital lintas negara, mengekstradisi pelaku, atau melacak aset yang terkait dengan kejahatan tersebut.

Kerja sama internasional juga menjadi aspek krusial, terutama dalam kasus peretasan kartu kredit yang sering kali melibatkan pelaku dari luar negeri atau infrastruktur teknologi yang berada di negara lain. Melalui kerja sama ini, Indonesia dapat menjalin kolaborasi dengan negara lain dalam hal pelacakan, pengumpulan bukti digital, dan penangkapan pelaku yang beroperasi secara global.⁶⁷ Kolaborasi ini tidak hanya melibatkan pemerintah tetapi juga lembaga penegak hukum internasional, seperti Interpol dan ASEANAPOL, yang membantu memfasilitasi investigasi kejahatan siber yang melibatkan beberapa negara.

⁶⁷ *International Cooperation in Cybercrime Investigations*, United Nations Office on Drugs and Crime (UNODC), diakses pada 31 Oktober 2024, dari <https://www.unodc.org/unodc/en/cybercrime/international-cooperation.html>.

B. Analisis Mekanisme Penegakan Hukum Tindak Pidana Peretasan Kartu Kredit dalam UU

Tindak pidana peretasan kartu kredit melalui internet atau yang dikenal dengan istilah *carding* telah menjadi tantangan serius dalam penegakan hukum di Indonesia. Sebagai bagian dari kejahatan siber, *carding* melibatkan akses ilegal terhadap sistem elektronik untuk memperoleh data kartu kredit guna melakukan transaksi tanpa izin pemiliknya. Mekanisme penegakan hukum terhadap tindak pidana ini memerlukan penguatan regulasi, koordinasi antar-lembaga, dan pengembangan kapasitas teknologi penegakan hukum.

1. Dasar Hukum Penegakan Tindak Pidana Peretasan Kartu Kredit

Dasar hukum utama yang digunakan dalam menindak kejahatan *carding* di Indonesia adalah Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 30 UU ITE mengatur bahwa setiap akses ilegal terhadap sistem elektronik, termasuk peretasan, merupakan tindak pidana. Sementara itu, Pasal 46 menetapkan sanksi pidana bagi pelaku dengan hukuman maksimal 8 tahun penjara atau denda paling banyak Rp800 juta.⁶⁸ Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) juga relevan, khususnya Pasal 362 tentang pencurian dan Pasal 378 tentang penipuan, yang sering diterapkan dalam kasus *carding* yang melibatkan penggelapan atau manipulasi data.⁶⁹

2. Proses Penegakkan Hukum

Mekanisme penegakan hukum terhadap tindak pidana ini mencakup beberapa tahapan:

- 1) Pelaporan dan Investigasi, yaitu Proses dimulai dengan laporan korban kepada pihak berwenang, baik melalui kepolisian maupun unit siber

⁶⁸ Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), Pasal 30 dan Pasal 46..

⁶⁹ Republik Indonesia, Kitab Undang-Undang Hukum Pidana (KUHP), Pasal 362 dan Pasal 378.

khusus seperti Direktorat Tindak Pidana Siber Bareskrim Polri.⁷⁰ Dalam tahap ini, forensik digital menjadi alat utama untuk melacak pelaku.

- 2) Penyidikan, merupakan Penyidikan dilakukan dengan memanfaatkan teknologi pelacakan jejak digital (*digital footprints*) dan bekerja sama dengan penyedia layanan internet. Penyelidikan sering kali melibatkan koordinasi dengan institusi internasional, mengingat sifat lintas batas dari kejahatan ini.⁷¹
- 3) Proses Peradilan, maksudnya Dalam proses peradilan, jaksa penuntut umum menggunakan bukti elektronik, sebagaimana diatur dalam UU ITE Pasal 5, yang menyatakan bahwa informasi elektronik dapat digunakan sebagai alat bukti hukum yang sah.⁷²

3. Kendala Dalam Penegakan Hukum

Penegakan hukum terhadap *carding* menghadapi sejumlah kendala:

- 1) Keterbatasan Teknologi dan Sumber Daya, yaitu kapasitas teknologi dalam penyidikan masih terbatas dibandingkan dengan tingkat kompleksitas kejahatan siber.⁷³
- 2) Kerjasama Internasional, merupakan mengingat pelaku sering berada di luar yurisdiksi Indonesia, keterlibatan negara lain menjadi tantangan besar. Perjanjian internasional seperti *Budapest Convention* menjadi penting, meskipun Indonesia belum sepenuhnya meratifikasinya.⁷⁴

⁷⁰ Direktorat Tindak Pidana Siber Bareskrim Polri, "Laporan Tindak Pidana Siber," 2023.

⁷¹ "Penguatan Teknologi Siber untuk Penegakan Hukum di Indonesia," *Jurnal Hukum dan Teknologi*, Vol. 15, No. 2, 2023.

⁷² Republik Indonesia, *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)*, Lembaran Negara Tahun 2016 No. 251, Tambahan Lembaran Negara No. 5952, Pasal 30 dan Pasal 46.

