TINDAK PIDANA PENCURIAN KARTU KREDIT *CARDING* MELALUI MEDIA ELEKTRONIK DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK
(STUDI KASUS: No.845/Pid.Sus/2020/PT SBY)

SKRIPSI

Diajukan Untuk Memenuhi Syarat
Memperoleh Gelar Sarjana Hukum

Oleh:

MUHAMMAD TAUFAN
NPM. 2106200418

FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2025

PENGESAHAN SKRIPSI

JUDUL SKRIPSI : **TINDAK PIDANA PENCURIAN KARTU KREDIT CARDING DITINJAU MELALUI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: NO.845/PID.SUS/2020/PT SBY)**

NAMA : **MUHAMMAD TAUFAN**

NPM : **2106200418**

PRODI/BAGIAN : **HUKUM / HUKUM PIDANA**

Skripsi tersebut di atas telah diujikan oleh Dosen Penguji Fakultas Hukum Universitas Muhammadiyah Sumatera Utara pada Tanggal 17 Setpember 2025.

Dosen Penguji

Assoc. Prof. Dr. Nursariani Simatupang, S.H., M.Hum. **NIDN: 0111117402**	**Dr. Rahmad Abduh, S.H., M.H.** **NIDN:** 0004127204	**Dr. Hj. Asliani Harahap, S.H., M.H.** **NIDN: 0126066802**

Disahkan oleh:
Dekan Fakultas Hukum UMSU

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

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
UMSU Unggul | Cerdas | Terpercaya
Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA 1

Panitia Ujian Sarjana Strata-I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Rabu, tanggal 17 September 2025, Jam 08.30 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan, menimbang:

MENETAPKAN

NAMA	:	**MUHAMMAD TAUFAN**
NPM	:	**2106200418**
PRODI/BAGIAN	:	**HUKUM / HUKUM PIDANA**
JUDUL SKRIPSI	:	**TINDAK PIDANA PENCURIAN KARTU KREDIT CARDING DITINJAU MELALUI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: No.845/Pid.Sus/2020/PT SBY)**

Dinyatakan:

(A) Lulus Yudisium dengan predikat Sangat Baik
( ) Lulus Bersyarat, memperbaiki/Ujian Ulang
( ) Tidak Lulus

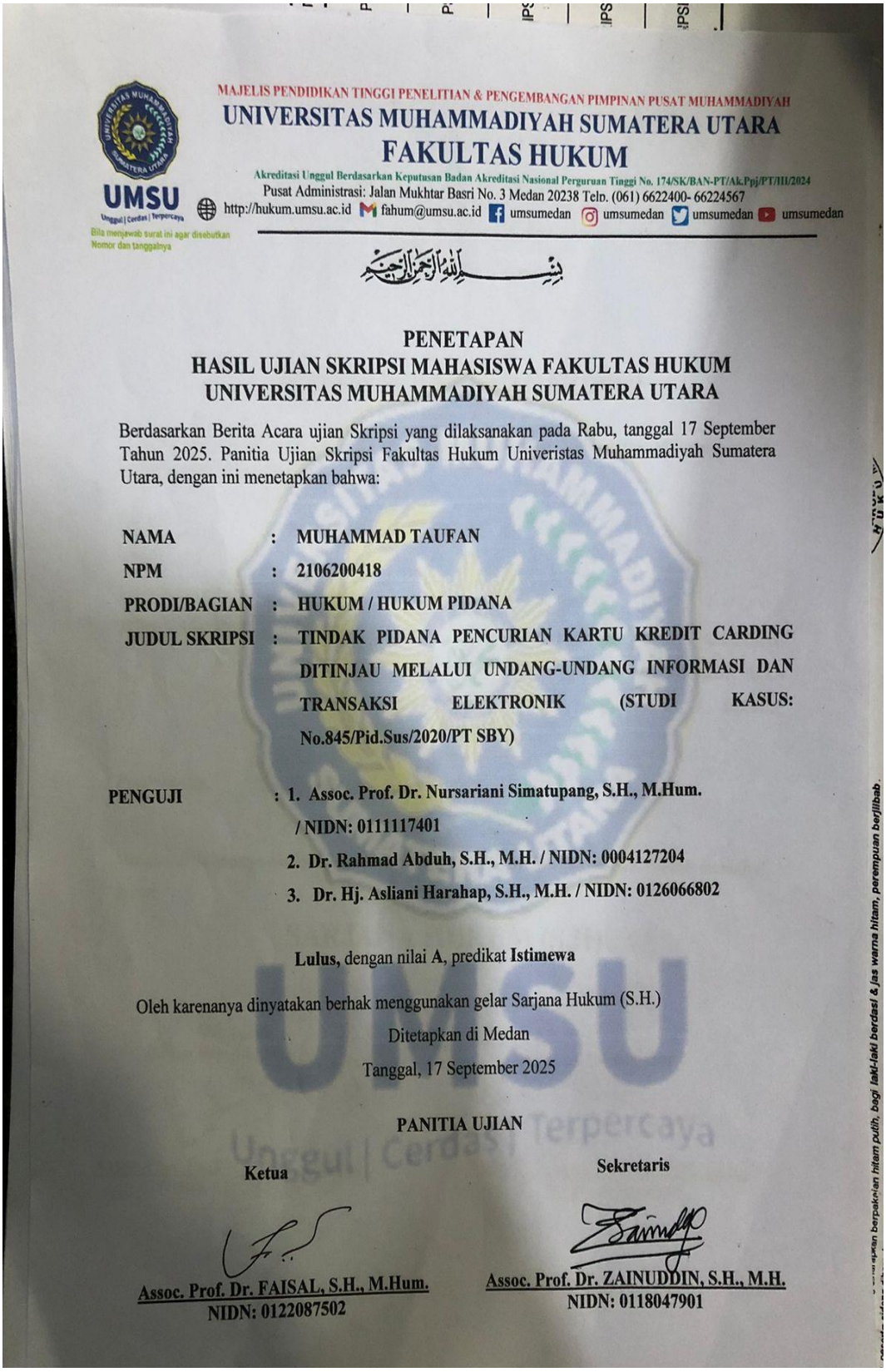
Setelah lulus, dinyatakan berhak dan berwenang mendapatkan gelar Sarjana Hukum (SH) dalam Bagian Hukum Pidana.

PANITIA UJIAN

Ketua	**Sekretaris**
Assoc. Prof. Dr. FAISAL, S.H., M.Hum.	**Assoc. Prof. Dr. ZAINUDDIN, S.H., M.H.**
NIDN: 0122087502	**NIDN: 0118047901**

ANGGOTA PENGUJI:

1. **Assoc. Prof. Dr. Nursariani Simatupang, S.H., M.Hum.** 1.
2. **Dr. Rahmad Abduh, S.H., M.H.** 2.
3. **Dr. Hj. Asliani Harahap, S.H., M.H.** 3.



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
UMSU Unggul | Cerdas | Terpercaya
Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بسم الله الرحمن الرحيم

PENETAPAN
HASIL UJIAN SKRIPSI MAHASISWA FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

Berdasarkan Berita Acara ujian Skripsi yang dilaksanakan pada Rabu, tanggal 17 September Tahun 2025. Panitia Ujian Skripsi Fakultas Hukum Univeristas Muhammadiyah Sumatera Utara, dengan ini menetapkan bahwa:

NAMA	:	**MUHAMMAD TAUFAN**
NPM	:	**2106200418**
PRODI/BAGIAN	:	**HUKUM / HUKUM PIDANA**
JUDUL SKRIPSI	:	**TINDAK PIDANA PENCURIAN KARTU KREDIT CARDING DITINJAU MELALUI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: No.845/Pid.Sus/2020/PT SBY)**
PENGUJI	:	**1. Assoc. Prof. Dr. Nursariani Simatupang, S.H., M.Hum. / NIDN: 0111117401**
		2. Dr. Rahmad Abduh, S.H., M.H. / NIDN: 0004127204
		3. Dr. Hj. Asliani Harahap, S.H., M.H. / NIDN: 0126066802

Lulus, dengan nilai **A**, predikat **Istimewa**

Oleh karenanya dinyatakan berhak menggunakan gelar Sarjana Hukum (S.H.)

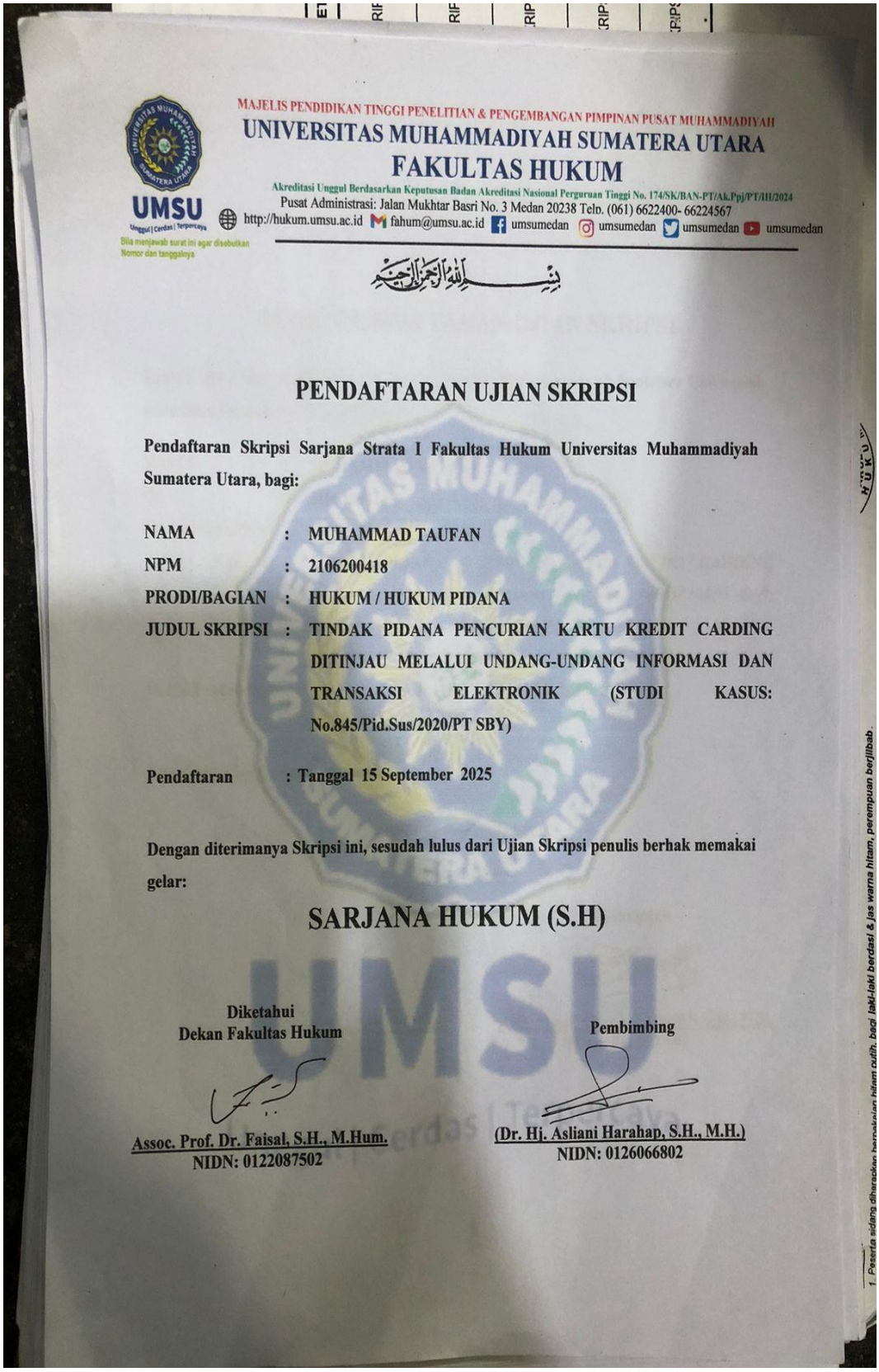
Ditetapkan di Medan

Tanggal, 17 September 2025

PANITIA UJIAN

Ketua	**Sekretaris**
Assoc. Prof. Dr. FAISAL, S.H., M.Hum.	**Assoc. Prof. Dr. ZAINUDDIN, S.H., M.H.**
NIDN: 0122087502	**NIDN: 0118047901**

Peserta ujian berpakaian hitam putih, bagi laki-laki berdasi & jas warna hitam, perempuan berjilbab.



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
UMSU Unggul | Cerdas | Terpercaya
Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بسم الله الرحمن الرحيم

PENDAFTARAN UJIAN SKRIPSI

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

NAMA	:	**MUHAMMAD TAUFAN**
NPM	:	**2106200418**
PRODI/BAGIAN	:	**HUKUM / HUKUM PIDANA**
JUDUL SKRIPSI	:	**TINDAK PIDANA PENCURIAN KARTU KREDIT CARDING DITINJAU MELALUI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: No.845/Pid.Sus/2020/PT SBY)**
Pendaftaran	:	**Tanggal 15 September 2025**

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

SARJANA HUKUM (S.H)

Diketahui	**Pembimbing**
Dekan Fakultas Hukum	
Assoc. Prof. Dr. Faisal, S.H., M.Hum.	**(Dr. Hj. Asliani Harahap, S.H., M.H.)**
NIDN: 0122087502	**NIDN: 0126066802**

1. Peserta sidang diharapkan berpakaian hitam putih, bagi laki-laki berdasi & jas warna hitam, perempuan berjilbab.

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS HUKUM

Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567

http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

UMSU Unggul | Cerdas | Terpercaya

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بسم الله الرحمن الرحيم

BUKTI PENDAFTARAN UJIAN SKRIPSI

Panitia Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara telah menerima Pendaftaran Ujian Skripsi:

NAMA	:	**MUHAMMAD TAUFAN**
NPM	:	**2106200418**
PRODI/BAGIAN	:	**HUKUM / HUKUM PIDANA**
JUDUL SKRIPSI	:	**TINDAK PIDANA PENCURIAN KARTU KREDIT CARDING DITINJAU MELALUI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: NO.845/PID.SUS/2020/PT SBY)**
Dosen Pembimbing	:	**Assoc. Prof. Dr. RAHMAT RAMADHANI, S.H., M.H. / NIDN: 0111088002**

Selanjutnya layak untuk diujikan.

Medan, 02 September 2025

Panitia Ujian

Ketua	**Sekretaris**
Assoc. Prof. Dr. FAISAL, S.H., M.Hum.	**Assoc. Prof. Dr. ZAINUDDIN, S.H., M.H.**
NIDN: 0122087502	**NIDN: 0118047901**

MAJELIS PENDIDIKAN TINGGI MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6624567 Fax. (061) 6625474
Website : http://www.umsu.ac.id http://www.fahum.umsu.ac.id E-mail : rektor@umsu.ac.id fahum@umsu.ac.id

Bila menjawab surat ini, agar disebutkan
Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA	:	**MUHAMMAD TAUFAN**
NPM	:	**2106200418**
PRODI/BAGIAN	:	**HUKUM/ PIDANA**
JUDUL SKRIPSI	:	**TINDAK PIDANA PENCURIAN KARTU KREDIT CARDING MELALUI MEDIA ELEKTRONIK DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: No.845/Pid.Sus/2020/PT SBY)**

Disetujui Untuk Disampaikan Kepada
Panitia Ujian Skripsi

Medan, September 2025

Pembimbing

Dr. Hj. Asliani Harahap, S.H., M.H
NIDN. 0126066802

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 1913/SK/BAN-PT/Ak.KP/PT/X1/2022
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بسم الله الرحمن الرحيم

PERNYATAAN KEASLIAN SKRIPSI

Saya saya bertanda tangan di bawah ini:

NAMA	:	**MUHAMMAD TAUFAN**
NPM	:	**2106200418**
PRODI/BAGIAN	:	**HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI	:	**TINDAK PIDANA PENCURIAN KARTU KREDIT *CARDING* DITINJAU MELALUI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: No.845/Pid.Sus/ 2020/PT SBY)**

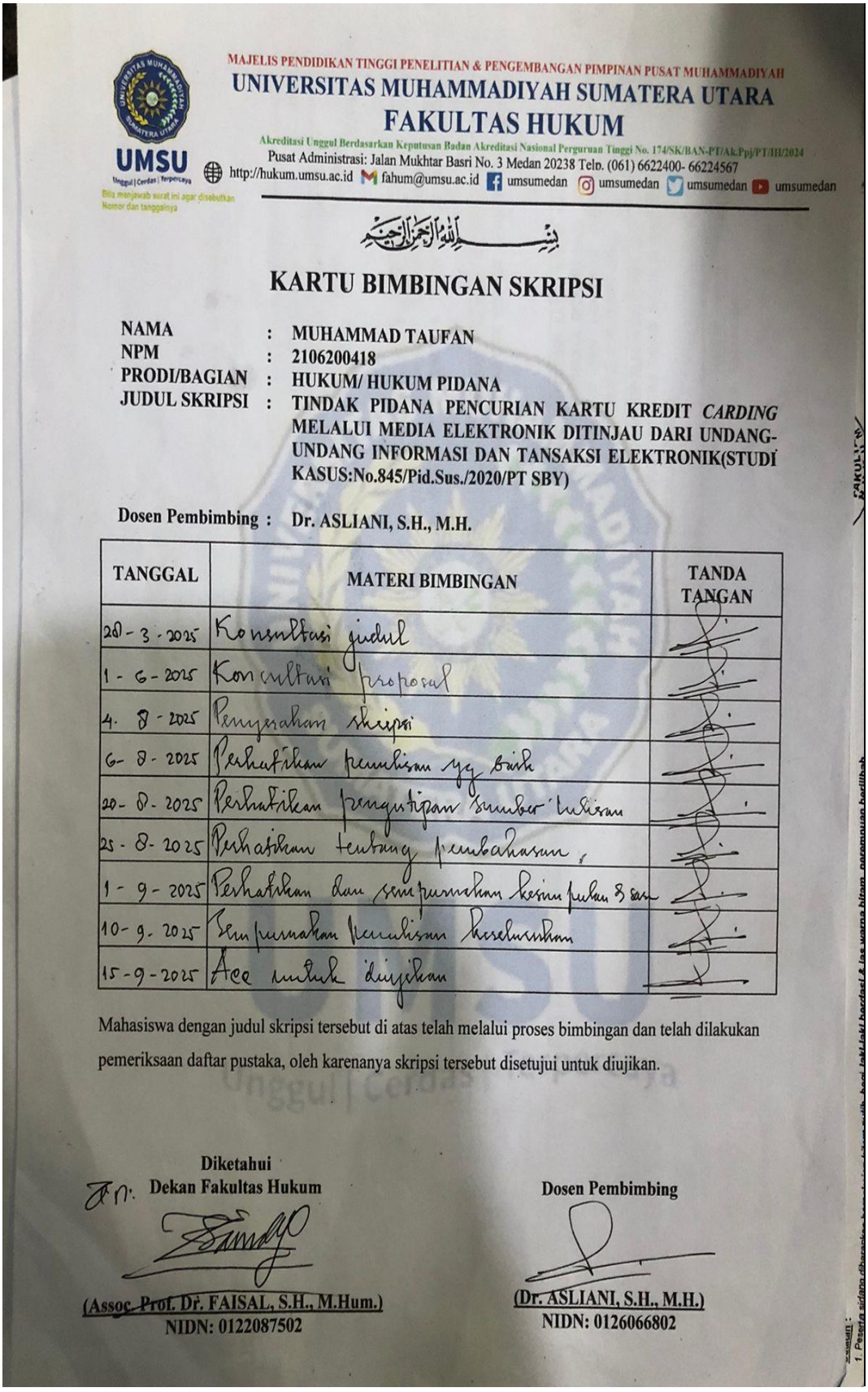
Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis, secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

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

Medan, September 2023
Saya yang menyatakan

METERAI TEMPEL
EFD2ANX084334322

Muhammad Taufan



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
UMSU Unggul | Cerdas | Terpercaya
Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بسم الله الرحمن الرحيم

KARTU BIMBINGAN SKRIPSI

NAMA : MUHAMMAD TAUFAN
NPM : 2106200418
PRODI/BAGIAN : HUKUM/ HUKUM PIDANA
JUDUL SKRIPSI : TINDAK PIDANA PENCURIAN KARTU KREDIT *CARDING* MELALUI MEDIA ELEKTRONIK DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TANSAKSI ELEKTRONIK(STUDI KASUS:No.845/Pid.Sus./2020/PT SBY)

Dosen Pembimbing : Dr. ASLIANI, S.H., M.H.

TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
20-3-2025	Konsultasi judul	
1-6-2025	Konsultasi proposal	
4-8-2025	Penyerahan skripsi	
6-8-2025	Perbaikan penulisan yg baik	
20-8-2025	Perbaikan penguttipan sumber tulisan	
25-8-2025	Perbaikan tentang pembahasan	
1-9-2025	Perbaikan dan penyempurnaan kesimpulan & saran	
10-9-2025	Penyempurnaan penulisan keseluruhan	
15-9-2025	Acc untuk diujikan	

Mahasiswa dengan judul skripsi tersebut di atas telah melalui proses bimbingan dan telah dilakukan pemeriksaan daftar pustaka, oleh karenanya skripsi tersebut disetujui untuk diujikan.

Diketahui
Dekan Fakultas Hukum

(Assoc. Prof. Dr. FAISAL, S.H., M.Hum.)
NIDN: 0122087502

Dosen Pembimbing

(Dr. ASLIANI, S.H., M.H.)
NIDN: 0126066802

Rahmat dan karunia... penulis panjatkan ... barakatuh

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

UMSU
Unggul | Cerdas | Terpercaya

UNDANGAN UJIAN TUGAS AKHIR

Nomor : 1813/II.3.AU/UMSU-06/F/2025

Prog. Studi : Hukum
Tempat : Ruang Sidang Fakultas Hukum UMSU
Jl. Kapten Mukhtar Basri No.03 Telp. (061) 6624567

Hari/Tanggal : **RABU, 17 SEPTEMBER 2025**
Waktu : **08.30 - 12.00**

NO	NAMA/NPM	DOSEN PENGUJI TUGAS AKHIR		JUDUL TUGAS AKHIR	BAGIAN	KET
		PEMBIMBING	PENGUJI UTAMA			
11	RIDHO DILO PERSADA GINTING 2106200038 217-SH-2025	1 TAUFIK HIDAYAT LUBIS, S.S., S.H., M.H.	1 Dr. RACHMAD ABDUH, S.H., M.H. 2 Dr. TENGKU ERWINSYAHBANA, S.H., M.Hum.	ANALISIS PERJANJIAN SEWA MENYEWA SECARA LISAN: KEPERCAYAAN MENJADI DASAR TIMBULNYA KESEPAKATAN	HUKUM PERDATA	SKRIP
12	ALDA TRI AQIL ULLAYYA LUBIS 2106200450 217-SH-2025	1 M. IQBAL, S.Ag., M.H.	1 Dr. GUNTUR RAMBEY, S.H., M.H. 2 TAUFIK HIDAYAT LUBIS, S.S., S.H., M.H.	KEPATUHAN HUKUM PELAKU INDUSTRI RUMAH TANGGA PANGAN DI KELURAHAN SIMARITO TERHADAP PERATURAN BPOM NOMOR 4 TAHUN 2024 DI KOTA PEMATANGSIANTAR	HUKUM BISNIS	SKRIPS
13	EKA SYAHPUTRA 2006200491 218-SH-2025	1 BENITO ASDHIE KODIYAT MS., S.H., M.H.	1 Assoc. Prof. Dr. FARID WAJDI, S.H., M.Hum. 2 M. IQBAL, S.Ag., M.H.	PERTANGGUNG JAWABAN KEUANGAN NEGARA AKIBAT MENTERI RANGKAP JABATAN SEBAGAI KETUA PARTAI POLITIK	HUKUM TATA NEGARA	SKRIPS
14	MUHAMMAD TAUFAN 2106200418 219-SH-2025	1 Dr. Hj. ASLIANI HARAHAP, S.H., M.H.	1 Assoc. Prof. Dr. NURSARIANI SIMATUPANG, S.H., M.Hum. 2 Assoc. Prof. Dr. RAHMAT RAMADHANI, S.H., M.H.	TINDAK PIDANA PENCURIAN KARTU KREDIT CARDING MELALUI MEDIA ELEKTRONIK DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS: NO.845/PID.SUS/2020/PT.SBY)	HUKUM PIDANA	SKRIPS
15	SAKTI RIZKY FAUZI HARAHAP 2106200061 220-SH-2025	1 Assoc. Prof. Dr. RAHMAT RAMADHANI, S.H., M.H.	1 PADIAN ADI SALAMAT SIREGAR, S.H., M.H. 2 BENITO ASDHIE KODIYAT MS., S.H., M.H.	PROSES MEDIASI PENYELESAIAN SENGKETA AHLI WARIS HAK ATAS TANAH (STUDI DI KANTOR BPN MANDAILING NATAL)	HUKUM ACARA	SKRIPS

Medan, 24 Rabi'ul Awwal 1447 H
16 September 2025 M

Disetujui Oleh:
Rektor

Prof. Dr. MUHAMMAD ARIFIN, H., S.H., M.Hum.

Ketua

Dr. FAISAL, S.H., M.Hum.

PANITIA UJIAN

Sekretaris

Dr. ZAINUDDIN, S.H., M.H.

Catatan :
1. Peserta sidang diharapkan berpakaian hitam putih, bagi ***laki-laki berdasi & jas warna hitam, perempuan berjilbab***.
2. peserta sidang diharapkan ***hadir 30 menit sebelum acara dimulai***, bila terlambat sidang yang bersangkutan ditunda.
3. Bagi penguji yang tidak hadir pada saat sidang berlangsung, kedudukannya akan diganti

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis panjatkan kehadiran Allah SWT, atas limpahan Rahmat dan karunianya kepada hambanya serta telah memberikan nikmat dan petunjuknya kepada penulis untuk dapat menyelesaikan penulisan skripsi ini. Shalawat beriringkan salam tak lupa penulis berikan kepada junjungan umat Nabi Muhammad SAW. Yang merupakan salah satu syarat yang harus dipenuhi untuk menempuh tingkat Strata-1 Hukum pada Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Skripsi Ini Berjudul: "**Tindak Pidana Pencurian Kartu Kredit Carding Melalui Media Elektronik Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik (Studi Kasus: No.845/Pid.Sus/2020/Pt Sby)**.

Penulis sadar bahwa Skripsi ini tidak akan selesai tanpa adanya bantuan, perhatian dan kasih sayang dari berbagai pihak yang mendukung pembuatan Skripsi ini , baik secara materil yang telah diberikan dalam penyelesaian Skripsi ini. Ucapan Terima kasih setinggi tingginya dengan rasa hormat dan penghargaan terdalam penulis sampaikan kepada kedua orang tua penulis yang tersayang dan terhebat dalam segala hal yaitu Ady syahputra dan Hasfidianti yang telah memberikan doa, dan curhahan kasih sayang, nasehat, perlindungan, pengorbanan, perjuangan, pengajaran, sungguh tidak ada balasan yang bisa melunaskan semua yang telah di berikan. Dan terima kasih juga kepada ibu sambung saya yaitu Tia Arivani dan terima kasih kakak saya Tiara Adyra dan

adik saya Tisya Adiba. Semoga tuhan yang Maha Esa senantiasa melindungi dan memberikan kesehatan dan rezeki yang belimpah.

Selain itu dengan selesainya Skripsi ini, penulis juga ingin mengucapkan terima kasih yang sebesar besarnya kepada:

1. Bapak Prof. Dr. Agussani, M.A.P selaku Rektor Universitas Muhammadiyah Sumatera Utara, atas kesempatan dan segala fasilitas yang telah diberikan, selama saya mengikuti dan menyelesaikan pendidikan Program Sarjana ini.
2. Bapak Dr. Faisal, S.H . M.Hum. selaku Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, atas kesempatan dan fasilitas yang diberikan kepada penulis sehingga dapat menyelesaikan pendidikan program sarjana ini.
3. Bapak Dr. Zainuddin, S.H., M.H selaku Wakil Dekan 1 Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.
4. Ibu Dr. Atikah Rahmi, S.H., M.H. selaku wakil dekan lll Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.
5. Ibu Dr. Muhammad Teguh Syuhada Lubis, S.H., M.H. selaku Kepala bagian Jurusan Hukum Pidana Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, yang telah memberikan masukan, petunjuk dan arahan sejak tahap penyusunan proposal, seminar proposal sampai selesainya skripsi ini.
6. Ibu Dr. Asliani, S.H., M.H. selaku dosen pembimbing yang dengan perhatian telah memberikan dorongan, bimbingan, petunjuk dan saran sejak awal penyusunan Skripsi hingga penulisan skripsi ini.

7. Ibu Dr. Nur Sariani Simatupang, S.H., M.hum. selaku penguji yang telah memberikan masukan dan penilaian yang luar biasa untuk perbaikan penelitian skripsi ini.
8. Seluruh Bapak atau ibu Dosen Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, atas jasa mereka yang selama ini telah memberikan ilmu pengetahuan dan mendidik penulis melalui perkuliahan sehingga dapat menyelesaiakan studi ini.
9. Seluruh Pegawai/staf Biro Fakutas Hukum Universitas Muhammadiyah Sumatera Utara atas kelancaran proses mengurus berkas-berkas.
10. Teruntuk Orang Tua saya terima kasih telah menjadi begian dari hidup saya, berkontribusi banyak selama perkuliahan saya, baik tenaga, waktu, dan lainnya. Selalu menjadi orang yang mendengar keluh kesah saya dan memberi semangat agar pantang menyerah, mungkin ucapan terima kasih tidak akan bisa membalas semua yang telah kalian berikan, bahkan jika saya menggendong kalian keliling dunia pun tidak akan bisa membalas apapun.
11. Teruntuk Keluarga Cakra, Dagole Family, Kids Gangster, Gold Steps, terima kasih untuk segala dukungan, dan semangat menyelesaikan skripsi ini.
12. Termasuk semua yang merasa menjadi teman saya, yang selalu memberikan support, informasi, dan saran yang baik.

Medan, 28 JULI 2025

Penulis,

MUHAMMAD TAUFAN
NPM. 2106200418

ABSTRAK

TINDAK PIDANA PENCURIAN KARTU KREDIT *CARDING* MELALUI MEDIA ELEKTRONIK DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK(STUDI KASUS: NOMOR 845/PID.SUS/2020/PT SBY

MUHAMMAD TAUFAN
NPM. 2106200418

Perkembangan teknologi informasi telah melahirkan bentuk-bentuk kejahatan baru yang tidak lagi terbatas pada ruang fisik, salah satunya adalah *Carding* atau pencurian data kartu kredit untuk kepentingan transaksi ilegal. Penelitian ini membahas tanggung jawab hukum terhadap pelaku *Carding* ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) melalui studi kasus Putusan Nomor 845/Pid.Sus/2020/PT SBY, dengan fokus pada kelemahan hukum yang menyebabkan rendahnya efek jera dan ketidakadilan dalam pemidanaan.

Pertanggungjawaban pidana diterapkan terhadap pelaku *Carding* serta apa saja kendala yang dihadapi sistem hukum dalam menanggulangi kejahatan tersebut. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan kasus dan peraturan perundang-undangan, serta analisis kualitatif terhadap isi putusan pengadilan dan ketentuan dalam UU ITE dan KUHP. Hasil kajian menunjukkan bahwa peran terdakwa sebagai fasilitator transaksi data kartu kredit hasil kejahatan tidak dibarengi dengan penjatuhan hukuman yang setimpal, yaitu hanya delapan bulan kurungan. Hal ini mencerminkan bahwa UU ITE belum memiliki kekuatan normatif dan sanksi pidana yang efektif dalam menjerat pelaku kejahatan siber secara komprehensif. Selain itu, kendala seperti lemahnya integrasi hukum antara UU ITE dan KUHP, minimnya pengakuan terhadap nilai ekonomi data pribadi sebagai objek pencurian, serta keterbatasan alat pembuktian digital, menjadi hambatan utama dalam proses pertanggungjawaban pidana. Kesimpulan dari penelitian ini adalah bahwa sistem hukum pidana Indonesia belum sepenuhnya mampu merespon.

Cyber crime masih hangat diperdebatkan di kalangan sarjana hukum. Ini karena bentuk kejahatan ini relatif baru. Hukum pidana positif (KUHP dan KUHAP) telah dikritik dan dipertahankan karena kemampuannya menangani kejahatan ini. Penjahat dunia maya akan ditangkap oleh penegak hukum. *Cyber crime* masih tertangkap berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP), terutama yang memenuhi kriteria pasal-pasal tipikal KUHP. Ketika produk ini dianggap tidak cukup untuk mencegah berbagai bentuk kejahatan *online*, banyak instrumen hukum pidana di luar KUHP dapat digunakan untuk menyelesaikan kejahatan melalui penerapan teknologi ini. Instrumen-instrumen ini mencakup pendekatan yang berbeda terhadap undang-undang hukum yang berbeda.

Kata Kunci: UU ITE, Pertanggungjawaban Pidana, *Carding*, *Cyber crime*

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang

Era digital saat ini menjadikan keseluruhan tugas dalam masyarakat tidak hanya melalui dunia nyata saja, karena perkembangan dari teknologi sendiri menjadikan masyarakat juga hidup dalam dunia internet. Perkembangan yang begitu cepat dari kemajuan teknologi informasi dan komunikasi telah memberikan perubahan baru bagi perilaku masyarakat secara global. Di samping itu, perkembangan teknologi informasi dan komunikasi telah menyebabkan dunia lebih dekar dan menjadi tanpa batas *borderless* dan menyebabkan perubahan sosial secara signifikan berlangsung secara cepat. [1]

Teknologi informasi dan komunikasi mampu memberikan kontribusi yang positif bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia namun terdapat sisi negatif pula yang dihasilkan dari perkembangan teknologi komunikasi dan informasi yakni digunakan sebagai sarana untuk melakukan kejahatan atau perbuatan melawan hukum yang berbasis teknologi komunikasi dan informasi. Teknologi global merupakan bagian dari warna dan sekaligus elemen utama dari globalisasi, karena globalisasi yang esensinya terletak pada konsep "desa dunia" tidaklah akan bisa berjalan dan bergerak mengepakkan sayap sayapnya jika tidak menggunakan kekuatan teknologi. [2]

---

[1] Hendri Diansah, (2022), *Kebijakan Hukum Pidana Terhadap Tindak Pidana Carding, Jurnal Of Criminal*, halaman 16.

[2] Simbolon Elisabeth , (2025), *Globalisasi Dan Identitas : Mencari Keseimbangan Dalam Keragaman Budaya Indonesia*, halaman 356.

Teknologi global adalah nama lain bangunan peradaban dunia yang tidak terpisahkan dari produk kemajuan teknologi. Sehingga globalisasi dapat dilihat dari bagaimana perkembangan kemajuan dari sebuah teknologi yang berdampak pada bagaimana masyarakat memanfaatkan kemajuan teknologi dalam berbagai bidang seperti industri, pendidikan dan perdagangan. Kemajuan teknologi dan industri yang merupakan hasil dari budaya manusia di samping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan dan peradaban manusia itu sendiri. Salah satu bentuk positif dalam perkembangan teknologi berada dalam sektor keuangan terutama di Indonesia, dimana saat ini masyarakat dipermudah dengan adanya bermacam kebijakan terbaru dan penciptaan berbasis teknologi oleh perbankan yang bisa diakses melalui *smartphone* yang sering digunakan masyarakat sehari-hari.

Perkembangan itu menghadirkan teknologi yang bisa membantu aktivitas transaksi keuangan dalam hal ini bank. Seperti melakukan transaksi pengiriman uang sekarang tidak harus pergi ke atm atau menggunakan cara konvensional, namun dengan kehadiran jaringan internet memberikan kemudahan pada nasabah bank untuk melakukan transaksi keuangan dengan cara *internet banking* atau *m-banking*, sehingga bisa dilakukan dengan mengoperasikan aplikasi *m-banking* yang ada di *smartphone* nasabah bank. [3] Dengan adanya modernisasi di bidang transaksi keuangan maka membuka pula potensi kejahatan modern yang bisa

[3] Erwin Taroreh, (2024), *Tinjauan Yuridis Terhadap Pelaku Peretasan Kartu Kredit Carding Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,* halaman 8879.

menyasar sistem transaksi keuangan. Struktur bisnis dengan teknologi yang memakai kartu angsuran (*credit card*) bisa diamati dalam bentuk bisnis elektronik (*electronic transaction*) lewat mesin Anjungan Tunai Mandiri (*Automated Teller Machine*), memakai telepon genggam (*phone banking*), jaringan internet perbankan (*internet banking*), serta lain serupanya selaku wujud terkini *delivery channel* memodernisasi tiap bisnis.

Electronic-based Uang Elektronik *(Electronic Money*) didefinisikan selaku perlengkapan pembayaran yang penuhi unsur-unsur ialah diterbitkan atas bawah angka duit yang disetor terlebih dulu pada pencetak, angka duit ditaruh dengan cara elektronik dalam sesuatu alat semacam *server* ataupun *chip,* serta angka duit elektronik yang di mengurus oleh pencetak bukan ialah dana begitu juga diartikan dalam hukum yang menata hal perbankan. Instrumen pembayaran *electronic based* terdiri dari *e-money*, *internet banking*, *mobile banking*, serta *electronic mall*. Bahwa revolusi sistem transaksi nyata-nyata telah terjadi dalam kurun waktu kurang dari 50 tahun belakangan, perubahan tersebut dari *paper based* menjadi *card based*, kemudian *card based* beralih menjadi *electronic based*. Tentu perubahan tersebut di pengaruhi oleh perkembangan teknologi. Namun jika dilihat secara mendalam revolusi teknologi tersebut memiliki latar belakang yang begitu kuat yaitu upaya untuk meningkatkan efektivitas/atau praktis dalam bertransaksi. Sehingga dalam hal bisnis perusahaan banking dapat menarik minat lebih banyak dari masyarakat yang awalnya tidak tertarik untuk menyimpan uangnya pada

bank, sekarang menjadi tertarik dan tidak ada alasan untuk tidak menyimpan uang pada bank. [4]

Bentuk kejahatan di internet saat ini beragam dan memiliki dampak yang berbeda dalam kultur kehidupan manusia itu sendiri, Dampak negatif yang dimaksud adalah berkaitan dengan dunia kejahatan. Semakin maju kehidupan masyarakat, maka kejahatan juga ikut semakin maju. Kejahatan juga ikut bagian hasil dari budaya sendiri. Hal ini berarti semakin tinggi tingkat budaya dan modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk sifat dan pelaksanaannya. [5]

Perkembangan jaringan internet memunculkan dampak negatif, sebagaimana dikemukakan oleh Muhammad Anthony Aldiano (2022), dalam jurnalnya ia mengutip perkataan dari Roy Suryo seorang pakar teknologi dan informasi, dalam penelitiannya menyatakan: "Kejahatan *cyber* (*Cyber crime*) kini marak di lima kota besar di Indonesia dan dalam taraf yang cukup memperhatikan serta yang dilakukan oleh para *hacker* yang rata-rata anak muda yang kelihatannya kreatif, tetapi sesungguhnya mereka mencuri nomor kartu kredit melalui internet". [6]

Cyber crime dibagi menjadi 2 kategori, yakni *Cyber crime* dalam pengertian sempit dan dalam pengertian luas. *Cyber crime* dalam pengertian

---

[4] Fakultas Hukum and Universitas Agustus Surabaya,1945, *Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik Pencegahan Kepada Kesalahan Carding*, halaman 66-67.