⁷³ Penguatan Teknologi Siber untuk Penegakan Hukum di Indonesia, "Penguatan Teknologi Siber untuk Penegakan Hukum di Indonesia," *Jurnal Hukum dan Teknologi*, Vol. 15, No. 2, 2023.

⁷⁴ Council of Europe, *Budapest Convention on Cybercrime*, diakses pada 31 Oktober 2024, dari <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

- 3) Kurangnya Literasi Digital Masyarakat, yaitu Sebagian besar masyarakat belum memahami pentingnya menjaga data pribadi, sehingga menjadi target empuk pelaku *carding*.⁷⁵

4. Upaya Penguatan Penegakan Hukum

Untuk memperkuat penegakan hukum, pemerintah perlu:

- 1) Meningkatkan Kapasitas Teknologi, yaitu Dengan memperkuat infrastruktur siber, seperti pusat pelaporan kejahatan siber, dan memanfaatkan kecerdasan buatan untuk melacak pola kejahatan.⁷⁶
- 2) Meningkatkan Kerjasama Internasional, yaitu Melalui partisipasi aktif dalam perjanjian internasional yang relevan, seperti *Budapest Convention*
- 3) Meningkatkan Literasi Digital, yaitu Melalui kampanye kesadaran masyarakat tentang pentingnya keamanan data pribadi dalam dunia digital.

C. Perlindungan Hukum bagi Korban Berdasarkan Regulasi yang Ada

Perlindungan hukum bagi korban peretasan kartu kredit melalui internet di Indonesia diatur dalam beberapa regulasi, termasuk Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta beberapa peraturan terkait lainnya. Perlindungan hukum ini bertujuan untuk memberikan keadilan dan pemulihan bagi korban yang mengalami kerugian akibat peretasan kartu kredit.

Salah satu bentuk perlindungan hukum yang diatur adalah hak korban untuk mengajukan gugatan ganti rugi ke pengadilan negeri berdasarkan Pasal 38 ayat (3) UU ITE. Selain itu, dalam konteks perlindungan konsumen, Pasal 46 ayat (1) UU Perlindungan Konsumen juga memberikan hak kepada korban untuk

⁷⁵ Kementerian Komunikasi dan Informatika Republik Indonesia, "Kampanye Kesadaran Hukum: Perlunya Edukasi Keamanan Siber," diakses pada 31 Oktober 2024, dari <https://www.kominfo.go.id>.

⁷⁶ "Penguatan Teknologi Siber untuk Penegakan Hukum di Indonesia," *Jurnal Hukum dan Teknologi*, Vol. 15, No. 2, 2023.

membawa kasus ke pengadilan demi mendapatkan kompensasi atas kerugian yang dialami.

Namun, dalam pelaksanaannya di lapangan, proses gugatan ganti rugi oleh korban sering menghadapi tantangan, seperti:

- 1) Kesulitan Pembuktian yaitu, bukti elektronik yang diperlukan sering kali rumit untuk diverifikasi atau tidak cukup kuat untuk membuktikan hubungan langsung antara peretasan dan kerugian korban.
- 2) Biaya dan Waktu yaitu, proses litigasi di pengadilan membutuhkan waktu yang lama dan biaya yang besar, sehingga banyak korban enggan untuk melanjutkan perkara.
- 3) Kemenangan Kasus yaitu, Berdasarkan analisis beberapa kasus, tingkat keberhasilan korban dalam mendapatkan ganti rugi di pengadilan negeri masih relatif rendah. Sebagai contoh, dalam kasus *A vs B* (2021), korban peretasan kartu kredit yang mengajukan gugatan ke pengadilan negeri dinyatakan kalah karena tidak dapat membuktikan dengan jelas bahwa kerugian keuangannya disebabkan oleh pelaku tertentu yang diidentifikasi dalam perkara.⁷⁷

Di sisi lain, terdapat kasus di mana korban berhasil mendapatkan ganti rugi, meskipun jumlahnya tidak sepenuhnya sesuai dengan tuntutan. Misalnya, dalam perkara *C vs D* (2022), pengadilan mengabulkan sebagian gugatan korban dengan memberikan kompensasi sebesar Rp50 juta dari total tuntutan Rp150 juta.⁷⁸ Hal ini menunjukkan bahwa meskipun regulasi memberikan dasar hukum yang kuat untuk perlindungan korban, efektivitas perlindungan ini masih memerlukan peningkatan, khususnya dalam hal pembuktian dan percepatan proses penyelesaian perkara di pengadilan

⁷⁷ Putusan Pengadilan Negeri Jakarta Pusat, *Perkara No. 123/Pdt.G/2021/PN.JKT.PST* (2021).

⁷⁸ Putusan Pengadilan Negeri Surabaya, *Perkara No. 456/Pdt.G/2022/PN.SBY* (2022).