[5] Kementerian Pendidikan Dan Kebudayaan Badan Pengembangan Dan Pembinaan Bahasa Bacaan Untuk Anak Tingkat SD Kelas 4, 5, Dan 6., "Mengenal media Sosial dan Tak Menyesal"

[6] Muhammad Anthony Aldriano and others, (2022) "*Cyber Crime* Dalam Sudut Pandang Hukum Pidana", Jurnal kewarganegaraan, Jurnal Kewarganegaraan halaman 2169.

sempit adalah kejahatan terhadap sistem komputer, sedangkan *Cyber crime* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer. [7]

Salah satu kejahatan *cyber crime* dengan menggunakan kartu kredit ialah *Carding*. Hal ini sejak tahun 2018 kejahatan yang menggunakan kartu kredit ini mulai marak dan popular di Indonesia terutama di kota-kota besar. Menurut riset *Clear Commerce Inc*, perusahaan teknologi informasi yang berbasis di *Texm,.as*, AS, Indonesia memiliki *carder* terbanyak kedua di dunia setelah Ukraina. Sebanyak 20 persen transaksi melalui internet dari Indonesia adalah hasil *Carding*. Akibatnya, banyak situs belanja *online* yang memblokir IP atau *internet protocol* (alamat komputer internet) asal Indonesia. [8]

Carding adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. Sebutan pelakunya adalah *carder*. Sebutan lain untuk kejahatan jenis ini adalah *cyber fraud* alias penipuan di dunia maya. [9]

Modus kejahatan menggunakan kartu debit/kredit atau *Carding* ini dapat dilakukan melalui berbagai program komputer untuk mencuri, memalsukan atau mendapatkan kartu debit/kredit, bagaimana membuat nomor-nomor kartu debit/kredit palsu, bagaimana menggandakan kartu kartu debit/kredit yang sah, dan bagaimana menggunakan kartu debit/kredit palsu. Termasuk cara-cara

[7] Rian wi Hapsari and Kuncoro Galih Pambayun, (2023) "Ancaman *Cyber Crime* Di Indonesia: Sebuah Tinjauan Pustaka Sistematis", *Jurnal Konstituen*, volume 5.1 halaman 2.

[8] *Ibid.*, halaman 9

[9] S. Nauli Situmeang, 2020, *CYBER LAW, ed. by Anggota IKAPI, Cyber Law*, CV.Cakra, hlm. 27

memperoleh data yang terkait dengan nomor rekening. Hal itu biasanya tanpa sepengetahuan pemegang kartu kredit, *merchant*, bank penerbit kartu debit/kredit sampai akhirnya rekening tersebut digunakan untuk melakukan kejahatan. [10]

Sampai saat ini di Indonesia belum memiliki perangkat hukum yang sesuai untuk mengatur aktivitas manusia di bidang *Cyber*. Tindak pidana *Carding* ini telah berkembang pesat di Indonesia, sementara itu sistem hukum Indonesia adanya celah dan lemahnya sistem pengawasan serta pengaturan dan penegakan hukum dalam tindak kejahatan ini. Salah satu bentuk lemahnya hukum dalam pengawasan Teknologi informasi ada pada putusan 845/Pid.Sus/2020/PT.SBY, seorang pelaku yang berinisial KWM (Terdakwa 1) menjual data diri kredit orang lain di situs penjualan *online* sosial media melalui facebook dengan melelangkan kartu kredit ilegal atas nama Amir Salim yang dibeli oleh pihak terdakwa bernama Choirul Anam yang mana dibeli dari akun Ridho Steven, dalam hal ini sang pemilik kartu kredit ilegal itu melancarkan aksinya dengan menjual hasil perasan terhadap kartu kredit milik orang lain yang didapatkan secara ilegal, KWM dianggap sebagai pihak ketiga karena mereka melakukan transaksi menggunakan rekening milik terdakwa KWM sehingga bisa dikatakan bahwa Choirul Anam adalah Pembeli dan penjualnya adalah Ridho Steven (terdakwa 2) yang mana Terdakwa 2 (berkas terpisah) ini mengambil barang milik KWM yang diniagakan, metode penjualan ini dianggap sebagai *Reselller* yang mana kartu kredit tersebut dapat digunakan di banyak *reseller* (Terdakwa 1). Hasil kerugian yang dimiliki

[10] I. Fikma Edrisy, 2019, *Pengantar Hukum Siber*, KAMILATUN : Sai Wawai Publishing, halaman. 7

sang pemilik kartu kredit atau korban tidak sebanding dengan kerugian yang dialami korban, KWM atau terdakwa 1 hanya di beri hukuman 2 tahun penjara dengan denda senilai Rp30.000.000,00 dan subsidair 4 bulan, lalu terdakwa mengajukan banding karena ia mendapatkan kartu kredit tersebut melalui seorang *hacker* sehingga pemangkasan hukuman oleh pelaku di total menjadi 8 bulan kurungan penjara. Tentu korban tidak terima dengan putusan dari pihak pengadilan, sehingga diajukanlah kasasi oleh pihak korban atas kerugian yang dialami secara materiil dan fisik sehingga putusan akhir dari terdakwa 1 dikenai hukuman kurungan selama 1 tahun penjara. [11]

Jika merujuk ke dalam pasal 30 ayat (1) UU ITE "(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.." Adapun sanksi yang mesti didapatkan adalah denda sebanyak 600 Juta rupiah dengan masa tahanan selama 6 tahun, tentu ini menjadi kesetimpangan atas putusan dari pihak pengadilan dan UU yang berlaku dalam pengaturan UU ITE, kurangnya penjelasan yang signifikan terhadap pengaturan UU ITE terkait permasalahan menjadi pokok utama mengapa putusan dari pihak pengadilan yang telah merugikan orang lain lebih singkat dan mirip dengan putusan pencurian ringan.

Dalam putusan tersebut tentu tidak adil karena dari tindak pidana pencurian memanfaatkan elektronik itu tidak sebanding dengan kerugian yang didapati korban, selain itu pusat dari pembobolan kartu kredit tersebut belum

[11] Mahkamah Agung, *Putusan Nomor 845/PID.SUS/2020/PT SBY*, 2020. hlm 20

ditemukan titik terangnya sehingga masih berkeliaran hingga saat ini, tentu hal ini menjadi evaluasi untuk pihak pemerintah dalam menangani kasus Teknologi informasi dan Elektronik yang saat ini semakin berkembang pesat, bahkan saat ini semakin majunya teknologi tidak akan dapat diketahui apa saja yang akan menjadi tindak pidana melalui elektronik berikutnya yang mana dikarenakan teknologi dan informasi semakin maju dalam kehidupan masyarakat dan tidak dapat dipisahkan.

Sehingga dalam hal ini penulis tertarik untuk membahas terkait **Tindak Pidana Pencurian Kartu Kredit Melalui Media Elektronik *Carding* Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik Studi Kasus No.845/Pid.Sus/2020/PT SBY**.

Dalam pandangan Islam memilih mencuri adalah hal yang keji, hal ini tentu sangat dilarang oleh Allah SWT, sebagaimana firman Allah SWT dalam Q.S Al-Maidah ayat 38 yang berbunyi :

كَسَبَا بِمَا جَزَاۤءًۢ اَيْدِيَهُمَا فَاقْطَعُوْٓا وَالسَّارِقَةُ وَالسَّارِقُ

۝٣٨ حَكِيْمٌ عَزِيْزٌ وَاللّٰهُ ۗ اللّٰهِ مِّنَ نَكَالًا

Terjemahannya :

Laki-laki maupun perempuan yang mencuri, potonglah tangan keduanya sebagai balasan atas perbuatan yang mereka lakukan dan sebagai siksaan dari Allah. Allah Maha perkasa lagi Maha bijaksana

1. Rumusan Masalah

Adapun pada skripsi ini, pokok rumusan masalah yang menjadi fokus adalah :

a. Bagaimana bentuk pencurian kartu kredit *Carding* Media Elektronik Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Studi Kasus No.845/Pid.Sus/2020/PT SBY?

b. Bagaimana tanggung jawab hukum untuk pelaku pencurian kartu kredit *Carding* ditinjau dari Media Elektronik Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik Studi Kasus No.845/Pid.Sus/2020/PT SBY?

c. Bagaimana kendala dalam pertanggungjawaban pidana pencurian kartu kredit *Carding* Studi Kasus No.845/Pid.Sus/2020/PT SBY?

2. Tujuan Penelitian

Setelah melihat rumusan masalah yang telah dibahas, maka tujuan dari penulisan ini adalah:

a. Untuk dapat memahami bentuk pencurian kartu kredit *Carding* Media Elektronik Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Studi Kasus No.845/Pid.Sus/2020/PT SBY.

b. Untuk dapat memahami tanggung jawab hukum untuk pelaku pencurian kartu kredit *Carding* ditinjau dari Media Elektronik Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik Studi Kasus No.845/Pid.Sus/2020/PT SBY

c. Untuk dapat mengetahui kendala dalam pertanggungjawaban pidana pencurian kartu kredit *Carding* Studi Kasus No.845/Pid.Sus/2020/PT SBY.

3. Manfaat Penelitian

Adapun yang menjadi suatu harapan dan tujuan dari hasil penelitian ini yaitu agar dapat memberikan manfaat baik secara teoritis dan secara praktis bagi semua pihak, antara lain sebagai berikut :

a. Secara Teoritis**.**

Penelitian ini memberikan sumbangsih bagi pengembangan teori hukum pidana, khususnya dalam ranah hukum pidana siber *cyber crime,* dengan menelaah bagaimana tindakan *Carding* dikonstruksikan sebagai tindak pidana berdasarkan norma-norma hukum positif yang berlaku di Indonesia. Melalui studi kasus No.845/Pid.Sus/2020/PT SBY.

b. Secara Praktis

Penelitian ini dapat memperkaya literatur akademik di lingkungan universitas, terutama dalam bidang hukum pidana, hukum siber, dan hukum perlindungan data. Hasil penelitian ini dapat digunakan sebagai bahan ajar, referensi perkuliahan, maupun pengembangan kurikulum yang berfokus pada kejahatan digital dan teknologi informasi. Selain itu, universitas dapat memanfaatkan kajian ini sebagai dasar pengembangan program penelitian lanjut atau kerja sama dengan lembaga penegak hukum.

B. Defenisi Operasional

Definisi operasional dalam penelitian ini adalah:

1. Tindak Pidana Pencurian adalah perbuatan atau perkara yang berkaitan dengan mencuri. Menurut Pasal 362 KUHP adalah : "Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau denda paling banyak sembilan ratus rupiah". [12]
2. *Carding* merupakan kejahatan yang memanfaatkan teknologi internet sebagai sarana utama untuk mengakses secara tidak sah suatu sistem sebuah website untuk mendapatkan data-data para nasabah kartu kredit. Tujuannya adalah untuk membelanjakan secara tidak sah kartu kredit yang telah didapatkan ataupun untuk mendapatkan dana milik pemegang kartu kredit tersebut.
3. Media Elektronik merupakan salah satu media masa yang memiliki kekhususan. Kekhususannya terletak pada dukungan elektronika dan teknologi yang menjadi ciri serta kekuatan dari media berbasis elektronik. Media elektronik merupakan media masa yang digandrungi oleh banyak kalangan orang, yang mana melalui media elektronik ini seseorang dapat memperoleh informasi dengan cepat melalui suara dan gambar. Dengan adanya penggunaan media elektronik dalam kehidupan sehari-hari maka

[12] Abd Haris Hamid dkk, 2022, *Hukum Tindak Pidana Pencurian & Kekerasan*, Cetakan I Chakti Pustaka Indonesia, hlm. 5

dapat menunjang dan memenuhi kebutuhan penggunanya sehingga lebih mudah. [13]

a. UU ITE adalah setiap bentuk peraturan perundangan yang diciptakan oleh lembaga yang kompeten dalam pembuatan undang-undang yaitu Dewan Perwakilan Rakyat dan Presiden sebagai kepala pemerintahan atau setiap keputusan tertulis sebagai hasil kerja sama antara pemegang kekuasaan eksekutif dan legislatif yang berisi aturan tingkah laku yang mengikat secara umum mengenai satu atau sekumpulan data elektronik, termasuk tapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data internet* (EDI), surat elektronik (*electronic mail*), telegram, *teleks*, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Pasal 30 Ayat (1) UU ITE berisi (1) "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun." Dikenakan sanksi denda sebanyak 600 Juta rupiah dengan masa tahanan selama 6 tahun

C. Keaslian Penelitian

Berdasarkan pemeriksaan yang telah dilakukan oleh peneliti di perpustakaan Universitas Muhammadiyah Sumatera Utara diketahui bahwa penelitian tentang "Tindak Pidana Pencurian Kartu Kredit Melalui Media

[13] Krista Yitawati, 2017, *Hukum & Teknologi*, Cetakan I Pustaka Iltizam, hlm. 22

Elektronik *Carding* Ditinjau dari Pasal 30 Ayat (1) Undang-Undang Informasi dan Transaksi Elektronik Studi Kasus No.845/Pid.Sus/2020/PT SBY." belum pernah dilakukan penelitian dalam memandang *Carding* yang masih awam ditelinga Sebagian orang. Peneliti mencantumkan karya tulis ilmiah yang temanya hampir sama dengan judul penelitian di atas, tetapi memiliki perbedaan dalam perumusan masalah yang dibahas yaitu:

1. Skripsi Khairunnisa Salsabila mahasiswi Fakultas Syariah dan Hukum Universitas Islam Negeri Sultan Syarif Kasim Riau Program Studi strata 1 Hukum tahun 2022 yang berjudul Analisis Yuridis Undang-Undang Nomor 19 Tahun 2016 dalam Kejahatan *Carding* Transaksi Jual Beli *Online*.
2. Skripsi Akhdiyat Mubaraq Mahasiswa Fakultas Hukum Universitas Hasanuddin Program strata 1 Hukum tahun 2021 yang berjudul Tinjauan Yuridis Tindak Pidana Peretasan Kartu Kredit Melalui Internet atau *Carding* Terhadap Warga Negara Asing.
3. Skripsi Ardan Farwansyah Mahasiswa Fakultas Hukum Universitas Islam Riau Profram Starata 1 Hukum Tahun 2018 yang berjudul Penegakan Hukum Tindak Pidana Pencurian Data Kartu Kredit (*Carding)* Di Wilayah Hukum Kepolisian Daerah Riau.

Berdasarkan ketiga skripsi *di atas* dengan skripsi ini memiliki persamaan yaitu sama-sama membahas mengenai tindak pidana *Carding* sebagai bentuk kejahatan siber yang melibatkan penggunaan kartu kredit secara ilegal. Dasar hukum yang digunakan juga serupa, yakni mengacu pada Undang-Undang Nomor

19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai kerangka regulasi utama.

Perbedaan fokus dan pendekatan kajian. Skripsi Khairunnisa Salsabila lebih menekankan pada kelemahan regulasi UU ITE dalam menjerat pelaku Carding, khususnya dalam konteks transaksi jual beli online, sehingga mendorong perlunya regulasi khusus yang lebih spesifik dan pedoman teknis terkait kejahatan siber. Sementara itu, skripsi Akhdiyat Mubaraq berbeda karena mengambil studi kasus konkret melalui Putusan Nomor 102/Pid.Sus/2020/PN.Wns mengenai Carding terhadap warga negara asing. Sedangkan skripsi ini cenderung memiliki kedekatan dengan Khairunnisa karena sama-sama fokus pada analisis normatif UU ITE dalam *Carding* jual beli *online*, tetapi penelitian ini lebih menyoroti aspek penerapan hukum positif di Indonesia, khususnya terkait kendala aparat penegak hukum serta perlunya optimalisasi dalam praktik.

Sedangkan skripsi Ardan Farwansyah lebih memfokuskan kepenegakan mengenai Tindak Pidana Pencurian Kartu Kredit (*Carding*) terutama di daerah Riau , serta tidak membahas putusan apapun.

D. Metode Penelitian

Menurut Sugiyono, metode penelitian adalah cara ilmiah untuk mendapatkan data yang valid, dengan tujuan menemukan, mengembangkan, dan

mendemonstrasikan pengetahuan tertentu, yang pada gilirannya dapat digunakan untuk memahami, memecahkan, dan mengantisipasi masalah. [14]

1. Jenis Penelitian

Jenis Penelitian dan pendekatan ini adalah yuridis normatif yaitu penelitian hukum doktrinal yang mengacu pada norma – norma hukum. Penelitian hukum normatif disebut juga penelitian hukum doktrinal, dimana hukum dikonsepkan sebagai apa yang tertuliskan Undang Undang (*law in books*), dan penelitian terhadap sistematika hukum dapat dilakukan pada Undang Undang atau hukum tertulis.

2. Sifat Penelitian

Penelitian merupakan alat yang digunakan manusia untuk memperkuat, membina, dan mengembangkan ilmu pengetahuan. Sebuah penelitian telah dimulai ketika seseorang mencoba untuk memecahkan masalah, secara sistematis, dengan metode-metode dan teknik-teknik tertentu secara ilmiah. Berdasarkan tujuan Penelitian Hukum tersebut, maka kecenderungan sifat penelitian yang digunakan adalah Deskriptif. Sifat Penelitian Deskriptif adalah penelitian yang hanya semata mata melukiskan keadaan obyek atau peristiwanya tanpa suatu maksud untuk mengambil kesimpulan kesimpulan yang berlaku secara umum.

[14] Jonaedi Efendy, Johnny Ibrahim, 2018, *Metode Penelitian Hukum*, Depok: Prenamedia Group, halaman 3

3. Pendekatan Penelitian

Pendekatan pada penelitian ini menggunakan metode pendekatan peraturan perundang-undangan (*statue approach*) yaitu dengan mengulas peraturan perundang-undangan yang berhubungan dengan topik yang dijadikan pembahasan pada penelitian ini, kemudian penulis juga menggunakan metode pendekatan Pendekatan (*Case Approach*) yaitu metode penelitian atau analisis hukum yang dilakukan dengan cara menelaah kasus hukum yang relevan untuk memahami bagaimana hukum diterapkan dalam praktik. Pendekatan normatif dipilih karena permasalahan yang diteliti berkaitan langsung dengan penafsiran ketentuan Pasal 30 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, dalam hubungannya dengan tindak pidana *Carding* atau pencurian kartu kredit melalui media elektronik. Melalui pendekatan ini, hukum dipahami sebagai kaidah normatif yang mengatur perilaku manusia dan berfungsi sebagai sarana untuk mencapai ketertiban dan keadilan. Penelitian normatif tidak berangkat dari realitas sosial, melainkan dari sistem hukum itu sendiri, termasuk studi atas putusan pengadilan yang menjadi objek kajian, yaitu Putusan No. 845/Pid.Sus/2020/PT SBY.

Pendekatan ini bertujuan untuk mengkaji kejelasan, konsistensi, dan penerapan hukum positif dalam menyikapi kejahatan siber yang bersifat teknologi dan lintas batas. Dengan demikian, analisis difokuskan pada interpretasi hukum, konstruksi yuridis, dan penerapan norma terhadap kasus konkret. Pendekatan normatif juga memungkinkan peneliti untuk menyusun argumentasi hukum

berdasarkan logika normatif dan prinsip-prinsip keadilan, bukan berdasarkan data empiris. Oleh sebab itu, penelitian ini berupaya menjawab rumusan masalah melalui studi literatur terhadap peraturan perundang-undangan yang berlaku, doktrin dari para sarjana hukum, dan analisis yuridis terhadap putusan pengadilan. Keseluruhan pendekatan ini sejalan dengan karakter penelitian hukum sebagai studi preskriptif dan aplikatif, yang bertujuan menjelaskan bagaimana seharusnya hukum ditegakkan dalam perkara pencurian data kartu kredit melalui sistem elektronik.

4. Sumber Data

Sumber Data adalah subjek dari mana data diperoleh. Hal ini, tidak bersumber dari satu saja melainkan dari beberapa sumber, di antaranya:

a. Data Hukum yang bersumber dari Hukum Islam Al-Qur'an yang di maksud dengan sumber dari Hukum Islam, dalam rangka menanamkan catur Dharma perguruan tinggi Muhammadiyah yang salah satunya "menanamkan dan mengamalkan nilai-nilai ajaran al-islam dan kemuhammadiyahan".

b. Data Sekunder yaitu dengan cara pengumpulan informasi yang sudah ada yang dijadikan referensi oleh penulis untuk menulis proposal ini, di antaranya sebagai berikut:

    1) Bahan buku Primer yang digunakan untuk melengkapi penelitian ini yaitu, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE). Judi *online* juga diatur dalam Undang-

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan UU Nomor 19 Tahun 2016 dan yang paling utama adalah KUHP.

2) Bahan Buku sekunder yang digunakan untuk melengkapi penelitian ini yaitu, artikel, jurnal, agar memperoleh informasi yang sangat berkaitan dengan penelitian yang diambil.

3) Bahan Buku Tersier yaitu, bahan yang dapat memberikan petunjuk, seperti kamus bahasa Indonesia untuk mengartikan pengertian atau istilah yang sulit dimengerti, pedoman skripsi untuk melihat cara pembuatan skripsi yang baik dan benar.

5. Alat Pengumpulan Data

Data yang diperoleh dalam penelitian ini dari data sekunder menggunakan alat pengumpul data berupa studi kepustakaan (*library research*) yang dilakukan melalui penelusuran literatur yang dilakukan di Perpustakaan Universitas Muhammadiyah Sumatera Utara, mengunjungi toko-toko buku guna menghimpun data sekunder seperti buku-buku hukum, dokumen, jurnal ilmiah, peraturan Perundang-undangan, dan lain sebagainya yang dibutuhkan dalam penelitian. Serta melakukan dengan cara searching melalui media internet guna menghimpun data sekunder yang dibutuhkan dalam penelitian dimaksud

6. Analisis Data

Analisis data adalah kegiatan memfokuskan, mengabstraksikan data secara sistematis dan rasional untuk memberikan bahan jawaban terhadap permasalahan. Analisis data yang dilakukan dengan melakukan studi kepustakaan (*library research*). Sehingga, dapat diambil pemecahan masalah yang akan diuraikan dengan menggunakan analisis kualitatif yakni pemilihan teori -teori, asas-asas, norma-norma, doktrin dan pasal-pasal di dalam UU yang relevan yang akan dibahas dalam penelitian ini..[15]

[15] I Made Pasek Diantha. 2016. *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*. Jakarta : Prenanda Media Group, halaman 152.

BAB II

TINJAUAN PUSTAKA

A. Tindak Pidana Pencurian

Tindak pidana pencurian sendiri telah banyak dan umum terjadi di tengah masyarakat Indonesia ini, dan bisa dibilang sangat meresahkan masyarakat karena menimbulkan kerugian bermacam-macam. Di dalam Kitab Undang-undang Hukum Pidana, pada Pasal 362 pencurian diartikan dengan "Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum…". Dari kutipan tersebut dapat diperjelas bahwa arti dari pencurian itu ialah seseorang yang mengambil barang milik orang lain tanpa sepengetahuan pemiliknya dan seseorang ini sebelumnya telah memiliki niatan untuk memiliki dengan cara melawan hukum. Pasal ini menjelaskan pencurian dalam golongan pencurian biasa. Yang dimaksudkan barang dalam kutipan tersebut ialah semua benda yang berwujud, seperti: uang, perhiasan, baju, termasuk binatang dan sebagainya. Dan ada benda yang tak berwujud, seperti aliran listrik yang disalurkan melalui kawat yang dilakukan tanpa izin dari pemilik aliran listrik yang diambil tadi. Dalam kutipan Pasal yang telah dijelaskan *di atas*, pencurian ini mempunyai beberapa unsur yaitu unsur obyektif dan unsur subyektif.

1. Unsur Obyektif, terdiri dari :
    a. Perbuatan (mengambil)
    b. Obyeknya yaitu suatu benda

c. Unsur keadaan yang melekat pada benda (benda tersebut statusnya seluruhnya atau sebagian milik oranglain)

2. Unsur Subyektif, terdiri dari :

a. Adanya maksud (niat)

b. Yang ditujukan untuk “memiliki”

c. Dengan melawan hukum (hal ini merujuk pada suatu perbuatan tersebut dapat dikatakan pencurian apabila telah memenuhi seluruh unsur-unsur yang telah di sebutkan. [16]

Jenis-jenis tindak pidana secara umum dapat diklasifikasikan berdasarkan beberapa kategori seperti :

1. Pencurian Biasa

Pencurian jenis ini dimuat dalam KUHP pasal 362 yang berbunyi Pasal 362 “Barang siapa mengambil sesuatu barang, yang sama sekali atau sebagian termasuk kepunyaan orang lain, dengan maksud akan memiliki barang itu dengan melawan hak, dihukum, karena pencurian, dengan hukuman penjara selama-lamanya lima tahun; atau denda sebanyak-banyaknya Rp.900”. Pencurian jenis ini merupakan bentuk pokok dalam hal kejahatan pencurian. Dengan memperhatikan bunyi pasal *di atas* maka yang diancam dan dilanggar dalam kejahatan tersebut ialah perbuatan ‘mengambil’ yang maksudnya mengambil sesuatu yang bukan miliknya untuk dimiliki secara melawan hak orang lain. Dalam hal melawan disini

[16] R. Prayuda Saputra. (2019). "Perkembangan Tindak Pidana Pencurian Di Indonesia". Jurnal Pahlawan. volume 2.2. halaman 45.

sangat diperlukan karena jika seseorang dikatakan pencuri hanya jika dia melakukan perbuatan itu tanpa seizin pemiliknya karena jika dilakukan dengan seizin pemilik bukan termasuk pencurian meskipun sama-sama bermaksud ingin memilikinya.

2. Pencurian Ringan

Pencurian ini dimuat pada pasal 364 KUHP yang berbunyi “Perbuatan yang diterangkan dalam Pasal 362 dan Pasal 363 butir 4, begitu pun perbuatan yang diterangkan dalam Pasal 363 butir 5, apabila tidak dilakukan dalam sebuah rumah atau pekarangan yang tertutup yang ada rumahnya, jika harga barang yang dicuri tidak lebih dari dua puluh lima rupiah, dikenai karena pencurian ringan dengan pidana penjara paling lama tiga bulan atau denda paling banyak dua ratus lima puluh rupiah". Pencurian ini memiliki unsur yang bentuknya pokok seperti pasal 362, ditambah dengan unsur lainnya yang meringankan ancaman mendapat pidananya menjadi ringan seperti contohnya jika seseorang melakukan pencurian dengan berbagai macam cara seperti dilakukan dua orang atau lebih, berusaha masuk dengan melakukan pembongkaran, pengerusakan, atau membuat kunci palsu, namun dengan syarat tidak dilakukan di dalam tempat kediaman atau rumah; dan nilai dari benda yang dicuri tidak lebih dari dua puluh lima rupiah maka kejahatan itu dianggap pencurian ringan. [17]

[17] *Ibid.*, halaman 45

3. Pencurian dengan pemberatan

Pasal yang mengaturnya ialah pasal 363 yang berbunyi (1) Diancam dengan pidana penjara paling lama tujuh tahun:

a. Pecurian ternak.
b. Pencurian pada waktu kebakaran, letusan banjir, gempa bumi, atau gempa laut, gunung meletus, kapal karam, kapal terdampar, kecelakaan kereta api. Huru-hara, pemberontakan atau banyak perang.
c. Pencurian waktu malam dalam sebuah rumah atau pekarangan tertutup yang ada rumahnya, yang dilakukan oleh orang yang adanya di situ dan diketahui atau tidak dikehendaki oleh yang berhak.
d. Pencurian yang dilakukan oleh dua orang atau lebih dengan bersekutu.
e. Pencurian yang untuk masuk ke tempat melakukan kejahatan atau untuk sampai ke barang yang diambilnya, dilakukan dengan merusak, memotong atau memanjat dengan memakai anak kunci palsu atau pakaian palsu.

Jika pencurian yang diterangkan dalam butir 3 disertai dengan salah satu tersebut butir 4 dan 5, maka dikenakan pidana paling lama sembilan tahun.”

Dengan memperhatikan pasal di atas yang dimaksud pencurian berat atau pemberatan adalah pencurian biasa (Pasal 362) dibarengi dengan cara dan

keadaan tertentu, sehingga disebutkan mempunyai sifat yang lebih berat dari hukuman maksimal pada pencurian biasa. [18]

4. Pencurian dengan kekerasan

Pencurian dengan kekerasan adalah pencurian yang diatur dalam Pasal 365 KUHP berbunyi:

a. Diancam dengan pidana penjara paling lama sembilan tahun, pencurian yang didahului, disertai atau diikuti dengan kekerasan atau ancaman kekerasan terhadap orang dengan maksud untuk mempersiapkan atau mempermudah pencurian atau dalam hal tertangkap tangan, untuk memungkinkan melarikan diri sendiri atau peserta lainnya atau untuk tetap menguasai barang yang dicurinya.
b. Diancam dengan pidana penjara paling lama dua belas tahun:
    1) jika perbuatan dilakukan pada waktu malam dalam sebuah rumah atau pekarangan tertutup yang ada rumahnya, di jalan umum atau dalam kereta api atau trem yang sedang berjalan.
    2) jika perbuatan dilakukan oleh dua orang atau lebih dengan bersekutu.
    3) jika masuknya ke tempat melakukan kejahatan dengan merusak atau memanjat atau dengan memakai anak kunci palsu, perintah palsu atau pakaian jabatan palsu.

[18] *Ibid.*,halaman 30

4) jika perbuatan mengakibatkan luka-luka berat.

c. Bila pembuatan mengakibatkan kematian, maka diancam pidana penjara paling lama lima belas tahun.

d. Diancam dengan pidana mati atau pidana penjara seumur hidup atau selama waktu tertentu paling lama dua puluh tahun, jika perbuatan mengakibatkan luka berat atau mati dan dilakukan oleh orang atau lebih dengan bersekutu, pula disertai oleh salah satu hal yang diterangkan dalam no.l dan 3.

Berdasarkan isi pasal keseluruhan dapat disebut pencurian dalam pasal ini memiliki unsur tersendiri yang berbeda, unsur itu ialah dengan menggunakan kekerasan atau ancaman kekerasan, dan juga mempersiapkan pencurian dan untuk mempermudah dilakukannya pencurian. Melakukan hal-hal itu dianggap telah memperberat hukuman, oleh karena itu pelaku tindak pidana ini diancam hukuman 9 tahun penjara dan dapat diperberat lagi jadi tahun bila memenuhi unsur yang ada pada ayat (2) jika mengakibatkan orang luka berat, hukuman dapat diperberat lagi dengan ancaman 15 tahun, jika mengakibatkan seseorang mati hukuman dapat diperberat jadi hukuman mati atau hukuman 20 tahun. [19]

5. Pencurian dalam keluarga

Pencurian ini diatur dalam Pasal 367 KUHP yang merupakan pencurian di kalangan keluarga. Dimana baik pelaku maupun korbannya masih satu keluarga, misalnya contoh yang terjadi, apabila seorang suami atau istri melakukannya

[19] *Ibid.*, halaman 30.

sendiri atau membantu orang lain melakukan pencurian terhadap harta benda istri atau suaminya. Secara singkat, tindak pidana terhadap harta benda ini telah diatur dalam Buku II KUHP dan khusus untuk tindak pidana pencurian itu sendiri diatur dalam BAB XXII pasal 362 KUHP sampai Pasal 367 KUHP dalam hal ini mencangkup tentang jenis pencurian secara pokok. Dan termuat lima kualifikasi pencurian, yaitu :

a. Pencurian biasa (Pasal 362 KUHP)

b. Pencurian berat (Pasal 363 KUHP)

c. Pencurian ringan (Pasal 364 KUHP)

d. Pencurian dengan kekerasan (Pasal 365 KUHP)

e. Pencurian beserta penurunan pencabutan hak (Pasal 366 KUHP)

f. Pencurian terhadap lingkungan keluarga (Pasal 367 KUHP).

Selain itu pencurian juga memiliki dua unsur yaitu, objektif dan subjektif, dari segi unsur objektif seperti halnya perbuatan mengambil, suatu barang, secara keseluruhan atau sebagian kepunysaan orang lain. Makna dari “Perbuatan” disini menjelaskan suatu perbuatan itu dilarang oleh Undang-undang, jika ada orang yang melanggar orang tersebut akan mendapatkan sanksi atau hukuman berupa penjara. Sedangkan dari unsur subjektifnya yaitu, dengan maksud, untuk memiliki barang atau kepunyaan milik orang lain, secara melawan hukum. [20]

[20] R. Mas Repati Artika. (2020). "Pencurian Antar Orang Yang Punya Hubungan Keluarga Tertentu Sebagai Delik Aduan Relatif Menurut Pasal 367 Ayat (2) KUHP". Jurnal Lex Privatum. volume 8.4. halaman 239 - 46.

B. Kartu Kredit

Menurut Yuhelson dalam bukunya menjelaskan bahwa kartu kredit didefinisikan sebagai berikut : *Credit card* atau kartu kredit merupakan suatu alat berbentuk kartu yang diterbitkan oleh suatu lembaga keuangan dan dapat digunakan sebagai alat pembayaran transaksi pembelian barang dan jasa yang pembayaran pelunasannya dapat dilakukan oleh pembeli secara sekaligus maupun angsuran pada jangka waktu tertentu setelah kartu digunakan sebagai alat pembayaran. Dengan mempunyai kartu kredit, seseorang dapat melakukan pembelian barang dan jasa pada tempat-tempat khusus yang menjalin kerja sama dengan perusahaan kartu kredit yang bersangkutan tanpa harus menggunakan uang tunai. Pembayaran pembelian dilakukan dengan cara menggesekkan kartu kredit pada perangkat yang sudah disiapkan oleh penjual barang dan jasa, sehingga transaksi pembelian tersebut tercatat pada alat tersebut dan dapat dicetak. Pembayaran atau angsuran oleh pemegang kartu diberikan secara langsung kepada perusahaan kartu kredit atau melalui pihak lain yang ditunjuk. [21]

1. Penerbit (*Issuer*)

Issuer adalah pihak atau lembaga yang menerbitkan dan mengelola kartu kredit. Lembaga penerbit ini dapat berupa lembaga keuangan bukan bank yang secara khusus bergerak dalam bidang kartu kredit, lembaga keuangan bukan bank lain, bank, atau perusahaan non lembaga keuangan.

[21] *Ibid.*, halaman 46

2. Pengelola (*Acquirer)*

Acquirer adalah pihak yang mewakili kepentingan penerbit kartu untuk menyalurkan kartu kredit, melakukan penagihan pada pihak *merchant*. Mengingat jangkauan dari penggunaan kartu kredit biasanya sangat luas dan penerbit kartu kredit tidak mungkin untuk memiliki kantor cabang di semua tempat, maka penerbit selalu memerlukan jasa *acquirer* dalam pengelolaan kartu kreditnya. Penerbit ada yang secara khusus menerbitkan kartu saja, sedangkan kegiatan operasional, penyaluran, penagihan, dan pembayaran diserahkan sepenuhnya kepada *acquirer.* Penerbit tertentu juga bertindak sebagai *acquirer* dari kartu kredit yang diterbitkan. Sebelum suatu perusahaan atau bank bertindak sebagai *acquirer* atas sesuatu kartu kredit tertentu, terlebih dahulu yang bersangkutan mengadakan perjanjian kerja sama dengan *acquirer*. [22]

3. Pemilik Kartu (*Card Holder*)

Pemilik kartu adalah pihak yang menggunakan kartu kredit untuk kegiatan pembayarannya. Seseorang yang ingin mempunyai kartu kredit belum tentu selalu disetujui apabila mengajukan permohonan kartu kredit kepada *acquirer* atau *issuer*.

4. Penjual (*Merchant*)

Merchant adalah pihak penjual barang dan jasa yang dibeli oleh pemilik kartu dengan menggunakan kartu kreditnya. Sebelum merchant menerima

[22] R Nurcahya Pramuhadi. (2020). "Gaya Hidup Penggunaan Kartu Kredit Masyarakat Urban Di Surabaya". Jurnal Sosiologi Dialektika. volume 15. halaman 72.

pembayaran dengan kartu kredit tertentu, merchant tersebut terlebih dahulu mengadakan perjanjian kerja sama dengan *issuer* dan *acquirer*. Untuk meminimalkan resiko, biasanya *issuer* dan *acquirer* melakukan seleksi atau analisis terlebih dahulu sebelum memutuskan seseorang layak memegang kartu kredit yang mereka terbitkan.

Persyaratan yang seharusnya dipenuhi pada dasarnya adalah :

a. Penghasilan yang jumlahnya cukup dan disesuaikan dengan fasilitas kredit melalui kartu kredit yang akan diberikan. Pemenuhan syarat ini biasanya dilihat melalui bukti tertulis tentang gaji atau penghasilan calon pemilik kartu seperti slip gaji, laporan keuangan usaha, mutasi rekening simpanan pada bank, dan lain-lain.

b. Kontinuitas penghasilan. Penghasilan seseorang yang tinggi belum tentu menggambarkan kemampuannya untuk dapat selalu memenuhi kewajibannya kepada perusahaan kartu kredit. Kontinuitas dari penghasilan yang cukup akan lebih dapat memberikan keyakinan atas kemampuan calon pemilik kartu bagi *issuer* atau *acquirer*.

c. Niat baik atau kemauan dari calon pemilik kartu untuk selalu memenuhi kewajibannya syarat paling sulit untuk diidentifikasikan. Salah satu cara melihat niat baik dari calon pemilik kartu adalah

melalui terdapat atau tidaknya nama calon pemilik kartu pada daftar hitam *(block list*) milik bank, bank sentral, atau lembaga lain. [23]

C. Pencurian Kartu Kredit Melalui Media Elektronik *Carding*

Kejahatan *Carding* adalah suatu kejahatan dimana komputer sebagai alat untuk melakukan kejahatan *Carding* tersebut, dimana tindak pidana *Carding* ini merupakan salah satu jenis kejahatan yang dikenal dengan istilah *cyber crime*. Istilah *cyber crime* saat ini merujuk pada satu tindakan kejahatan yang berhubungan dengan dunia maya (*cyber space*). Ada ahli yang menyamakan antara tindak kejahatan siber (*cyber crime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan diantara keduanya. Secara etimologis Kejahatan *Carding* merupakan kejahatan yang memanfaatkan teknologi internet sebagai sarana utama untuk mengakses secara tidak sah suatu sistem sebuah *website* untuk mendapatkan data-data para nasabah kartu kredit. Tujuannya adalah untuk membelanjakan secara tidak sah kartu kredit yang telah didapatkan ataupun untuk mendapatkan dana milik pemegang kartu kredit tersebut. [24] *Carding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. Sebutan pelakunya adalah *carder*. Sebutan lain untuk kejahatan jenis ini adalah *cyber fraud* alias penipuan di dunia maya. Sifat *Carding* secara umum adalah *non-violence* kekacauan yang ditimbulkan tidak terlihat secara langsung, tapi dampak yang ditimbulkan bisa sangat besar. Karena *Carding* merupakan salah satu dari

[23] Deny Slamet Pribadi. (2005). "Aspek Hukum Penggunaan Kartu Kredit Sebagai Alat Jaminan", Jurnal Risalah Hukum. halaman 8.

[24] *Ibid'.*, halaman 8

kejahatan *cyber crime* berdasarkan aktivitasnya. Salah satu contohnya dapat menggunakan nomor rekening orang lain untuk belanja secara *online* demi memperkaya diri sendiri. Yang sebelumnya tentu pelaku (*carder*) sudah mencuri nomor rekening dari korban.