1. Perlindungan Berdasarkan UU ITE

UU ITE memberikan dasar hukum yang kuat bagi korban untuk menuntut keadilan dan mendapatkan perlindungan dari negara. Pasal 26 UU ITE mengatur hak-hak individu dalam hal penghapusan informasi pribadi yang melanggar privasi atau digunakan tanpa izin. Dalam konteks peretasan kartu kredit, korban berhak untuk meminta penghapusan data pribadi mereka yang telah diakses atau digunakan oleh peretas secara ilegal.⁷⁹

Selain itu, korban juga berhak untuk mengajukan gugatan perdata terhadap pelaku peretasan untuk mendapatkan ganti rugi atas kerugian yang diderita. Pasal 36 UU ITE memungkinkan korban untuk menuntut pelaku dengan dasar perbuatan melawan hukum, dan pengadilan dapat memerintahkan pelaku untuk membayar ganti rugi yang setimpal.⁸⁰

2. Perlindungan Berdasarkan Undang-Undang Perlindungan Konsumen

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen juga memberikan perlindungan bagi korban peretasan kartu kredit. Konsumen memiliki hak atas keamanan dan kenyamanan dalam melakukan transaksi elektronik. Jika terjadi peretasan, konsumen dapat mengajukan keluhan kepada lembaga perlindungan konsumen atau membawa kasus ini ke pengadilan.⁸¹

Pasal 4 UU Perlindungan Konsumen menyatakan bahwa konsumen berhak untuk mendapatkan kompensasi, ganti rugi, dan/atau penggantian jika

⁷⁹ Republik Indonesia, *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*, diakses pada 31 Oktober 2024, dari <https://www.menkominfo.go.id>.

⁸⁰ A. H. Bakri, "Tanggung Jawab Pelaku Kejahatan Siber dan Hak Korban," *Jurnal Hukum dan Perundang-Undangan* 7, no. 1 (2021): halm. 25-35

⁸¹ Republik Indonesia, *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*, diakses pada 31 Oktober 2024, dari <https://www.konsumen.go.id>.

mengalami kerugian akibat penggunaan barang atau jasa, termasuk dalam kasus peretasan kartu kredit.⁸²

3. Perlindungan Berdasarkan Peraturan Bank Indonesia

Bank Indonesia (BI) sebagai otoritas moneter dan pengawas sistem pembayaran juga memiliki peraturan yang melindungi konsumen dalam transaksi elektronik. Bank yang menerbitkan kartu kredit wajib menerapkan standar keamanan yang ketat dan memberikan perlindungan kepada nasabah yang menjadi korban peretasan.

Peraturan Bank Indonesia tentang Manajemen Risiko dan Pengendalian Intern untuk Aktivitas Sistem Pembayaran mengatur bahwa bank harus bertanggung jawab atas keamanan data nasabah dan harus mengambil langkah-langkah yang diperlukan untuk melindungi informasi keuangan nasabah dari ancaman peretasan. Jika terjadi pelanggaran, bank berkewajiban untuk bekerja sama dengan penegak hukum dan memberikan bantuan kepada nasabah untuk memulihkan kerugian yang dialami.⁸³

4. Hak untuk Mendapatkan Informasi dan Bantuan Hukum

Korban peretasan kartu kredit juga berhak untuk mendapatkan informasi yang jelas dan bantuan hukum dalam menindaklanjuti kasusnya. Penyedia layanan keuangan dan internet berkewajiban memberikan informasi yang diperlukan kepada korban mengenai langkah-langkah yang harus diambil setelah peretasan terjadi.

Selain itu, korban juga dapat mencari bantuan hukum dari lembaga bantuan hukum atau advokat yang berpengalaman dalam menangani kasus-kasus

⁸² E. N. Wijaya, "Perlindungan Konsumen dalam Transaksi Elektronik," *Jurnal Hukum dan Bisnis* 4, no. 2 (2022): halm. 99-110.

⁸³ Peraturan Bank Indonesia tentang Manajemen Risiko dan Pengendalian Intern untuk Aktivitas Sistem Pembayaran, diakses pada 31 Oktober 2024, dari <https://www.bi.go.id>.

kejahatan siber. Bantuan ini bisa mencakup pendampingan dalam proses hukum, penyusunan gugatan, hingga perwakilan di pengadilan.⁸⁴

5. Perlindungan Hukum Internasional

Karena kejahatan siber, termasuk peretasan kartu kredit, sering kali melibatkan pelaku dari luar negeri, kerja sama internasional menjadi penting. Indonesia telah menjalin kerja sama dengan berbagai negara dan organisasi internasional dalam rangka penegakan hukum siber. Perlindungan hukum bagi korban dapat diperkuat melalui perjanjian ekstradisi, kerjasama lintas batas dalam investigasi, dan pertukaran informasi antarnegara.⁸⁵



⁸⁴ L. M. Santoso, "Bantuan Hukum bagi Korban Kejahatan Siber," *Jurnal Kejahatan dan Hukum* 3, no. 1 (2023): halm. 75-85.

⁸⁵ "Kerja Sama Internasional dalam Penanganan Kejahatan Siber," diakses pada 31 Oktober 2024, dari <https://www.interpol.int/en/Crimes/Cybercrime>.