Kejahatan *Carding* ini lebih dikhususkan dalam transaksi penjualan baik itu yang dilakukan secara fisik maupun secara *online*. Secara fisik, *Carding* dilakukan dengan menggunakan data atau identitas milik orang lain untuk digunakan berbelanja di tempat belanja yang menerima pembayaran memakai kartu kredit. Kemudian teknik penggandaan kartu kredit dilakukan dengan membaca data kartu kredit menggunakan MSR (*Magnetic Stripe Card Reader*), lalu datanya ditulis ke sebuah kartu kosong atau kartu bodong menggunakan *Magneti Tripe Card Writer*. Selanjutnya kartu inilah yang digunakan untuk berbelanja ke berbagai tempat yang melayani pembayaran dengan kartu kredit. Sementara itu, secara *online*, *Carding* dilakukan dengan menggunakan data atau identitas milik orang lain untuk berbelanja di tempat belanja *online*. Selain itu, tentang teknik *hacking Carding*, yakni melakukan pencurian data transaksi dari pengelola suatu layanan *online shopping* yang dilakukan oleh seorang *black hacker*. Selanjutnya data pemilik kartu kredit dari *data base* ini seorang *hacker/cracker* akan menggunakannya untuk bertransaksi dan otomatis tagihan akan masuk kepada pemilik kartu kredit. Terminologi *Carding* dalam bahasa formal atau bahasa hukum, digolongkan sebagai *credit/debit card fraud* (penipuan menggunakan kartu kredit/kartu debit), yang menurut IFCC (*Internet Fraud Compalint Center*) yaitu salah satu unit di *FBI* yang menangani komplain dari

masyarakat berkaitan dengan *Cyber crime*, adalah: "*The unauthorized use of a credit/debit card number can be stolen from unsecured web sites, or can be obtained in an identity theft scheme* "(Penyalahgunaan kartu kredit/debet untuk menipu dalam mendapatkan uang atau *property*. Nomor kartu kredit dapat dicuri dari *website* yang tidak terjaga/tidak aman atau didapatkan melalui pencurian identitas). [25]

Kejahatan *Carding* mempunyai dua ruang lingkup, nasional dan transnasional. Secara nasional adalah pelaku *Carding* melakukannya dalam lingkup satu negara. Transnasional artinya adalah pelaku *Carding* melakukannya melewati batas negara. Tujuannya adalah untuk berbelanja dengan kartu kredit tidak valid tersebut atau mendapatkan dana dari kartu kredit yang tidak sah tersebut. Tindak pidana *Carding* yang dilakukan oleh para pelaku atau disebut *carder* dapat dikategorikan dalam 2 (dua) bentuk yaitu transaksi konvensional atau *offline* dan transaksi maya atau *online*. Sebagai salah satu jenis kejahatan berdimensi baru *Carding* mempunyai karakteristik tertentu dalam pelaksanaan aksinya yaitu :

1. *Minimize of physycal contact* karena dalam modusnya antara korban dan pelaku tidak pernah melakukan kontak secara fisik karena peristiwa tersebut terjadi di dunia maya , namun kerugian yang ditimbulkan adalah nyata. Ada suatu fakta yang menarik dalam kejahatan *Carding* ini dimana pelaku tidak perlu mencuri secara fisik kartu kredit dari pemilik aslinya

[25] I Gede Krisna Ginara, I Made Minggu Widyantara, and Ni Komang Arini Styawati. "Kriminalisasi Terhadap Kejahatan *Carding* Sebagai Bentuk *Cyber crime* Dalam Hukum Pidana Indonesia". Jurnal Preferensi Hukum. volume 3.1. halaman 138.

tapi cukup dengan mengetahui nomornya pelaku sudah bisa melakukan aksinya, dan ini kelak membutuhkan teknik dan aturan hukum yang khusus untuk dapat menjerat pelakunya.

2. *Non violance* (tanpa kekerasan) tidak melibatkan kontak fisik antara pelaku dan korban seperti ancaman secara fisik untuk menimbulkan ketakutan sehingga korban memberikan harta bendanya. Pelaku tidak perlu mencuri kartu kredit korban tapi cukup dengan mengetahui nomor dari kartu tersebut maka ia sudah bisa beraksi.
3. *Global* karena kejahatan in terjadi lintas negara yang mengabaikan batas-batas geografis dan waktu.
4. *High Tech* karena menggunakan peralatan berbasis teknologi serta memanfaatkan sarana jaringan informatika dalam hal ini adalah internet untuk melakukan kejahatannya. Berdasarkan karakteristik perbedaan tersebut untuk penegakan hukumnya tidak bisa dilakukan secara tradisional, sebaiknya dilakukan dengan menggunakan hukum tersendiri. Sifat *Carding* secara umum adalah non-violence sehingga kekacauan yang disebabkan oleh kejahatan ini tidak terlihat secara langsung tetapi dampak yang timbulkannya bisa sangat besar.

Ada dua jenis model transaksi yang rawan terjadi pencurian informasi kartu kredit *Carding*, antara lain:

a. Card Present.

Yaitu transaksi dengan menggunakan kartu dalam bentuk fisik melalui mesin EDC ("*Electronic Data Capture*") pada *merchant* (misalnya toko atau hotel). Pada jenis transaksi *card present*, pelaku mendapatkan segala informasi kartu kredit korban dengan teknik *skimming* menggunakan alat yang bernama *card skimmer*. *Card skimmer* adalah alat yang mampu merekam data/informasi pada kartu kredit. Karena ukuran alatnya cukup kecil, biasanya pelaku menyembunyikan alat tersebut di bawah meja kasir. Pelaku atau *carder* mengambil data/informasi pada kartu kredit korbannya dengan cara menggesekkan kartu kredit korban pada *card skimmer* sesaat setelah dilakukan transaksi pada mesin EDC.

b. Card Not-Present

Pengertian transaksi tanpa menggunakan kartu kredit dalam bentuk fisik yang dilakukan secara *online* melalui internet atau melalui telepon (*mail order*) atau tidak secara langsung. Transaksi ini lebih berisiko karena transaksi dilakukan tanpa menggunakan kartu kredit dalam bentuk fisik. Pelaku juga lebih mudah untuk mendapatkan data-data kartu kredit korbannya tanpa menggunakan alat tertentu. Teknik yang umum di gunakan diantaranya adalah *phishing* dan *hacking*. *Phishing* dilakukan dengan cara pelaku atau *carder* melakukan penyamaran menjadi pihak yang dapat dipercaya atau seolah-olah merupakan pihak yang sesungguhnya untuk mendapatkan informasi kartu kredit dari korbannya. Contohnya dengan meminta verifikasi informasi kartu kredit melalui *e-mail* atau telepon dan mengaku sebagai petugas bank atau memancing korban dengan

berbagai promo fiktif seperti yang terjadi baru-baru ini yakni dengan promo tiket pesawat murah yang mengarahkan korban untuk memasukkan nomor kartu kredit lalu diambil data-data dari kartu kredit tersebut. Teknik lainnya adalah *hacking* yaitu dilakukan dengan cara mengeksploitasi atau menjebol celah keamanan pada suatu *website ecommerce*

Pengaturan mengenai kejahatan atau tindak pidana *Carding* tidak diatur secara eksplisit dalam undang-undang apa pun di Indonesia pada saat ini. Tidak ada undang-undang khusus. Semua dasar hukum yang dipakai oleh para penegak hukum dalam usaha pemberantasan kejahatan atau tindak pidana *Carding* sebagian besar adalah hasil dari penafsiran analogi beberapa Pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang disesuaikan dengan unsur-unsur dari kejahatan atau tindak pidana *Carding*.

D. Pasal-Pasal Tindak Pidana (*Carding)*

Pembahasan pasal-pasal yang digunakan untuk menjerat para pelaku sekaligus tersangka tindak pidana kejahatan kartu kredit *Carding*, yaitu sebagai berikut :

1. Penipuan

   Dalam Pasal 378 Kitab Undang-undang Hukum Pidana (KUHP), ditentukan bahwa : Barang siapa dengan maksud untuk menguntungkan dirinya sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu, dengan tipu muslihat, ataupun rangkaian bohong, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya,

atau supaya memberi hutang maupun melepaskan piutang, diancam karena penipuan dengan penjara paling lama empat tahun.

2. Pemalsuan

Dalam ketentuan Pasal 263 KUHP ayat (1), ditegaskan bahwa: Barang siapa yang membuat palsu atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan atau pembebasan utang, atau yang diperuntukkan sebagai bukti daripada sesuatu hal dengan maksud untuk memakai atau menyuruh orang lain memakai surat tersebut seolah-olah isinya benar dan tidak palsu, diancam jika pemakaian tersebut dapat menimbulkan kerugian, karena pemalsuan surat, dengan pidana penjara paling lama enam tahun. Sehubungan dengan hal tersebut, salah satu unsur yang paling esensial dari tindak pidana yang diatur dalam Pasal 263 KUHP, adalah : Adanya surat palsu, kertas yang palsu atau yang dipalsukan. Untuk dapat menerapkan Pasal 263 KUHP pada tindak pidana kartu kredit, memang bahwa kartu kredit itu adalah jenis kertas walaupun plastik yang sudah dipalsukan oleh pelaku tindak pidana.

3. Pencurian

Dalam Pasal 362 Kitab Undang-undang Hukum Pidana (KUHP), ditentukan bahwa barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak

sembilan ratus rupiah. Lalu pengaturan mengenai kejahatan atau tindak pidana *Carding* Pasal 31 jo Pasal 47 dan Pasal 32 jo Pasal 48 Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik yang berbunyi sebagai berikut : Pasal 31 Ayat (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. [26] 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 32 Ayat (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. Pasal 48 Ayat (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)

[26] Qammaddin, Sulfikar Sallu, and Ahmad Fathoni. 2023. "Implementasi Teknik Forensik Dalam *Cyber crime Carding*" Jurnal Hukum. Halaman 29

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Bagaimana Bentuk Pencurian Kartu Kredit *Carding* Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Studi Kasus: No.845/Pid.Sus/2020/PT SBY

Cyber crime masih hangat diperdebatkan di kalangan sarjana hukum. Ini karena bentuk kejahatan ini relatif baru. Hukum pidana positif (KUHP dan KUHAP) telah dikritik dan dipertahankan karena kemampuannya menangani kejahatan ini. [27] Penjahat dunia maya akan ditangkap oleh penegak hukum. *Cyber crime* masih tertangkap berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP), terutama yang memenuhi kriteria pasal-pasal tipikal KUHP. Ketika produk ini dianggap tidak cukup untuk mencegah berbagai bentuk kejahatan *online,* banyak instrumen hukum pidana di luar KUHP dapat digunakan untuk menyelesaikan kejahatan melalui penerapan teknologi ini. Instrumen-instrumen ini mencakup pendekatan yang berbeda terhadap undang-undang hukum yang berbeda. [28]

Kejahatan siber semakin menjadi ancaman nyata bagi individu, perusahaan, dan bahkan pemerintah di era komputer dan internet saat ini. Tindakan kriminal yang dilakukan menggunakan teknologi digital, seperti

[27] Hasan Hiawatha, Rifai and Asmak U I Hosnah. (2024) "Tinjauan Yuridis Terhadap Tindak Pidana Pencurian Identitas Di Bawah Ketentuan KUHP". Jurnal Pendidikan Tambusai. Volume 8.2. halaman 4.

[28] Kemal Idris Balaka, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany. (2024). "Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital". Jurnal Yustitiabelen. volume 10.2. halaman 105.

komputer, jaringan internet, dan perangkat *mobile*, disebut kejahatan siber.[29] Motivasi pelaku adalah salah satu faktor penentu yang paling penting dalam kejahatan siber. Ada berbagai motif yang mendorong seseorang untuk terlibat dalam kejahatan siber, termasuk motivasi keuangan, balas dendam, dan kepuasan pribadi. Pelaku kejahatan siber menggunakan motivasi keuangan untuk mendapatkan keuntungan finansial dengan mencuri data pribadi, melakukan pencurian identitas, atau meretas sistem keuangan.[30] Peluang juga menentukan kejahatan siber selain motivasi.

Berkembangnya teknologi digital telah membuka lebih banyak kesempatan bagi para pelaku kejahatan siber. Masyarakat yang terlibat dalam kejahatan siber melihat kemampuan untuk menyusup ke dalam jaringan yang tidak terlindungi atau mengeksploitasi kerentanan sistem sebagai peluang yang menarik.[31]

Faktor tambahan yang menentukan kejahatan siber adalah pengetahuan dan keterampilan teknis pelaku. Pada umumnya, kejahatan siber dilakukan oleh individu atau kelompok yang sangat mahir dalam komputer, jaringan, dan sistem keamanan. Hanya orang yang memiliki kemampuan untuk menggunakan perangkat lunak jahat, mencari dan mengeksploitasi kerentanan sistem, serta

---

[29] Tri Ginanjar Laksana and Sri Mulyani. (2024). "*Key Determinants* Of *Cyber Crime*s Targeting *The Human Population*", Jurnal Maret. volume 11.2.

[30] Ginara, Widyantara, and Styawati. *Opt cit.*, halaman 138

[31] Nurul Maghfirah and Abshoril Fithry. (2024). "Analisis Tindak Pidana Terhadap Kerusakan Program Dan Data Komputer (Studi Kasus Perlindungan Sistem Hukum Informatika". Jurnal Prosiding SNAPP : Sosial Humaniora, Pertanian, Kesehatan Dan Teknologi. volume 2.1. halaman 191 - 95.

menyusup ke dalam jaringan yang dilindungi. [32]

Salah satu bentuk kejahatan *cyber* dalam segi keuangan adalah *Carding*. *Carding* atau *credit card fraud*, salah satu bentuk dari pencurian (*theft*) dan kecurangan (*fraud*) di dunia internet yang dilakukan oleh pelakunya dengan menggunakan kartu kredit (*credit card*).[33] kartu kredit palsu yang dibuat sendiri dengan tujuan untuk membeli barang secara tidak sah atas beban rekening dari pemilik kartu kredit yang sebenarnya (yang asli) atau untuk menarik dana secara tidak sah dari suatu rekening bank milik orang lain. [34]

Kejahatan *Carding* memiliki dua ruang lingkup, maksudnya ruang lingkup nasional dan internasional.[35] Secara nasional yaitu pelakunya melakukan dalam negara yang sama (satu lingkup), sedangkan internasional/transnasional pelaku *Carding* melakukan kejahatan tersebut melawati batas negara atau lintas negara. Penyalahgunaan kartu kredit dapat dilakukan dengan dua cara, antara lain: [36]

1. Kartu kreditnya sah namun tidak digunakan sesuai peraturan yang ditentukan dalam perjanjian yang telah disepakati oleh pemegang kartu kredit dengan bank sebagai pengelola dari kartu kredit;

---

[32] Muhammad Khairul Faridi. (2019)."Kejahatan Siber Dalam Bidang Perbankan". Jurnal Cyber Security Dan Forensik Digital, volume 1.2. halaman 61.

[33] *Ibid*., halaman 57

[34] Deardo Pieter Saragih. (2022). "Transnational *Carding* Crime Analysis Is Reviewed From International Criminal Law". Jurnal Hukum Dan HAM Wara Sains. volume 1. halaman 108 - 20.

[35] Ridwan Arifin, Hartini Atikasari, and Waspiah. (2020). "The Intersection of Criminal Law, Technology and Business Commercial Law on *Carding*as *Cyber* Fraud". Jurnal Hukum Novelty. volume 11.2. halaman 235.

[36]*Ibid*., halaman 235

2. Kartu kredit tidak sah atau palsu, digunakan dengan cara yang tidak sah pula. Kategori siber berdasarkan cara-cara kejahatannya dibagi menjadi dua, yaitu: Pertama, kejahatan dilakukan dengan kekerasan atau si pelaku melakukan kejahatan dengan tindak kekerasan. Kedua, kejahatan dilakukan tanpa adanya kekerasan. *Carding* termasuk kepada kategori kedua karena *Carding* dilakukan tanpa adanya kekerasan secara fisik untuk melancarkan perbuatannya. Jenis-jenis *Carding* adalah sebagai berikut:

    a. *Misus* (*compromise*) *of card data*, jenis ini merupakan penyalahgunaan kartu kredit yang tidak di presentasikan. Maksud dari tidak dipresentasikan adalah pengguna *credit card* tidak menyadari bahwasanya kartu kredit telah digunakan oleh orang lain sampai pengguna yang menerima tagihan tersebut.

    b. *Counter feiting*, jenis ini yaitu pemalsuan *credit card*. Kartu palsu telah dibuat dan dimodifikasi sedemikian rupa sehingga identik dengan kartu yang asli. *Carding* jenis ini termasuk yang paling canggih karena bekerja sama dengan orang-orang yang memiliki keahlian tertentu.

    c. *Wire tapping*, cara kerja dari jenis *Carding* yang ini adalah dengan cara penyadapan transaksi *credit card* melalui jaringan komunikasi. Sehingga jumlah yang di dapat oleh pelaku sangat banyak dan tingkat kerugian pengguna sangat tinggi.

d. Phising, merupakan penyadapan yang dilakukan melalui *link*/situs website dan *e-mail* agar data pribadi nasabah/konsumen/pengguna dapat dicuri. [37]

Dalam kehidupan masyarakat Indonesia, kejahatan terhadap kartu kredit di Indonesia terus meningkat dengan banyaknya cara atau modus operandi dalam penyalahgunaan kartu kredit baik dari segi kuantitas dan kualitas yang mengakibatkan kerugian baik bagi pihak bank yang mengeluarkan kartu kredit maupun masyarakat sebagai nasabah pemegang kartu kredit itu sendiri. Hal ini disebabkan karena penyalahgunaan kartu kredit semakin modern dan dimana pelaku kejahatan yang memiliki pengetahuan akan teknologi serta ketelitian dalam melakukan kejahatan kartu kredit tersebut.

Kejahatan kartu kredit *Carding* dapat dilakukan dengan berbagai modus operandi diantaranya sebagai berikut :

1. *Fraud application*; Menggunakan kartu kredit asli yang diperoleh dengan aplikasi palsu. Pelaku memalsu data pendukung dalam proses aplikasi seperti: KTP, Paspor, rekening koran, Surat Keterangan Penghasilan.
2. *Non received card*; Menggunakan kartu kredit asli yang tidak diterima oleh pemegang kartu kredit yang sah (berhak) kemudian pelaku membubuhkan tanda tangan di kolom tanda tangan. Kartu kredit diperoleh melalui kurir atau membobol kantor pos bila dikirim melalui Pos.

[37] Rafi Septia Budianto Pansariadi and Noenik Soekorini. 2023. "Tindak Pidana *Cyber crime* Dan Penegakan Hukumnya". Jurnal Binamulia Hukum. volume 12.2. halaman 287.

3. *Lost/stolen card*; Menggunakan kartu kredit asli hasil curian atau hilang. Pada waktu melakukan transaksi pelaku menandatangani *sales draft* dan meniru tanda tangan pada kartu kredit atau tanda tangan pemegang kartu yang sah. Transaksi dilakukan di bawah *floor limit* agar tidak perlu dilakukan otorisasi.

4. *Altered card*; Menggunakan kartu kredit asli yang sudah diubah datanya. Pelaku menggunakan kartu hasil curian (*lost/stolen, non received, expired card*) dan kartu reliefnya dipanasi dan diratakan kemudian pelau melakukan *reembossed* dengan data baru. Sedangkan *magnetic stripe* diisi data baru dengan *reencoded* yang diperoleh dari *point of compromise* (POC).

5. *Totally counterfeited*; Menggunakan kartu kredit yang seluruhnya palsu. Pelaku mencetak kartu tiruan dengan menggunakan data nomor dan pemegang kartu yang masih berlaku dengan melakukan *reembossed* dan *reencoded.*

6. *White plastic card*; Menggunakan kartu plastik polos yang berisi data asli. Pelaku mencetak data dari pemegang kartu kredit yang sah pada plastik polos, tanpa meniru hologram dan logo penerbit. *Magnetic stripe* diisi dengan data pemegang kartu dengan cara *encoding*.

7. *Record of charge* (Roc) *pumping*; Penggandaan *sales draft* oleh *merchant* (pedagang). *Sales* 31 *draft* yang satu tidak ditandatangani oleh pemegang

kartu yang sah dan diserahkan kepada *merchant* lain untuk diisi dengan data transaksi fiktif.

8. *Altered amount*; Mengubah nilai transaksi pada *sales draft* oleh *merchant* (pedagang).
9. *Telephone/mail ordered* Memesan barang melalui telepon atau surat dengan menggunakan kartu kredit orang lain yang sudah diketahui nama dan nomornya.
10. Mengubah program *Electronic Data/Draft Capture* (EDC); Mengubah dan merusak program pada alat otorisasi (*electronic data/draft capture*/EDC) milik pengelola oleh *merchant* (pedagang).
11. *Fictius merchant.* Pelaku berpura-pura menjadi pedagang dengan mengajukan aplikasi disertai dengan data-data palsu. Pelaksanaan modus operandi tersebut juga didukung berbagai instrumen seperti *skimmer* atau *software* untuk *generate* nomor kartu kredit dan kesempatan yang relatif terbuka untuk mencuri data dari kartu kredit seperti di hotel, restoran, *card centre* dll. sehingga identitas kartu kredit dapat diperoleh dengan mudah.

Para *carder* memiliki dua cara untuk mendapatkan data-data kartu kredit para korban, yang pertama dengan menyentuh langsung kartu kredit milik korban yang pada umumnya dilakukan di gerai ritel seperti restoran dan toko. Tindakan tersebut dilakukan oleh karyawan dengan alasan yang sah untuk memiliki kartu kredit korban, selanjutnya karyawan memanfaatkan *electronic* data *capture* untuk mencuri data-data yang tersimpan di dalam kartu (*skimming*). Tindakan *skimming*

tersebut seperti yang terjadi di cabang *The Body Shop* Jakarta. Cara yang kedua adalah memanfaatkan teknologi internet. Salah satunya adalah Phising, teknik ini digunakan oleh para *carder* untuk memperoleh data-data kartu kredit dengan mengarahkan korban untuk masuk ke sebuah situs *website* jebakan yang telah dibuat menyerupai *website* asli.

Biasanya para *carder* melakukan Phising dengan mengirimkan sebuah email kepada para korban. Setelah mendapatkan nomor kartu kredit beserta data-datanya, *carder* membelanjakannya di pedagang (*merchant*) *online* yang diinginkan. Barang yang dibeli akan dikirimkan ke alamat teman *carder* yang ada di luar negeri seperti Australia atau Singapura, hal ini dilakukan karena banyak *merchant* yang tidak berkenan mengirimkan barang ke alamat Indonesia. Setelah itu barang akan dikirimkan oleh teman *carder* ke alamat Indonesia Dari modus operandi tersebut dapat dilihat bahwa *carder* yang memanfaatkan teknologi internet dapat menjangkau para nasabah pemegang kartu kredit yang berada di luar negara dimana *carder* berada dan dapat membelanjakan kartu kredit tersebut di toko mana pun yang menyediakan pembelian secara *online*. Hal tersebut dapat dilakukan karena sifat dari teknologi internet yang tanpa batas (*borderless*).

Menurut pasal 3 ayat (2) United *Nations Convention Against Transnational Organized Crim*e, suatu kejahatan dapat dikategorikan sebagai kejahatan transnasional apabila:

1. *It is committed in more than one State;*

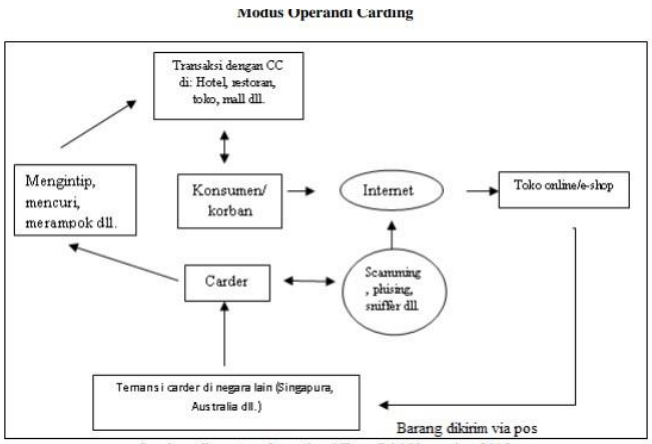
2. *It is committed in one State but a substansial part of its preparation, planning, direction or control takes place in another State;*
3. *It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or*
4. *It is committed in one State but has substansial effects in another State.*

Kejahatan *Carding* dapat dikategorikan dalam kejahatan transnasional karena:

1. Pencurian data-data kartu kredit nasabah oleh para *carder* bisa dilakukan di beberapa negara.
2. Persiapan, perencanaan pengarahan dan pengawasan oleh pelaku kejahatan *Carding* dilakukan di satu negara tetapi target kejahatan tersebut berada di luar negara dimana *carder* berada.
3. Para *carder* bisa mendapatkan data-data kartu kredit dibantu oleh teman mereka di luar negeri yang bekerja di gerai ritel seperti restoran atau toko yang melayani pembayaran melalui kartu kredit. Mereka juga bisa mendapatkan data tersebut melalui forum-forum *Carding* dengan memanfaatkan teknologi internet.
4. Kejahatan *Carding* memiliki target yang berada di lebih dari satu negara. Kejahatan *Carding* merupakan sebuah perbuatan penipuan kartu kredit yang dimana dilakukan dengan berbagai cara oleh pelaku yang disebut *carder*, yaitu berupa pembobolan serta peretasan kartu kredit melalui media internet, dengan tujuan akan memesan benda melalui media *online*

atau mengambil sejumlah dana yang tidak sah dari rekening bank milik korban dalam kejahatan *Carding* ini memiliki beberapa bentuk yaitu, mengakses komputer secara ilegal (*Cyber* trespass).

Gambar 1



Sumber : Reportase Investigasi Trans7 16 November 2013

Mencuri informasi yang memiliki nilai sudah bisa dikategorikan *Cyber theft*. Penipuan melalui internet *Cyber fraud*. Merusak data *Destructive cyber crimes*. Adapun beberapa pengaturan hukum positif yang berlaku di Indonesia yang dapat mengkriminalisasi kejahatan *Carding* yaitu dalam Pasal 362, 363 ayat (1), dan Pasal 378 KUHP. Dalam Pasal 362 KUHP yang mempunyai dan mengatur tentang pencurian, dimana kaitannya dalam kasus kejahatan *Carding* ini bergantung pada modus operandi yang dilakukan oleh pelaku, jika pelaku melakukan kejahatan *Carding* ini dengan mencuri kartu kredit seseorang secara non fisik menggunakan *software*, maka dapat dikenakan pasal ini. Untuk Pasal 363 KUHP ayat (1) yang memiliki poin persekongkolan, kaitannya dengan kejahatan *Carding* yakni dalam proses kejahatan berlangsung dilakukan dengan cara bersekongkol dengan satu orang atau lebih dari dua orang, maka pasal ini

dapat dikenakan karena pelaku kejahatan *Carding* telah melakukan kerja sama dengan satu orang atau lebih dalam prosesnya. Sedangkan Pasal 378 KUHP yang menyatakan artian bahwa dengan sengaja melakukan kejahatan untuk keuntungan pribadi atau orang lain dengan cara menipu.

Adapun kaitannya dengan kejahatan *Carding* ini, apabila sang pelaku melakukan kejahatan ini dengan seolah-olah menawarkan suatu barang dengan memasang iklan pada sebuah website atau media sosial untuk menarik korban, demi mendapatkan nomor kartu kredit yang diinginkan agar dapat dipergunakan secara pribadi untuk memenuhi kebutuhannya. Jika modus yang dilakukan oleh pelaku seperti yang sudah dijelaskan di atas ataupun modus yang memiliki kemiripan dalam melakukan kejahatan ini, maka pasal ini dapat dikenakan kepada pelaku kejahatan tersebut.

Untuk menunjang Pasal KUHP yang dapat mengriminalisasi kejahatan *Carding*, dapat dilihat juga dari beberapa pasal UU ITE No. 19 Tahun 2016 yang dimuat pada Pasal 30 tentang pengaksesan elektronik orang lain demi memperoleh informasi secara ilegal, Pasal 31 ayat (1) dan (2) yang memiliki arti penyadapan elektronik secara ilegal, Pasal 32 tentang pengrusakan, memindahkan sebuah informasi elektronik yang bersifat rahasia secara ilegal, Pasal 34 tentang pendistribusian/menyediakan alat untuk melakukan kejahatan, dan 35 tentang sengaja memanipulasi informasi elektronik secara ilegal. Pada permasalahan lemahnya hukum dalam pengawasan Teknologi informasi ada pada putusan 845/Pid.Sus/2020/PT.SBY, seorang pelaku yang berinisial KWM (Terdakwa 1) menjual data diri kredit orang lain di situs penjualan *online* sosial media melalui

facebook dengan melelangkan kartu kredit ilegal atas nama Amir Salim yang dibeli oleh pihak terdakwa bernama Choirul Anam yang mana dibeli dari akun Ridho Steven, dalam hal ini sang pemilik kartu kredit ilegal itu melancarkan aksinya dengan menjual hasil perasan terhadap kartu kredit milik orang lain yang didapatkan secara ilegal, KWM dianggap sebagai pihak ketiga karena mereka melakukan transaksi menggunakan rekening milik terdakwa KWM sehingga bisa dikatakan bahwa Choirul Anam adalah Pembeli dan penjualnya adalah Ridho Steven (terdakwa 2) yang mana Terdakwa 2 (berkas terpisah) ini mengambil barang milik KWM yang diniagakan, metode penjualan ini dianggap sebagai *Reselller* yang mana kartu kredit tersebut dapat digunakan di banyak reseller (Terdakwa 1).

Hasil kerugian yang dimiliki sang pemilik kartu kredit atau korban tidak sebanding dengan hukuman para terdakwa, KWM atau terdakwa 1 hanya di beri hukuman 2 tahun penjara dengan denda senilai Rp30.000.000,00 dan subsidair 4 bulan, lalu terdakwa mengajukan banding karena ia mendapatkan kartu kredit tersebut melalui seorang *hacker* sehingga pemangkasan hukuman oleh pelaku di total menjadi 8 bulan kurungan penjara. Tentu korban tidak terima dengan putusan dari pihak pengadilan, sehingga diajukanlah kasasi oleh pihak korban atas kerugian yang dialami secara materiil dan fisik sehingga putusan akhir dari terdakwa 1 hanya dikenai hukuman kurungan selama 1 tahun penjara.

Beralih merujuk ke dalam pasal 30 ayat (1) UU ITE “(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun..” Adapun

sanksi yang mesti didapatkan adalah denda sebanyak 600 Juta rupiah dengan masa tahanan selama 6 tahun, tentu ini menjadi kesetimpangan atas putusan dari pihak pengadilan dan UU yang berlaku dalam pengaturan UU ITE, kurangnya penjelasan yang signifikan terhadap pengaturan UU ITE terkait permasalahan menjadi pokok utama mengapa putusan dari pihak pengadilan yang telah merugikan orang lain lebih singkat dan mirip dengan putusan pencurian ringan. [38]

Putusan yang dihasilkan bahwa hukuman untuk Kingditho Wulanesa hanya berlaku 8 bulan untuk pelelangan kartu kredit atas nama Amir Salim yang merugikan besar Amir Salim secara materi selama kartu kreditnya terbukti terkena tindak pidana *Carding*.

Hukum seakan-akan ringan untuk pelaku yang mana sekitar 8 bulan, Penuntut Umum tidak sependapat dengan putusan Hakim tingkat pertama yang menyatakan terdakwa telah terbukti bersalah melakukan tindak pidana membantu tindak pidana Informasi dan Transaksi Elektronik. [39]

Dalam dakwaan tunggal sebagaimana diatur dan diancam pidana dalam pasal 48 ayat (2) Jo pasal 32 ayat (2) UU Nomor 19 tahun 2016 tentang perubahan atas UU Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik Jo pasal 56 KUHP, dengan pidana penjara selama 8 (delapan) bulan, karena kita sepakat menjunjung tinggi prinsip menegakkan Hukum dengan tanpa mengabaikan rasa keadilan, sesuai dengan tujuan pemidanaan, hukuman yang

[38] *Ibid.*, . Putusan Nomor 845/PID.SUS/2020/PT SBY.

[39] Raden D. (2021). "Fenomena Kejahatan *Carding* Berdasarkan Dalam Hukum Pidana Indonesia". Jurnal Hukum Das Sollen. volume 6.2. halaman 99.

dijatuhkan kepada setiap terdakwa bertujuan tidak sekedar bersifat menghukum, tetapi dapat diharapkan mampu menimbulkan efek jera kepada terdakwa dan orang lain dan pada akhirnya Penuntut Umum mohon Majelis Hakim Tingkat Banding menjatuhkan pidana kepada terdakwa sesuai dengan tuntutan semula yaitu 8 bulan untuk pelaku tindak pidana *Carding*.

Hal ini menjadi kesetimpangan proses hukum di Indonesia yang kurang kuat dalam pemrosesan untuk tindak pidana digital seperti ini, bahkan eksekusi di Indonesia tergolong masih jauh untuk siap berhadapan dengan teknologi dan berbagai aspek kejahatan yang mengintai.[40] Berbeda dengan negara maju seperti Amerika Serikat sendiri memiliki beragam bentuk penguatan dalam membuktikan suatu tindak pidana digital dan memberikan layanan terbaik dalam sistem informasi agar tetap kuat dan menghindari kebocoran data seperti kasus Amir Salim yang mana kartu kreditnya di bobol untuk dijual belikan kepada orang lain dan orang lain membelanjakannya tanpa memikirkan biaya yang akan ditanggung Amir Salim. Beberapa bentuk penanganan kejahatan *cyber* di Amerika Serikat antara lain : [41]

1. *The National Institute of Standards and Technology* (NIST) *Cybersecurity Framework.*

[40]Prigel A.. (2025). "Perbandingan Hukum Pidana *Cyber crime* Dan Pengaruhnya Dalam Penegakan Hukum Antara Indonesia Dan Amerika Comparison of *Cyber crime* Criminal Law and Its Impact on Law Enforcement Between Indonesia and America". Jurnal Kompilasi Hukum. volume 10.1. halaman 58.

[41] Rania N. (2025). "Analisis Strategi Amerika Serikat Dan Tiongkok Dalam Menanggulangi *Cyber crime* Pasca-Pandemi". Triwikrama: Jurnal Ilmu Sosial. volume 9.2. halaman 14.

National Institute of Standards and Technology (NIST) mengembangkan *Cyber security Framework* untuk menyediakan pedoman dan praktik terbaik bagi organisasi dalam mengelola dan meningkatkan manajemen risiko keamanan siber mereka. Kerangka kerja ini mencakup standar, pedoman, dan praktik untuk meningkatkan keamanan siber. Organisasi di Amerika Serikat didorong untuk menggunakan Kerangka Kerja Keamanan Siber NIST untuk menilai dan meningkatkan postur keamanan siber mereka, yang sejalan dengan kebutuhan manajemen risiko dan tujuan bisnis mereka. Kemampuan adaptasi kerangka kerja ini memungkinkannya untuk diterapkan di berbagai sektor, yang berkontribusi pada dunia maya yang lebih tangguh dan aman. [42]

2. *Health Insurance Portability and Accountability Act* (HIPAA).

HIPAA menetapkan standar untuk perlindungan informasi kesehatan pasien yang sensitif. Entitas yang tercakup, termasuk penyedia layanan kesehatan dan perusahaan asuransi kesehatan, harus mematuhi peraturan HIPAA untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi kesehatan. Peraturan Keamanan HIPAA menguraikan kerangka kerja komprehensif untuk mengamankan PHI elektronik (ePHI). Peraturan ini mengamanatkan bahwa entitas yang tercakup, seperti penyedia layanan kesehatan, rencana kesehatan, dan lembaga kliring layanan kesehatan, menerapkan perlindungan

[42] Dasril Aldo. 2018. "Pengaruh *Cyber* Attack Terhadap Kebijakan *Cyber* Security Amerika Serikat". Journal of International Relations. volume 4.3. halaman 393.

administratif, fisik, dan teknis untuk memastikan kerahasiaan, integritas, dan ketersediaan ePHI. Kerangka kerja tersebut mencakup langkah-langkah seperti kontrol akses, enkripsi, kontrol audit, dan penilaian risiko.

3. *Gramm-Leach-Bliley Act* (GLBA)

GLBA mengharuskan lembaga keuangan untuk menjaga kerahasiaan informasi keuangan pribadi nasabah. GLBA mencakup ketentuan mengenai keamanan dan kerahasiaan informasi pribadi non publik dan mengamanatkan pengembangan dan penerapan program keamanan informasi. Berdasarkan GLBA, dapat mempengaruhi lembaga keuangan dimana lembaga keuangan diharuskan untuk mengembangkan, menerapkan, dan memelihara program keamanan informasi yang komprehensif.

4. *Federal Information Security Modernization Ac*t (FISMA)

Undang-Undang Modernisasi Keamanan Informasi Federal (FISMA), yang disahkan pada tahun 2002, merupakan undang-undang keamanan siber utama di Amerika Serikat. Undang-undang ini mengamanatkan lembaga federal untuk menerapkan kontrol keamanan guna melindungi sistem informasi dan data mereka. Tujuan utamanya adalah untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi yang dikumpulkan, disimpan, dan digunakan oleh lembaga federal. Dengan adanya FISMA, mempengaruhi lembaga untuk membuat program keamanan informasi yang komprehensif, yang mencakup

penilaian risiko rutin, pengujian keamanan, perencanaan respons insiden, dan pemantauan berkelanjutan terhadap kontrol keamanan. Selain itu, lembaga diharuskan melaporkan kepatuhan mereka terhadap hukum kepada *Office of Management and Budget* (OMB)/ Kantor Manajemen dan Anggaran dan Department of Homeland Security (DHS)/ Departemen Keamanan Dalam Negeri.

5. *Cyber security Information Sharing Ac*t (CISA)

Undang-Undang Pembagian Informasi Keamanan Siber (CISA), yang disahkan pada tahun 2015 oleh Kongres AS, mendorong perusahaan swasta untuk berbagi informasi tentang ancaman siber dengan pemerintah dan memberikan perlindungan tanggung jawab atas pembagian tersebut. Dalam hal ini CISA memiliki pengaruh untuk meningkatkan pertukaran informasi ancaman siber antara pemerintah dan sektor swasta, yang bertujuan untuk melindungi infrastruktur penting dan keamanan nasional dari serangan siber.

CISA mengizinkan perusahaan swasta untuk berbagi data ancaman siber dengan lembaga federal, termasuk *epartment of Homeland Security* (DHS)/Departemen Keamanan Dalam Negeri, dan memungkinkan pembagian informasi secara timbal balik dari pemerintah ke entitas swasta. Peraturan-peraturan dan kebijakan keamanan siber di atas memiliki pengaruh penting dalam menjaga lanskap digital Amerika Serikat. Dalam beberapa tahun terakhir, meningkatnya frekuensi dan kecanggihan ancaman siber telah mendorong pemerintah untuk

menetapkan kerangka kerja yang komprehensif guna melindungi infrastruktur penting, data sensitif, dan keamanan nasional.

Efektivitas peraturan dan kebijakan ini menjadi subjek pengawasan dan evaluasi yang berkelanjutan. Salah satu inisiatif penting dalam bidang keamanan siber adalah *the Cyber security Enhancement Ac*t tahun 2014, yang memperkuat upaya penelitian dan pengembangan, menetapkan praktik terbaik, dan meningkatkan koordinasi antara pemerintah dan sektor swasta. Undang-undang tersebut menekankan pentingnya berbagi informasi dan kolaborasi untuk mengurangi ancaman siber secara efektif. Pembentukan CISA pada tahun 2018 menandai tonggak sejarah dalam konsolidasi upaya keamanan siber dalam pemerintahan Amerika.

CISA memainkan peran utama dalam mengkoordinasikan inisiatif keamanan siber, memberikan dukungan kepada entitas infrastruktur penting, dan menyebarluaskan intelijen ancaman. Upaya lembaga ini ditujukan untuk memperkuat ketahanan negara terhadap ancaman siber. Selain itu, regulasi di sektor khusus, seperti HIPAA untuk sektor perawatan kesehatan dan PCI DSS untuk industri keuangan, berkontribusi pada pendekatan yang lebih khusus dalam menangani kerentanan sektor khusus.

B. Tanggung Jawab Hukum Dalam Menangani Tindak Pidana Pencurian Kartu Kredit Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Studi Kasus No.845/Pid.Sus/2020/PT SBY

Di Indonesia saat ini Kejahatan dunia maya di Indonesia meliputi pembajakan perangkat lunak, terorisme dunia maya, penipuan (termasuk penipuan berbasis dunia maya dan pelanggaran hukum transaksi elektronik), peretasan, manipulasi data, web *phishing*, dan serangan dunia maya terhadap sistem keamanan digital. Penipuan saat ini merupakan jenis kejahatan yang paling banyak terjadi di Indonesia. Ledakan *e-commerce* telah berkontribusi pada peningkatan kasus penipuan. Pemerintah Indonesia telah mengambil langkah untuk memerangi kejahatan dunia maya dengan memberlakukan undang-undang seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Kerentanan data pribadi publik Indonesia juga terungkap pada tahun 2020. Pakar keamanan dunia maya memperkirakan bahwa jumlah kejahatan dunia maya dan serangan mungkin meningkat hampir dua kali lipat karena teknologi komputerisasi modern dan keterampilan teknis perangkat lunak yang berbeda membuat individu melakukan kejahatan dunia maya. Saat ini para penegak hukum bekerja sama untuk memberantas kejahatan ITE. Polisi juga telah membentuk unit khusus untuk menyelidiki kasus kejahatan dunia maya dan memiliki laboratorium forensik digital untuk mendukung penyelidikan mereka. Direktorat Tindak Pidana Siber (Dittipidsiber) di bawah Badan Reserse Kriminal (Bareskrim Polri) bertugas menegakkan hukum terhadap kejahatan dunia maya di Indonesia. Mereka

menangani dua kategori kejahatan dunia maya: kejahatan komputer dan kejahatan terkait komputer.