BAB IV PENUTUP

A. Kesimpulan

Dalam skripsi ini, telah dibahas secara komprehensif mengenai tinjauan yuridis terhadap tindak pidana peretasan kartu kredit melalui internet berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Berdasarkan analisis yang telah dilakukan, beberapa kesimpulan penting dapat diambil:

1. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur tindak pidana peretasan kartu kredit sebagai bagian dari kejahatan siber. Pasal 30 hingga Pasal 36 UU ITE dengan tegas melarang dan mengancam pidana terhadap akses ilegal serta penyalahgunaan data elektronik. Regulasi ini bertujuan memberikan perlindungan hukum terhadap sistem elektronik dan transaksi digital. Namun, implementasinya menghadapi tantangan terkait pembuktian digital dan keterbatasan teknologi, yang menghambat penegakan hukum secara efektif. Penegakan hukum terhadap tindak pidana peretasan kartu kredit mencakup tahapan penyelidikan, penyidikan, penuntutan, dan peradilan, yang melibatkan institusi seperti kepolisian, kejaksaan, dan pengadilan. Proses ini didukung oleh UU ITE dan undang-undang terkait lainnya. Meskipun demikian, penegakan hukum masih menghadapi kendala, terutama dalam memahami bukti digital serta koordinasi lintas lembaga, terutama untuk kasus lintas yurisdiksi.
2. Penegakan hukum terhadap tindak pidana peretasan kartu kredit di Indonesia mencakup tahapan penyelidikan, penyidikan, penuntutan, dan peradilan, yang melibatkan institusi seperti kepolisian, kejaksaan, dan pengadilan. Proses ini didukung oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) serta undang-undang terkait lainnya. Penanganan kejahatan siber sangat bergantung pada kemampuan aparat dalam

3. memahami dan mengolah bukti digital, yang sering kali bersifat kompleks dan memerlukan keahlian forensik teknologi. Namun, penegakan hukum masih menghadapi kendala dalam hal koordinasi lintas lembaga dan keterbatasan pemahaman terhadap bukti digital. Kesulitan ini semakin diperparah pada kasus yang melibatkan lintas yurisdiksi, karena membutuhkan kerja sama dengan lembaga internasional seperti Interpol dan ASEANAPOL. Tantangan-tantangan tersebut menunjukkan perlunya peningkatan kapasitas sumber daya manusia, harmonisasi antarinstansi, serta pembaruan teknologi untuk memperkuat efektivitas penegakan hukum terhadap kejahatan siber di Indonesia.
4. Bagi korban tindak pidana peretasan kartu kredit, perlindungan hukum mencakup pengembalian kerugian materiil dan tindakan hukum terhadap pelaku. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan hak kepada korban untuk melindungi privasi data pribadi serta mendapatkan kompensasi melalui jalur hukum, baik perdata maupun pidana. Ketentuan ini bertujuan untuk memulihkan hak-hak korban serta memberikan efek jera kepada pelaku. Namun, pelaksanaan perlindungan hukum ini sering terkendala oleh rendahnya edukasi masyarakat mengenai hak-hak mereka dan mekanisme hukum yang tersedia. Selain itu, akses terhadap proses pemulihan sering kali terbatas, terutama bagi korban yang tidak memiliki pengetahuan atau sumber daya yang memadai. Kendala ini menunjukkan perlunya upaya peningkatan literasi hukum masyarakat dan perbaikan aksesibilitas mekanisme hukum, agar perlindungan bagi korban dapat berjalan lebih optimal.

B. Saran

Saran yang dapat penulis sampaikan mengenai skripsi ini yaitu:

1. Revisi dan Penyesuaian UU ITE. Mengingat perkembangan teknologi informasi yang sangat cepat, perlu dilakukan revisi dan penyesuaian terhadap UU ITE dan peraturan terkait lainnya agar lebih relevan dengan tantangan kejahatan siber saat ini. Revisi ini harus mencakup penambahan ketentuan yang lebih spesifik tentang berbagai bentuk kejahatan siber, peningkatan sanksi bagi pelaku yang melibatkan teknologi canggih, serta penguatan mekanisme perlindungan data pribadi.
2. Peningkatan Kapasitas dan Teknologi Penegak Hukum. Pemerintah dan institusi terkait perlu memperkuat kapasitas teknis dan sumber daya aparat penegak hukum, khususnya di bidang kejahatan siber. Hal ini dapat dilakukan melalui pelatihan intensif, peningkatan teknologi forensik digital, serta pengembangan unit khusus untuk menangani kejahatan siber yang semakin kompleks. Selain itu, penegak hukum juga perlu dilengkapi dengan infrastruktur teknologi yang lebih canggih untuk dapat mendeteksi dan menindak pelaku peretasan dengan lebih efektif.
3. Peningkatan Perlindungan Hukum bagi Korban. Perlindungan hukum bagi korban peretasan kartu kredit perlu diperkuat, terutama dalam hal pemulihan kerugian dan bantuan hukum. Pemerintah harus memastikan bahwa korban mendapatkan akses yang mudah dan cepat untuk mengajukan klaim ganti rugi serta mendapatkan perlindungan hukum yang memadai. Selain itu, perlu dibentuk mekanisme pengawasan yang lebih ketat untuk memastikan bahwa penyelenggara sistem elektronik mematuhi standar keamanan yang tinggi dalam melindungi data konsumen.