Kejahatan komputer menggunakan komputer sebagai alat utama operasi kejahatan seperti peretasan, manipulasi data, *phishing* web, dan serangan dunia maya terhadap sistem keamanan digital. Kejahatan terkait komputer menggunakan komputer sebagai fasilitator kejahatan. Polisi Siber berpatroli di dunia maya untuk mencari, mengamati, memantau, dan memprediksi potensi ancaman yang dapat mengganggu ketenteraman dan keamanan masyarakat Indonesia.

Kejahatan dunia maya dapat berdampak signifikan pada individu dan bisnis. Kejahatan dunia maya seperti pencurian identitas, penipuan, dan pelanggaran data dapat menyebabkan kerugian finansial, kerusakan reputasi, dan tekanan emosional bagi individu. Bisnis juga rentan terhadap kejahatan dunia maya, dengan potensi kerugian finansial akibat pencurian data atau serangan *ransomware*. Selain itu, bisnis dapat dikenai denda peraturan jika gagal mematuhi undang-undang perlindungan data. Beberapa upaya yang dapat dilakukan sebagai langkah preventif untuk menghindari *cyber crime*.

Teknologi yang terus berkembang juga membuat serangan *cyber* semakin kompleks dan sulit untuk dideteksi. Dalam konteks Indonesia, kejahatan siber juga menjadi masalah serius. Jenis-jenis kejahatan siber yang sering terjadi di Indonesia mencakup *malware*, *phishing*, DDoS, *cyber* stalking, identitas palsu, *cyber bullying*, kejahatan finansial, dan serangan pada infrastruktur kritis. Penting untuk terus memperbarui sistem keamanan dan meningkatkan kesadaran akan risiko *cyber crime* bagi pengguna internet. Selain itu, kerja sama lintas negara

juga penting untuk mengatasi kejahatan siber yang sering melibatkan pelaku dari berbagai negara.[43] Penanganan kejahatan siber menjadi semakin kompleks dan memerlukan upaya yang terkoordinasi dari berbagai pihak. Dalam era digital yang semakin maju, penting bagi individu, perusahaan, dan pemerintah untuk mengambil tindakan yang serius dalam melindungi diri dari ancaman *cyber crime* dan bekerja sama untuk menciptakan lingkungan *online* yang lebih aman. Indonesia menduduki peringkat kedua dunia untuk kejahatan dunia maya setelah Ukraina. *Cyber crime* merupakan jenis kejahatan baru yang melibatkan teknologi komputer dalam pelaksanaannya. *Cyber crime* mencakup berbagai jenis kejahatan seperti *hacking*, *phishing*, pornografi, penipuan *online,* dan pencurian nomor kartu kredit. Kejahatan dunia maya yang paling banyak terjadi di Indonesia adalah penyebaran konten provokatif dan penipuan *online*. [44]

Pada tahun 2022, terdapat 8.831 kasus kejahatan dunia maya yang dilaporkan oleh Polri dari Januari hingga Desember (Pusiknas Polri, 2022) Kejahatan dunia maya di Indonesia meliputi pembajakan perangkat lunak, terorisme dunia maya, penipuan (termasuk penipuan berbasis dunia maya dan pelanggaran hukum transaksi elektronik), peretasan, manipulasi data, web *phishing*, dan serangan dunia maya terhadap sistem keamanan digital. Penipuan saat ini merupakan jenis kejahatan yang paling banyak terjadi di Indonesia. [45]

[43] *Ibid.*, halaman 23 - 35
[44] *Ibid*., halaman 23 - 35
[45] hendri, D. "Dasar Pertimbangan Hakim Dalam Putusan Pengadilan Negeri Palembang Kepada Sanksi Tindak PidanaTerhadap Pelaku Penangkapan Ikan Menggunakan Bahan Peledak Dalam Putusan Nomor: 1/Pid.Sus-PRK/2018/PN.Plg'.

Pemerintah Indonesia telah mengambil langkah untuk memerangi kejahatan dunia maya dengan memberlakukan undang-undang seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Meskipun ada undang-undang keamanan siber di Indonesia, banyak kasus kejahatan siber telah disaksikan selama Covid-19. Kerentanan data pribadi publik Indonesia juga terungkap pada tahun 2020. Pakar keamanan dunia maya memperkirakan bahwa jumlah kejahatan dunia maya dan serangan mungkin meningkat hampir dua kali lipat karena teknologi komputerisasi modern dan keterampilan teknis perangkat lunak yang berbeda membuat individu melakukan kejahatan dunia maya.[46]

Memahami perlindungan korban dapat dilihat dari dua (2) pengertian:

1. Dimaknai sebagai perlindungan agar tidak menjadi korban kejahatan (maksudnya perlindungan Hak Asasi Manusia (HAM) atau kepentingan hukum seseorang).
2. Dimaknai sebagai memperoleh perlindungan asuransi/ganti rugi hukum atas kerugian/ketidakadilan

Orang yang menjadi korban (identik dengan penjaminan korban). Bentuk ganti rugi tersebut dapat berupa pembenaran/rehabilitasi, pemulihan

[46] Oheo Kaimuddin Haris, Sabrina Hidayat, and Riski Dwitasari. (2018). "Kejahatan *Carding* Sebagai Bentuk *Cyber crime* Dalam Hukum Pidana Indonesia *Carding* Crime as a Form of *Cyber crime* in Indonesian Criminal Law". jurnal Halu Oleo Legal, Vol. 5, No. 2. halaman 33 .

keseimbangan, antara lain dengan pengampunan, ganti rugi, seperti restitusi, ganti rugi, jaminan/kompensasi untuk kesejahteraan sosial, dan sebagainya.[47]

Adanya unsur-unsur internasional dari kejahatan *Carding* tentunya akan menimbulkan masalah tersendiri, khususnya berkenaan dengan masalah yurisdiksi. Yurisdiksi adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum). Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak ikut campur tangan. Yurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum. Berdasarkan asas umum dalam hukum internasional, setiap negara memiliki kekuasaan tertinggi atau kedaulatan atas orang dan benda ada dalam wilayahnya sendiri. Oleh karena itu, suatu negara tidak boleh melakukan tindakan yang bersifat melampaui kedaulatannya (*act of sovereignty*) di dalam wilayah negara lain, kecuali dengan persetujuan negara itu sendiri. bersifat melampaui kedaulatannya (*act of sovereignty*) di dalam wilayah negara lain, kecuali dengan persetujuan negara itu sendiri. [48]

Yurisdiksi merupakan prinsip dasar dari kedaulatan negara yang dibuat berdasarkan kepentingan dari negara tersebut. Beberapa negara telah menggunakan prinsip yurisdiksi ekstrateritorial dalam hukum nasionalnya. Prinsip ekstrateritorial ini digunakan ketika dampak yang ditimbulkan dari suatu tindak pelanggaran berakibat kepada banyak pihak. Kondisi lain yang dapat

[47] Asliani Harahap. 2024. "Legal Protection Against Rape Victims Based On Victimology". Jurnal kepangkatan dosen UMSU. Volume 1. Halaman 7

[48] *Opt cit.*. Oheo Kaimuddin Haris, Sabrina Hidayat, and Riski Dwitasari, halaman 33

menimbulkan penggunaan prinsip ekstrateritorial adalah ketika wilayah tempat terjadinya tindak pelanggaran tersebut tidak mengaturnya namun tetap merugikan pihak lain akibat tindak pelanggaran tersebut.

Pemberlakuan prinsip ekstrateritorial secara materiilnya tergambar atau dapat kita lihat di dalam Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pada pasal 2, yakni bahwa pengaturan teknologi informasi yang diterapkan oleh suatu negara berlaku untuk setiap orang yang melakukan perbuatannya baik yang berada di wilayah negara tersebut maupun di luar negara apabila perbuatan tersebut memiliki akibat di Indonesia. Butuhnya pengaturan yurisdiksi ekstrateritorial dikarenakan kejahatan *Carding* dapat merugikan kepentingan orang atau negara walaupun perbuatan *locus delicti* dilakukan di wilayah negara lain. Oleh karena itu, peraturan mengenai pemanfaatan teknologi informasi dan komunikasi tersebut harus dapat mencakup perbuatan yang dilakukan di luar wilayah Indonesia tetapi merugikan kepentingan orang atau negara dalam wilayah Indonesia.[49]

Berdasarkan pengertian dari pasal 2 Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut menunjukkan bahwa sebenarnya penggunaan prinsip yurisdiksi ekstrateritorial dalam menyelesaikan permasalahan hukum yang mencakup lebih dari satu wilayah teritorial suatu negara terkait penggunaan teknologi informasi dapat diterapkan selama perbuatan yang dilakukan oleh warga negara ataupun Permasalahan lainnya yang timbul

[49] *Opt cit.*., Oheo Kaimuddin Haris, Sabrina Hidayat, and Riski Dwitasari, halaman 33.

terkait prinsip ini yakni bentuk pemberlakuan dalam penerapan prinsip yurisdiksi ekstrateritorial tersebut.[50] Meskipun prinsip ini terlihat di dalam Undang-undang nomor 11 tahun 2008 pasal 2, pemberlakuan prinsip ini tidak dapat dipergunakan secara meluas dengan paksaan atau kehendak dari negara pembuat undang-undang (dalam hal ini Indonesia), melainkan dibutuhkan adanya pengakuan peratifikasian yang dilakukan oleh suatu negara. Seperti contohnya di Indonesia, pemberlakuan prinsip yurisdiksi ekstrateritorial yang tercantum dalam pasal 2 tersebut tidak mengikat dan menjadi aturan hukum umum bagi negara lain selama pemberlakuan Undang-undang nomor 11 tahun 2008 tersebut hanya bagi negara Indonesia (tidak adanya peratifikasian yang dilakukan oleh negara lain). [51]

Untuk melakukan upaya pencegahan kejahatan *Carding* perlu adanya penguatan pada Undang-undang Nomor 11 Tahun 2008.[52] Penguatan hukum tersebut dimaksudkan untuk mengefektifkan fungsi pencegahan (preventif), sehingga kejahatan tersebut tidak lagi timbul. Berdasarkan tabel di atas, terdapat beberapa norma dari *Convention on Cyber crime* yang telah diadopsi ke dalam UU ITE, yaitu mengenai *Illegal access, Illegal Interception, Data Interference, System Interference, Misuse of Device, Computer Related Forgery, Offences*

[50] Brigita Cynthia Liwandra Denata and Aju Putrijanti. (2023). "Perlindungan Hukum Bagi Pemegang Kartu Kredit Atas Tagihan Yang Tidak Benar". Jurnal Notarius. volume 16.3. halaman 98.

[51] Diyu Sulaeman and Anyelir Puspa Kemala. (2025). "Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia". Jurnal Politik, Sosial, Hukum Dan Humaniora. volume 3.2. halaman 48.

[52] Mehda Zuraida. (2024). "Credit Card Fraud *Carding* Dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia". Jurnal Analisis Hubungan Internasional. Vol. 4, No. 1, halaman 42.

Related to Child Pornography.[53] Penyertaan dan kerja sama internasional. Maka perlu adanya penambahan pasal ke dalam UU ITE agar sesuai dengan ketentuan di dalam CoC, yaitu : *Computer Related Fraud* : 6HWLDSorang dengan sengaja dan tanpa hak menyebabkan kerugian kepada seseorang dengan cara :

a. Memasukkan, mengubah, menghapus atau menahan data komputer;

b. Mengganggu fungsi sistem komputer dengan niat tidak jujur dan menipu untuk menguntungkan diri sendiri atau membantu pelanggaran yang ditetapkan dalam pasal *International Co-operation*, [54] Kerjasama internasional dibutuhkan untuk proses penyidikan yang tidak berada di satu yurisdiksi negara saja, namun terdapat di beberapa negara. Di dalam CoC terdapat beberapa ketentuan mengenai kerja sama internasional yang dapat mempermudah proses penyidikan, yaitu :

1. Pasal 24 *Extradition* Konvensi ini membuka penerapan prinsip yurisdiksi seluas-luasnya sehingga dapat diterapkan dalam menangani kasus *cyber crime* secara optimal. Pengaturan pada pasal ini berarti bahwa masing-masing pihak harus melakukan tindakan-tindakan lainnya sebagaimana diperlukan untuk menetapkan yurisdiksi atas setiap pelanggaran yang dilakukan sesuai dengan pasal 2 sampai 11 dari konvensi ini apabila pelanggaran tersebut dilakukan :

[53] N A Kurniawan. (2014). "Pencegahan Kejahatan *Carding* Sebagai Kejahatan Transnasional Menurut Hukum Internasional". Jurnal Mahasiswa Fakultas Hukum Universitas Brawijaya. halaman 14.

[54] Insan Pribadi. (2018). "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana". Jurnal Lex Renaissance. volume 3.1. halaman 24.

a. Di wilayahnya; atau

b. Di atas kapal yang berbendera pihak tersebut;

c. Di atas kapal yang terdaftar menurut hukum pihak tersebut

d. Oleh salah satu warga negaranya apabila pelanggaran tersebut dikenakan hukuman berdasarkan hukum pidana dimana hal tersebut dilakukan atau apabila pelanggaran tersebut dilakukan di luar yurisdiksi wilayah negara manapun.[55]

Masing-masing pihak berhak untuk tidak menggunakan atau menggunakan hanya dalam kasus-kasus atau keadaan-keadaan khusus aturan yurisdiksi yang ditetapkan dalam ayat (1).b sampai 1.d dari pasal ini atau dari setiap bagiannya. Masing-masing pihak dapat melakukan tindakan-tindakan sebagaimana diperlukan untuk menetapkan yurisdiksi atas pelanggaran-pelanggaran yang dimaksudkan dalam pasal 24 ayat (1), dalam kasus dimana pelanggar yang diduga berada di wilayahnya dan pihaknya tidak mengekstradisi orang tersebut kepada pihak lainnya semata-mata berdasarkan kebangsaannya, setelah permohonan ekstradisi.[56]

2. Pasal 25 *General principal relating to mutual assistance* Para negara anggota harus saling memberikan bantuan semaksimal mungkin untuk penyidikan-penyidikan atau penuntutan, menerapkan undang-undang dan tindak-tindakan lain yang diperlukan untuk pelaksanaan kewajiban-

[55] *Ibid*., halaman 24
[56] *Ibid*., halaman 24.

kewajiban yang disebutkan dalam pasal 27-35. Ketentuan tentang *mutual assistance,* termohon diperbolehkan untuk memberikan bantuan hanya jika ada kriminalitas ganda. [57]

3. Pasal 26 *Spontaneous information* Negara anggota berhak dalam batas dari undang-undang dan tanpa permintaan sebelumnya, meneruskan informasi yang didapat melalui kerangka penyidikannya sendiri kepada pihak lain dan pihak penyedia informasi dapat meminta agar kerahasiaan informasi tersebut dijaga atau hanya bisa digunakan atas persyaratan tertentu Para negara anggota harus saling memberikan bantuan semaksimal mungkin untuk penyidikan-penyidikan atau penuntutan, menerapkan undang-undang dan tindak-tindakan lain yang diperlukan untuk pelaksanaan kewajiban-kewajiban yang disebutkan dalam pasal 27-35. Ketentuan tentang *mutual assistance,* termohon diperbolehkan untuk memberikan bantuan hanya jika ada kriminalitas ganda. [58]
4. Pasal 26 *Spontaneous information* Negara anggota berhak dalam batas dari undang-undang dan tanpa permintaan sebelumnya, meneruskan informasi yang didapat melalui kerangka penyidikannya sendiri kepada pihak lain dan pihak penyedia informasi dapat meminta agar kerahasiaan informasi tersebut dijaga atau hanya bisa digunakan atas persyaratan tertentu.

[57]Hasan. "Pertimbangan Hakim Atas Tindak Pidana Pencurian Dengan Modus *Carding* berdasarkan Undang – Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik".

[58] Cole Durham. (2022). "Amicus Curiae". Jurnal hukum Revista Latinoamericana de Derecho y Religión. halaman 11.

5. Pasal 27-28 *Procedures pertaining to mutual assistance requests in the absence of applicable international agreements* Pasal ini mengatur tentang permintaan bantuan tanpa perjanjian internasional dengan menunjuk satu otoritas sentral atau otoritas-otoritas yang bertanggung jawab untuk mengirim dan menjawab permintaan-permintaan bantuan, mengeksekusi, memberitahukan kepada otoritas yang kompeten untuk melakukan eksekusi. [59]
6. Pasal 29-30 *Mutual assistance regarding provisional measures* Pasal ini mengatur ketentuan-ketentuan khusus tentang pemeliharaan data yang tersimpan dalam komputer yang berlokasi di dalam wilayah pihak negara lain.
7. Pasal 31-35 *Mutual assistance regarding investigative powers* Negara anggota diperbolehkan meminta pihak negara lain untuk mencari atau mengakses, menyita atau mengamankan data yang tersimpan dengan menggunakan sistem komputer yang berlokasi di dalam wilayah pihak termohon.[60]

Penanganan kasus kejahatan *Carding*diterapkan pada Pasal 378 KUHP yang dikenakan untuk kasus *Carding* yaitu dimana pelaku melakukan penipuan dengan menggunakan data atau identitas milik orang lain untuk bisa mendapatkan keuntungan dari kartu kredit milik orang lain untuk bisa

[59] Adik, N. (2021). "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi". Jurnal Hukum Pidana Dan Kriminologi. halaman 29.

[60] Dewi Maesyaroh. (2024). "Peran Digital Forensik Terhadap Pencurian Data Pribadi Sektor Perbankan Digital". Datin Law Jurnal. halaman 28.

dibelanjakan secara *online* dalam melakukan transaksi di *e-commerce.* Adanya kebijakan dalam pengaturan tindak pidana *Carding* terdapat di dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu yang berkaitan dengan perbuatan menggunakan dan atau mengakses kartu kredit orang lain secara tanpa hak. Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11Tahun 2008 tentang Informasi dan Transaksi Elektronik hanya dapat menjangkau pelanggaran pemalsuan data kartu kredit pada tahapan *card embossing and encoding.* [61]

Tidak semua modus operandi dalam tahapan tersebut dapat terjangkau, karena ketentuan Pasal 35 jo. Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik hanya mengatur perbuatan yang dilakukan oleh orang yang menggunakan kartu kredit tetapi tidak termasuk pedagang yang juga dapat menjadi pelaku tindak pidana *Carding*. Dalam penjelasan unsur-unsur Pasal 35 Undang-Undang ITE menjelaskan, setiap orang dilarang dengan sengaja dan melawan hukum: [62]

a. Menggunakan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak dengan maksud memperoleh informasi data keuangan dari lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya.

[61] *Opt cit.*, Insan Pribadi, halaman 24..
[62] *Opt cit.*, Dewi Maesyaroh, halaman 28.

b. Menggunakan dan atau mengakses dengan cara apa pun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan. Terjadinya *Carding* oleh pelaku *carder* dengan cara memperoleh data kartu kredit secara tidak sah dengan memanfaatkan teknologi informasi (Internet) yaitu menggunakan nomor kartu kredit orang lain untuk melakukan pemesanan barang secara *online*. Komunikasi awalnya dibangun melalui email untuk menanyakan kondisi barang dan melakukan transaksi.