Melalui penerapan saran-saran ini, diharapkan penanganan tindak pidana peretasan kartu kredit di Indonesia dapat lebih efektif dan mampu menghadapi tantangan di era digital yang semakin kompleks.

DAFTAR PUSTAKA

A. Buku

- Ahmad Faisal, *Penegakan Hukum Terhadap Kejahatan Siber di Indonesia* (Jakarta: Kencana, 2018).
- Bunga Ayu Lestari, Budi Suharjo, dan Istiqlaliyah Muflikhat. "Penggunaan Kartu Kredit dalam Era Digital." Dalam *Hukum Perbankan Indonesia*, Jakarta: Sinar Grafika, 2016.
- Debarati Halder dan K. Jaishankar. *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global, 2012.
- Direktorat Tindak Pidana Siber Bareskrim Polri. "Laporan Tindak Pidana Siber," 2023
- Kavita Verma. *Digital Forensics: Concepts and Applications*. Boca Raton: CRC Press, 2021.
- M. Edy Susilo. *Hukum Siber: Perlindungan Privasi, Tindakan Penipuan dan Keamanan Informasi*. Bogor: Ghalia Indonesia, 2016.
- Peter Mahmud Marzuki. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2014.
- Philippe Nonet dan Philip Selznick. *Law and Society in Transition: Toward Responsive Law*. Harper & Row, 2001.
- Philippe Nonet dan Philip Selznick. *Law and Society in Transition: Toward Responsive Law*. Harper & Row, 2001
- Romli Atmasasmita. *Penegakan Hukum di Indonesia: Problematika dan Solusi*. Jakarta: Sinar Grafika, 2017.
- Satjipto Rahardjo. *Hukum Progresif: Sebuah Sintesa Hukum di Tengah Kehidupan Masyarakat Modern*. Yogyakarta: Genta Publishing, 2012.
- Satjipto Rahardjo. *Hukum Progresif: Sebuah Sintesa Hukum Indonesia*. Yogyakarta: Genta Publishing, 2009.
- Soerjono Soekanto. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Pers, 2004.

B. Jurnal

- A. H. Bakri, "Tanggung Jawab Pelaku Kejahatan Siber dan Hak Korban," *Jurnal Hukum dan Perundang-Undangan* 7, no. 1 (2021): hlm. 25–35.
- Ahmad Faisal. "Penegakan Hukum Terhadap Kejahatan Siber di Indonesia." *Jurnal Hukum & Pembangunan*, Vol. 49, No. 2, 2019.

- Alcianno G. Gani. "Cybercrime (Kejahatan Berbasis Komputer)." *Jurnal Sistem Informasi Universitas Suryadarma*, Vol. 5, No. 1, 2014, hlm. 16.
- Bambang Hartono. "Penerapan Sanksi Pidana Terhadap Tindak Pidana Carding." *Jurnal Universitas Bandar Lampung (UBL)*, Vol. 4, No. 1, 2016, hlm. 168.
- Diny Luthfah. "Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata Dalam Perspektif Hukum Keamanan Nasional Indonesia." *Jurnal Keamanan Nasional*, Vol. 3, 2021, hlm. 12.
- E. N. Wijaya, "Perlindungan Konsumen dalam Transaksi Elektronik," *Jurnal Hukum dan Bisnis* 4, no. 2 (2022): hlm. 99–110.
- Hardianto Djanggih dan Nurul Qamar. "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan kejahatan Siber (Cyber Crime)." *Pandecta: Research Law Journal*, Vol. 13, No. 1, 2018, hlm. 12.
- I Gede Krisna Ginara, I Made Minggu Widyantara, dan Ni Komang Arini Styawati. "Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia." *Jurnal Preferensi Hukum*, Vol. 3, No. 1, 2022, hlm. 169.
- L. M. Santoso, "Bantuan Hukum bagi Korban Kejahatan Siber," *Jurnal Kejahatan dan Hukum* 3, no. 1 (2023): hlm. 75–85..

C. Dokumen Hukum

- Republik Indonesia. *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)*. Lembaran Negara Tahun 2016 No. 251, Tambahan Lembaran Negara No. 5952.
- Budapest Convention on Cybercrime, Council of Europe. Diakses pada 31 Oktober 2024 dari <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.
- International Cooperation in Cybercrime Investigations, United Nations Office on Drugs and Crime (UNODC). Diakses pada 31 Oktober 2024 dari <https://www.unodc.org/unodc/en/cybercrime/international-cooperation.html>.
- International Cooperation in Cybercrime Investigations, United Nations Office on Drugs and Crime (UNODC). Diakses pada 31 Oktober 2024 dari <https://www.unodc.org/unodc/en/cybercrime/international-cooperation.html>.

Kementerian Komunikasi dan Informatika Republik Indonesia.
"Kampanye Kesadaran Hukum: Perlunya Edukasi Keamanan Siber."
Diakses pada 31 Oktober 2024 dari <https://www.kominfo.go.id>.

Republik Indonesia. *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)*, Lembaran Negara Tahun 2016 No. 251, Tambahan Lembaran Negara No. 5942.

Otoritas Jasa Keuangan (OJK). *Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen di Bidang Jasa Keuangan*. Jakarta: Otoritas Jasa Keuangan, 2013.

Bank Indonesia. *Peraturan Bank Indonesia Nomor 11/11/PBI/2009 tentang Alat Pembayaran Menggunakan Kartu (APMK)*. Lembaran Negara Republik Indonesia Tahun 2009 No. 11.



Lampiran 1.1 UU No.11 Tahun 2008



PRESIDEN
REPUBLIK INDONESIA

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 11 TAHUN 2008

TENTANG
INFORMASI DAN TRANSAKSI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA
PRESIDEN REPUBLIK INDONESIA,

- Menimbang :
- a. bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat;
 - b. bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa;
 - c. bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru;
 - d. bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkuat persatuan dan kesatuan nasional berdasarkan Peraturan Perundang-undangan demi kepentingan nasional;
 - e. bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat;
 - f. bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia;
 - g. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f, perlu membentuk Undang-Undang tentang Informasi dan Transaksi Elektronik;

Mengingat . . .



PRESIDEN
REPUBLIK INDONESIA

- 14 -

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Pasal 26

- (1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
- (2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

BAB VII

PERBUATAN YANG DILARANG

Pasal 27

- (1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesucilaan.
- (2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
- (3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
- (4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 28 . . .



PRESIDEN
REPUBLIK INDONESIA

- 15 -

Pasal 28

- (1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
- (2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi.

Pasal 30

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

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 . . .



PRESIDEN
REPUBLIK INDONESIA

- 16 -

- (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.
- (3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
- (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
- (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34 . . .



PRESIDEN
REPUBLIK INDONESIA

- 17 -

Pasal 34

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
 - a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
 - b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
- (2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

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 36

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Pasal 37

Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

BAB VIII . . .



PRESIDEN
REPUBLIK INDONESIA

- 18 -

BAB VIII
PENYELESAIAN SENGKETA

Pasal 38

- (1) Setiap Orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menimbulkan kerugian.
- (2) Masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 39

- (1) Gugatan perdata dilakukan sesuai dengan ketentuan Peraturan Perundang-undangan.
- (2) Selain penyelesaian gugatan perdata sebagaimana dimaksud pada ayat (1), para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan.

BAB IX

PERAN PEMERINTAH DAN PERAN MASYARAKAT

Pasal 40

- (1) Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan Peraturan Perundang-undangan.
- (2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.
- (3) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi.
- (4) Instansi atau institusi sebagaimana dimaksud pada ayat (3) harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.

(5) Instansi . . .



PRESIDEN
REPUBLIK INDONESIA

- 19 -

- (5) Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya.
- (6) Ketentuan lebih lanjut mengenai peran Pemerintah sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 41

- (1) Masyarakat dapat berperan meningkatkan pemanfaatan Teknologi Informasi melalui penggunaan dan Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik sesuai dengan ketentuan Undang-Undang ini.
- (2) Peran masyarakat sebagaimana dimaksud pada ayat (1) dapat diselenggarakan melalui lembaga yang dibentuk oleh masyarakat.
- (3) Lembaga sebagaimana dimaksud pada ayat (2) dapat memiliki fungsi konsultasi dan mediasi.

BAB X

PENYIDIKAN

Pasal 42

Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini.

Pasal 43

- (1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

(2) Penyidikan . . .



PRESIDEN
REPUBLIK INDONESIA

- 20 -

- (2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.
- (3) Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.
- (4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.
- (5) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:
 - a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana berdasarkan ketentuan Undang-Undang ini;
 - b. memanggil setiap Orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang terkait dengan ketentuan Undang-Undang ini;
 - c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana berdasarkan ketentuan Undang-Undang ini;
 - d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana berdasarkan Undang-Undang ini;
 - e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini;
 - f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana berdasarkan ketentuan Undang-Undang ini;
 - g. melakukan penyegelan dan penyitaan terhadap alat dan atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan Peraturan Perundang-undangan;

h. meminta . . .



PRESIDEN
REPUBLIK INDONESIA

- 21 -

- h. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau
 - i. mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku.
- (6) Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.
- (7) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan menyampaikan hasilnya kepada penuntut umum.
- (8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.

Pasal 44

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

- a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
- b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

BAB XI

KETENTUAN PIDANA

Pasal 45

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap . . .



PRESIDEN
REPUBLIK INDONESIA

- 22 -

- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Pasal 46

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
- (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

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 Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 48

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

(2) Setiap . . .



PRESIDEN
REPUBLIK INDONESIA

SALINAN

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 19 TAHUN 2016
TENTANG
PERUBAHAN ATAS UNDANG-UNDANG
NOMOR 11 TAHUN 2008
TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

- Menimbang : a. bahwa untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu masyarakat yang demokratis perlu dilakukan perubahan terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik agar terwujud keadilan, ketertiban umum, dan kepastian hukum;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu membentuk Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
- Mengingat : 1. Pasal 5 ayat (1), Pasal 20, Pasal 25A, Pasal 28D ayat (1), Pasal 28E ayat (2), Pasal 28E ayat (3), Pasal 28F, Pasal 28G ayat (1), Pasal 28J ayat (2), dan Pasal 33 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

Dengan . . .



PRESIDEN
REPUBLIK INDONESIA

- 5 -

19. Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
 20. Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
 21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
 22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
 23. Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.
2. Ketentuan Pasal 5 tetap dengan perubahan penjelasan ayat (1) dan ayat (2) sehingga penjelasan Pasal 5 menjadi sebagaimana ditetapkan dalam penjelasan pasal demi pasal Undang-Undang ini.
 3. Ketentuan Pasal 26 ditambah 3 (tiga) ayat, yakni ayat (3), ayat (4), dan ayat (5) sehingga Pasal 26 berbunyi sebagai berikut:

Pasal 26

- (1) Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
- (2) Setiap Orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

(3) Setiap . . .



PRESIDEN
REPUBLIK INDONESIA

- 6 -

- (3) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan.
 - (4) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.
 - (5) Ketentuan mengenai tata cara penghapusan Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah.
4. Ketentuan Pasal 27 tetap dengan perubahan penjelasan ayat (1), ayat (3), dan ayat (4) sehingga penjelasan Pasal 27 menjadi sebagaimana ditetapkan dalam penjelasan pasal demi pasal Undang-Undang ini.
 5. Ketentuan ayat (3) dan ayat (4) Pasal 31 diubah sehingga Pasal 31 berbunyi 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.

(3) Ketentuan . . .



PRESIDEN
REPUBLIK INDONESIA

- 7 -

- (3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.
 - (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang.
6. Di antara ayat (2) dan ayat (3) Pasal 40 disisipkan 2 (dua) ayat, yakni ayat (2a) dan ayat (2b); ketentuan ayat (6) Pasal 40 diubah; serta penjelasan ayat (1) Pasal 40 diubah sehingga Pasal 40 berbunyi sebagai berikut:

Pasal 40

- (1) Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan peraturan perundang-undangan.
- (2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan.
- (2a) Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.
- (2b) Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.

(3) Pemerintah . . .



PRESIDEN
REPUBLIK INDONESIA

- 8 -

- (3) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi.
 - (4) Instansi atau institusi sebagaimana dimaksud pada ayat (3) harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.
 - (5) Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya.
 - (6) Ketentuan lebih lanjut mengenai peran Pemerintah sebagaimana dimaksud pada ayat (1), ayat (2), ayat (2a), ayat (2b), dan ayat (3) diatur dalam peraturan pemerintah.
7. Ketentuan ayat (2), ayat (3), ayat (5), ayat (6), ayat (7), dan ayat (8) Pasal 43 diubah; di antara ayat (7) dan ayat (8) Pasal 43 disisipkan 1 (satu) ayat, yakni ayat (7a); serta penjelasan ayat (1) Pasal 43 diubah sehingga Pasal 43 berbunyi sebagai berikut:

Pasal 43

- (1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.
- (2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan integritas atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.

(3) Penggeledahan . . .



PRESIDEN
REPUBLIK INDONESIA

- 9 -

- (3) Penggeledahan dan/atau penyitaan terhadap Sistem Elektronik yang terkait dengan dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana.
- (4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.
- (5) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:
 - a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
 - b. memanggil setiap Orang atau pihak lainnya untuk didengar dan diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
 - c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
 - d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
 - e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
 - f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
 - g. melakukan . . .



PRESIDEN
REPUBLIK INDONESIA

- 10

- g. melakukan penyegelan dan penyitaan terhadap alat dan/atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan peraturan perundang-undangan;
 - h. membuat suatu data dan/atau Sistem Elektronik yang terkait tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik agar tidak dapat diakses;
 - i. meminta informasi yang terdapat di dalam Sistem Elektronik atau informasi yang dihasilkan oleh Sistem Elektronik kepada Penyelenggara Sistem Elektronik yang terkait dengan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
 - j. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik; dan/atau
 - k. mengadakan penghentian penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan hukum acara pidana.
- (6) Penangkapan dan penahanan terhadap pelaku tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana.
- (7) Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) dalam melaksanakan tugasnya memberitahukan dimulainya penyidikan kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia.
- (7a) Dalam hal penyidikan sudah selesai, Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) menyampaikan hasil penyidikannya kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia.
- (8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti sesuai dengan ketentuan peraturan perundang-undangan.

8. Ketentuan . . .



PRESIDEN
REPUBLIK INDONESIA

- 11

8. Ketentuan Pasal 45 diubah serta di antara Pasal 45 dan Pasal 46 disisipkan 2 (dua) pasal, yakni Pasal 45A dan Pasal 45B sehingga berbunyi sebagai berikut:

Pasal 45

- (1) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).
- (4) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(5) Ketentuan . . .



PRESIDEN
REPUBLIK INDONESIA

- 12

- (5) Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan.

Pasal 45A

- (1) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pasal 45B

Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

Pasal II

Undang-Undang ini mulai berlaku pada tanggal diundangkan.

Agar . . .



PRESIDEN
REPUBLIK INDONESIA

- 13

Agar setiap orang mengetahuinya, memerintahkan pengundangan Undang-Undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Disahkan di Jakarta
pada tanggal 25 November 2016

PRESIDEN REPUBLIK INDONESIA,

ttd

JOKO WIDODO

Diundangkan di Jakarta
pada tanggal 25 November 2016

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

YASONNA H. LAOLY

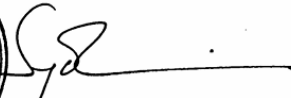
LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2016 NOMOR 251

Salinan sesuai dengan aslinya

KEMENTERIAN SEKRETARIAT NEGARA
REPUBLIK INDONESIA

Asisten Deputi Bidang Perekonomian,
Departemen Hukum dan Perundang-undangan,




Silvia Silvana Djaman

Lampiran SK Pembimbing



SURAT KEPUTUSAN DEKAN FAKULTAS SYARIAH DAN HUKUM
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
Nomor: 1494/Un.08/FSH/PP.00.9/5/2024

TENTANG

PENETAPAN PEMBIMBING SKRIPSI MAHASISWA

- Menimbang :
- Bahwa untuk kelancaran bimbingan KKU Skripsi pada Fakultas Syariah dan Hukum, maka dipandang perlu menunjukkan pembimbing KKU Skripsi tersebut;
 - Bahwa yang namanya dalam Surat Keputusan ini dipandang mampu dan cakap serta memenuhi syarat untuk diangkat dalam jabatan sebagai pembimbing KKU Skripsi.
 - Bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan keputusan Dekan Fakultas Syariah dan Hukum UIN Ar-Raniry Banda Aceh.
- Mengingat :
- Undang-Undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
 - Undang-Undang Nomor 14 Tahun 2005 tentang Guru dan Dosen;
 - Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi;
 - Peraturan Pemerintah Nomor 19 Tahun 2005 tentang Standar Nasional Pendidikan;
 - Peraturan Pemerintah RI Nomor 04 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi;
 - Peraturan Presiden RI Nomor 64 Tahun 2013 tentang Perubahan Institut Agama Islam Negeri IAIN Ar-Raniry Banda Aceh Menjadi Universitas Islam Negeri;
 - Keputusan Menteri Agama 492 Tahun 2003 tentang Pendelegasian Wewenang Pengangkatan, Pemindahan dan Pemberhentian PNS di lingkungan Departemen Agama RI;
 - Peraturan Menteri Agama Republik Indonesia Nomor 12 Tahun 2014 tentang Organisasi dan Tata Kerja Universitas Islam Negeri Ar-Raniry Banda Aceh;
 - Peraturan Menteri Agama Republik Indonesia Nomor 12 Tahun 2020 tentang Statuta Universitas Islam Negeri Ar-Raniry Banda Aceh;
 - Surat Keputusan Rektor UIN Ar-Raniry Nomor 01 Tahun 2015 tentang Pemberi Kuasa dan Pendelegasian Wewenang Kepada Para Dekan dan Direktur Program Pasca Sarjana dalam Lingkungan UIN Ar-Raniry Banda Aceh;

MEMUTUSKAN:

- Menetapkan : KEPUTUSAN DEKAN FAKULTAS SYARIAH DAN HUKUM UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH TENTANG BIMBINGAN SKRIPSI
- KESATU : Menunjuk Saudara (j):
- | | |
|---------------------------|-----------------------|
| a. M. Syuib, S.H.I., M.H. | Sebagai Pembimbing I |
| b. Muhammad Iqbal, SE.,MM | Sebagai Pembimbing II |
- untuk membimbing KKU Skripsi Mahasiswa (j):
- | | |
|-------|--|
| Nama | : Rausyan Fikry |
| NIM | : 190106107 |
| Prodi | : Ilmu Hukum |
| Judul | : Tinjauan Yuridis Terhadap Tindak Pidana Peretasan Kartu Kredit Melalui Internet Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (UU ITE) Di Indonesia |
- 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 2023;
- 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 02 Mei 2024
DEKAN FAKULTAS SYARIAH DAN HUKUM,



Tembusan:

- Rektor UIN Ar-Raniry;
- Ketua Prodi Ilmu Hukum;
- Mahasiswa yang bersangkutan;
- Arsip

DAFTAR RIWAYAT HIDUP

Data Diri

Nama : Rausyan Fikry
NIM : 190106107
Tempat/ Tgl. Lahir : Desa Pisang/03 Desember 1999
Status : Belum Menikah
Alamat : Kp. Pisang, Kecamatan Labuhan Haji,
Kabupaten Aceh Selatan
No. Hp : 082286438025
Email : rausyanfikry123@gmail.com

Riwayat Pendidikan

1. SD : Lulus Tahun 2011
2. SMP : Lulus Tahun 2014
3. SMA : Lulus Tahun 2017
4. Fakultas Syariah dan Hukum

Data Orang Tua

Nama Ayah : Anhar, S.Ag
Pekerjaan : PNS
Nama Ibu : Habibah S,Ag
Pekerjaan : PNS
Alamat Orang tua : Kp. Pisang, Kecamatan Labuhan Haji,
Kabupaten Aceh Selatan