Setelah terjadi kesepakatan, pelaku memberikan nomor kartu kreditnya dan penjual mengirimkan barangnya. *Carding* sendiri merupakan Tindakan pidana yang bersifat *illegal interception*, dan kemudian menggunakan nomor kartu kredit tanpa kehadiran fisik kartunya untuk belanja. Modus ini dapat terjadi akibat lemahnya sistem *authentication* yang digunakan dalam memastikan identitas. Permasalahan hukum dalam kejahatan *Carding* yaitu ketika terkait dengan penyampaian informasi, pengaturan, komunikasi dan transaksi secara elektronik, khususnya dalam pembuktian hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik. [63]

Carding sendiri merupakan bagian *cyber crime* dalam transaksi *online* yang menggunakan sarana internet sebagai basis transaksi khususnya sistem layanan *online*. Jadi sejauh ini kasus *Carding* di Indonesia baru bisa di atasi dengan Pasal 378 dalam KUHP dan Pasal 51 ayat (1) Jo Pasal 35 atau Pasal 48 Jo

[63] Oky Syalendro, Arief Fahmi Lubis, and R. Yusak Andri Ende Putra. (2025). "Tindak Pidana *Cyber crime* Dalam Hukum Indonesia Serta Upaya Dan Penanganan Kasus Tindak Pidana *Cyber crime*". Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia. halaman 47.

Pasal 32 dalam Undang-Undang ITE. [64] Menurut G. P. Hoefnagels, mengemukakan bahwa sanksi dalam hukum pidana adalah semua reaksi terhadap pelanggar hukum yang ditentukan oleh undang-undang dimulai dari penahanan tersangka dan penuntutan terdakwa sampai pada penjatuhan vonis oleh hakim. Penetapan sanksi dalam hukum pidana merupakan suatu rangkaian kebijakan dalam suatu sistem pemidanaan.[65]

Beberapa teori mengenai tujuan pemidanaan atau pemberian sanksi pidana yang umum diterima dalam hukum pidana, yaitu:

1. Teori Absolut atau Pembalasan

   Pemidanaan merupakan pembalasan secara absolut atas kesalahan yang telah dilakukan, yang berorientasi pada perbuatan dan terjadinya kejahatan itu sendiri. Oleh karena itu teori ini disebut juga dengan Teori Pembalasan. Melalui teori ini dapat diketahui bahwa pemidanaan diberikan karena orang melakukan kejahatan *quia peccatum* dan bukan untuk mencapai tujuan yang lain. Dengan demikian, pemidanaan merupakan suatu retribusi yang adil bagi kerugian yang sudah diakibatkan. Adapun pembagian yang lain mengenai teori ini yaitu:

   a. Teori pembalasan yang objektif, yaitu: berorientasi pada pemenuhan kepuasan dari perasaan dendam dari masyarakat.

---

[64] *Ibid.*, halaman 47

[65] Miftakhur Rokhman Habibi and Isnatul Liviani. (2020). "Kejahatan Teknologi Informasi (*Cyber crime*) Dan Penanggulangannya Dalam Sistem Hukum Indonesia". Jurnal Pemikiran Dan Pembaharuan Hukum Islam. halaman 26.

b. Teori pembalasan yang subjektif, yaitu: berorientasi pada pembuat kejahatan, dimana kesalahan pembuat kejahatanlah yang harus mendapat balasan.

2. Teori Relatif

Teori ini mendasarkan pandangan mengenai maksud atau tujuan dari pemidanaan yaitu untuk perlindungan masyarakat dan pencegahan terjadinya kejahatan. Pemidanaan dilakukan supaya orang jangan melakukan kejahatan. Adapun teori ini terbagi yaitu:

a. Teori Prevensi Umum yaitu pencegahan ditujukan kepada masyarakat pada umumnya, untuk menciptakan tekanan jiwa sehingga masyarakat takut untuk melakukan kejahatan bahwa pemidanaan diberikan dengan tujuan menakuti melalui hukuman yang berat. Pemidanaan ditujukan untuk melindungi masyarakat terhadap perbuatan-perbuatan jahat melalui pengasingan terhadap penjahat.

b. Teori Prevensi Khusus yaitu pencegahan ditujukan kepada orang yang melakukan kejahatan supaya tidak lagi melakukan kejahatan. Dalam teori ini terdapat unsur reparasi atau memperbaiki pribadi penjahat.

3. Teori Integratif atau Penyatuan Pandangan Grotius yang mengatakan bahwa secara kodrat, siapa pun yang melakukan kejahatan akan terkena

derita, namun dalam menetapkan berat ringannya derita yang dikenakan tergantung pada kemanfaatan sosial.[66]

Tindak pidana kejahatan *Carding* di Indonesia, sanksi yang ditetapkan terhadap terdakwa didasarkan pada Undang-Undang ITE sebagai *lex specialis*, tidak tertutup kemungkinan dapat juga digunakan KUHP sebagai *lex generalis*, tergantung pada penilaian hakim terhadap fakta persidangan dan alat bukti yang dihadirkan. Khusus untuk Undang-Undang ITE, sanksi pidana yang ditekankan ialah sanksi pidana penjara dan pidana denda, sebagaimana yang ditegaskan dalam Pasal 45-Pasal 52 dari Undang-Undang ITE tersebut. Pengaturan sanksi pidana terhadap tindak pidana *Carding* di Indonesia sangat menekankan teori absolut atau pembalasan, karena dari teori absolut atau pembalasan ini menekankan aspek retribusi yang adil terhadap pelaku tindak pidana *Carding* yang dilakukannya karena kerugian yang terjadi. Adanya pembalasan dendam masyarakat terhadap pelaku tindak pidana *Carding* yaitu *carder* atau hacker. Mekanisme teori absolut atau pembalasan terdapat suatu upaya untuk melindungi masyarakat dari kejahatan *Carding*, sekaligus untuk mencegah terjadinya kejahatan yang serupa di kemudian hari. [67]

Penerapan sanksi pidana yang menekankan sisi pembalasan dalam pidana penjara dan denda yang diatur oleh Undang-Undang ITE menunjukkan bahwa pemidanaan di Indonesia *Carding* sama sekali tidak memperhatikan aspek kuratif terhadap pelaku tindak pidana. Hukum pidana diciptakan untuk mengembalikan

[66] Sigid Suseno and n Syarif A. Barmawi. (2004). "Kebijakan Pengaturan *Carding* Dalam Hukum Pidana Di Indonesia". Jurnal Ilmu - Ilmu Sosial Dan Humaniora, volume. 6. halaman 55

[67] Rofikah. 2014. "Model Penanggulangan *Carding*". Jurnal Yustisia, no. 90. halaman 82.

situasi harmoni dan seimbang sebagaimana awal terciptanya masyarakat. Keadaan masyarakat yang aman, hukum pidana harus memperhatikan semua aspek yang terlibat dalam satu tindak pidana, khususnya korban, pelaku, dan masyarakat secara keseluruhan. [68]

Penerapan suatu sanksi pidana yang berlatar belakang pembalasan sebagaimana diatur dalam Undang-Undang ITE, tidak akan mampu mengembalikan situasi masyarakat yang harmoni dan seimbang apabila aspek penyembuhan terhadap pelaku tindak pidana *Carding* tidak diperhatikan. Pengaturan mengenai sanksi pidana dalam Undang-Undang ITE, harus menekankan juga sanksi tindakan *maatregel*. Sanksi tindakan yang diterapkan dalam hukum pidana terfokus pada aspek kuratif atau penyembuhan pelaku, yaitu agar pelaku dapat berubah dari suatu perbuatannya yang jahat menuju kepribadian yang bermanfaat bagi masyarakat. Sanksi tindakan dapat menekankan suatu aspek pembelajaran yang positif terhadap sisi ilmiah atau keilmuan dari para pelaku kejahatan *Carding* dapat di didik dan bisa mempelajari lebih lanjut secara positif untuk bisa dapat mengembangkan kemampuannya yang sewaktu-waktu bisa dapat digunakan oleh penegak hukum dan pihak perbankan untuk membantu mengungkap dan menyelesaikan masalah kejahatan *cyber crime* atau kejahatan *Carding*di masa yang akan datang.[69]

Ditinjau dari perspektif hukum pidana konvensional sebagaimana diatur dalam KUHP, maka *Carding* sejatinya dapat dipandang sebagai pencurian dengan

[68] Ginara, Widyantara, and Styawati. 2023. "Kriminalisasi Terhadap Kejahatan *Carding* Sebagai Bentuk *Cyber crime* Dalam Hukum Pidana Indonesia". Jurnal Hukum. Halaman 40

[69] Ibid'., halaman 40

pemberatan. Pasal 362 KUHP tentang pencurian menyatakan bahwa barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam pidana penjara paling lama lima tahun. Bila ditambahkan dengan pemberatan sesuai Pasal 363 karena dilakukan oleh lebih dari satu orang atau dengan cara khusus (dalam hal ini menggunakan teknologi), maka ancamannya bisa ditingkatkan. Perluasan interpretasi bahwa data pribadi termasuk "barang tidak berwujud tetapi bernilai ekonomi" semestinya memungkinkan KUHP untuk diterapkan secara paralel atau kumulatif dengan UU ITE. Kelemahan hukum ITE dalam menanggulangi *Carding*juga terletak pada minimnya pengakuan terhadap status korban dan kerugian konkret. Dalam perkara ini tidak diuraikan siapa korban kartu kreditnya secara jelas, dan tidak dihitung secara spesifik berapa nilai kerugiannya. Aspek ini menyebabkan sistem peradilan cenderung menilai ringan perkara tersebut. Padahal, dalam banyak yurisdiksi lain seperti Amerika Serikat atau negara-negara Uni Eropa, tindak pidana pencurian data pribadi dan penyalahgunaan informasi kartu kredit dianggap sebagai bentuk pencurian identitas dan penipuan berat, dengan ancaman pidana bertahun-tahun bahkan puluhan tahun. [70]

Di Indonesia, absennya sistem pemantauan dampak dan tidak adanya ketegasan terhadap jaringan kejahatan membuat aparat hukum lebih cenderung melihat pelaku hanya sebagai individu tunggal, bukan bagian dari jejaring yang lebih besar. Hal ini terlihat dari minimnya upaya untuk mengungkap pelaku utama pemilik data, pembobol sistem, atau pembuat malware yang memperoleh data

[70] *Ibid.*, halaman 40

kartu kredit. Secara teoritis, sistem hukum pidana memiliki dua tujuan utama: menjerakan pelaku dan mencegah terulangnya kejahatan oleh pihak lain. Namun dengan hanya menjatuhkan vonis delapan bulan penjara terhadap pelaku yang sadar, sistematis, dan berulang-ulang melakukan tindakan sebagai perantara *Carding*, negara justru menunjukkan ketidakmampuan dalam mengendalikan tindak kejahatan siber. Ketika pemidanaan tidak mencerminkan bobot kejahatan, maka nilai pencegahannya hilang.[71]

Masyarakat yang memiliki keahlian teknologi dan akses terhadap forum digital bisa saja tergoda melakukan hal serupa, karena tahu bahwa ancaman hukumannya rendah dan bisa dinegosiasikan di pengadilan. Hal ini merupakan bentuk ketidakadilan tidak hanya terhadap korban, tetapi terhadap sistem hukum itu sendiri.[72] Maka dalam perspektif keadilan hukum dan efektivitas perlindungan terhadap hak elektronik, perlu disarankan agar pendekatan terhadap kejahatan siber seperti *Carding* dilakukan secara integral. Salah satunya adalah dengan memanfaatkan pasal-pasal KUHP tentang pencurian dan penipuan secara bersamaan dengan UU ITE. Tindak pidana pencurian data kartu kredit, walau tidak menyentuh barang fisik, memiliki karakteristik yang identik dengan pencurian konvensional, bahkan lebih canggih dan berdampak luas. Pasal 32 ayat (2) UU ITE jo Pasal 362 atau 378 KUHP maka tuntutan dan putusan bisa mencerminkan kejahatan itu secara utuh, termasuk niat jahat, keuntungan ekonomi, dan kerugian korban. Selain itu, perlu dilakukan revisi UU ITE yang

[71] *Ibid.*, halaman 40
[72] *Ibid.*, halaman 40.

secara tegas memasukkan data kartu kredit sebagai "objek ekonomi yang dilindungi", dan menambahkan ketentuan pidana khusus terhadap pelaku yang berperan dalam perantara transaksi seperti rekber yang digunakan dalam aktivitas ilegal. [73]

Penanggulangan *Carding* tidak cukup hanya melalui pemidanaan ringan terhadap pelaku lapangan. Negara perlu membangun sistem penegakan hukum yang adaptif, menyesuaikan dengan perkembangan teknologi digital dan jaringan kriminal global. Jika tidak, kejahatan seperti *Carding* akan terus berkembang, sementara sistem hukum tertinggal dalam menanganinya. Putusan seperti perkara Kingditho hanya menjadi catatan yuridis yang membenarkan praktik impunitas dan absennya keadilan substantif. Ketika kejahatan digital tidak ditindak tegas, bukan hanya data yang dicuri, tapi juga kepercayaan masyarakat terhadap hukum itu sendiri. [74]

C. Kendala Dalam Pertanggungjawaban Pidana atas Kejahatan Pencurian Kartu Kredit *Carding* Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Studi Kasus No.845/Pid.Sus/2020/PT SBY

Praktik hukum di Indonesia aturan mengenai hukum siber merupakan suatu hal yang memiliki tantangan tersendiri, hal ini karena peraturan perundang-undangan yang mengatur mengenai hukum siber sendiri dinilai masih “seumur jagung”. kedudukan hukum siber membawa implikasi ke dalam perubahan yang terjadi di dalam masyarakat, perubahan seperti semakin canggihnya teknologi

[73] *Ibid.,* halaman 40
[74] Putusan Mahkamah Agung. "Nomor 845/PID.SUS/2020/PT SBY".

komputer telah membantu manusia dalam kehidupan sehari-hari yang lebih mudah terutama pada bidang pekerjaan, penyalahgunaan teknologi komputer sebagai sarana untuk melakukan kejahatan dalam perkembangannya menimbulkan persoalan yang cukup rumit terutama pada proses pembuktian pidananya, hal ini dikarenakan kejahatan yang dilakukan dengan komputer dinilai memiliki karakteristik sendiri sehingga berbeda dengan kejahatan pada umumnya.[75]

Salah satu cara paling efektif untuk melindungi situs web dari peretas adalah dengan selalu memperbarui perangkat lunak. [76] Perusahaan harus menginstal SSL dan *plugin* keamanan, memiliki perangkat lunak keamanan terbaru, dan menggunakan HTTPS. Penting juga untuk berinvestasi dalam pencadangan otomatis. Sekalipun semua tindakan lain diambil, masih ada risiko kehilangan segalanya karena peretasan situs web. Mencadangkan informasi secara teratur dapat membantu mencegah hal ini. Cara lain untuk melindungi situs web dari peretas adalah dengan berhati-hati saat menerima unggahan *file* melalui situs. Saat seseorang memiliki opsi untuk mengunggah sesuatu ke situs web, mereka dapat menyalahgunakan hak istimewa tersebut dengan memuat *file* berbahaya. [77]

Baik pemerintah maupun personal juga harus memeriksa kata sandi secara teratur. Kata sandi harus kuat dan unik untuk setiap akun. Penting juga untuk memantau log aktivitas secara teratur karena membantu memberi sinyal perubahan sehingga aktivitas yang tidak sah dapat dihentikan sejak awal.

---

[75] Situmeang. *CYBER LAW*.

[76] Ichwan Kurnia, 2024, *Hukum Pidana Siber*, Jawa Tengah: CV. Eureka Media Aksara. halaman 36

[77] *Ibid.*, halaman 36

Terakhir, pemerintah atau personal perlu menyadari bahwa melindungi situs web mereka dari peretas dan serangan berbahaya adalah proses yang berkelanjutan. Mereka perlu menyadari perubahan ancaman dan mengambil langkah proaktif menuju keamanan (Nirvana, 2021). Kejahatan siber di Indonesia telah mencatat berbagai peristiwa penting yang menitikberatkan terhadap dampak negatif yang ditimbulkannya, misalnya saja kerugian finansial, permasalahan diplomasi. Berbagai saran dan upaya pencegahan juga telah dilakukan diantaranya terkait penggunaan kata sandi kuat dan pemahaman tentang hak privasi kepada masyarakat. [78] Pembahasan ini juga menggarisbawahi tentang pentingnya pembaruan secara terus-menerus dalam keamanan siber untuk melindungi data dan sistem *online*, karena tantangan ini akan terus meningkat seiring dengan perkembangan teknologi. dan tindakan pemerasan dan pengancaman Unsur-unsur yang terdapat dalam pasal 27 merupakan pengembangan modus kejahatan seperti yang terdapat pada KUHP hanya saja pada UU ITE modus kejahatan dilakukan dengan media komputer.

Sebelum berbicara mengenai aturan yang berlaku di Indonesia, terlebih dahulu akan dijelaskan mengenai yurisdiksi *cyber* space. Yurisdiksi sendiri merupakan kekuasaan atau kompetensi hukum suatu Negara terhadap orang, benda maupun peristiwa hukum yang direfleksikan dari prinsip dasar kedaulatan, kesamaan derajat, dan tidak campur tangan sebuah Negara. Makna dari yurisdiksi sendiri selalu membahas mengenai persoalan wilayah, akan tetapi dalam praktiknya setiap Negara tetap memiliki kedaulatan untuk mengadili suatu tindak

[78] *Ibid.*, halaman 36

pidana yang dilakukan diluar wilayah negaranya, dikarenakan hal tersebut didasari dengan adanya prinsip-prinsip dalam Hukum Internasional yang berlaku, diantaranya: [79]

1. Prinsip teritorial, dalam hal kejahatan siber prinsip ini dapat digunakan karena dalam perkembangannya mengalami perluasan makna sehingga dapat meliputi perbuatan pidana yang dilakukan menggunakan media komputer atau internet, yang seharusnya bersifat tidak dapat disentuh.
2. Prinsip nasionalitas, memiliki makna suatu Negara dapat mengadili warga negaranya dimanapun dia berada, prinsip ini dibedakan menjadi dua, yaitu prinsip nasional aktif dan juga prinsip nasional pasif.
3. Prinsip perlindungan, prinsip ini merupakan sebuah upaya sebuah Negara untuk melindungi kepentingan vital Negara tersebut, sehingga Negara memiliki kewenangan untuk mengadili Warga Negara Asing yang berbuat kejahatan di dalam maupun luar negaranya yang mengancam keamanan Negara tersebut.
4. Prinsip universal, menilai bahwa setiap Negara memiliki kewenangan untuk mengadili tindak kejahatan tertentu, dan hal tersebut diterima secara umum karena dianggap sebagai tindakan yang mengancam masyarakat internasional. Dalam menentukan kewenangan hukum pidana siber di Indonesia, diuraikan dari segi tempat atau biasa disebut *locus delicti* yang mana untuk menentukan apakah hukum pidana

[79] Edrisy. *Pengantar Hukum Siber*.

Indonesia berlaku untuk mengadili perbuatan pidana tersebut atau tidak, berhubungan dengan kompetensi relatif pengadilan mana yang berwenang mengadili perkara tersebut.

Istilah "kebijakan kriminalisasi" mengacu pada proses di mana suatu tindakan yang sebelumnya tidak ilegal dibuat sedemikian rupa oleh undang-undang. Karena menggunakan mekanisme hukum pidana, maka kebijakan kriminalisasi dapat dianggap sebagai bagian dari kebijakan hukum pidana yang lebih luas. Sejak Proklamasi Kemerdekaan Indonesia, proses kriminalisasi terus berlanjut. Sekarang ada beberapa delik baru berkat UU No. 1 Tahun 1946. Perlunya jenis delik baru ini mencerminkan budaya dan iklim politik pada saat dikodifikasi menjadi undang-undang. Berikut ini adalah contoh mengapa perilaku tertentu dikriminalisasi: [80]

a) Ada reaksi sosial karena;

b) Perbuatan ini merugikan masyarakat;

c) Sudah sering dilakukan; dan

d) Ada bukti.

Dengan menggunakan keempat kriteria tersebut, tidak selalu suatu perbuatan yang tidak dikehendaki memenuhi ambang batas formalisasi sebagai perbuatan pidana (kejahatan). Tindakan mencuri data kartu kredit dan menggunakan untuk transaksi pembelian secara ilegal di *platfrom* belanja *online*.

[80] Diyu Sulaeman and Anyelir Puspa Kemala. 2020 "Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia". Jurnal hukum. Halaman 54

Carding biasanya dilakukan dengan cara memperoleh informasi kartu kredit korban secara tidak sah, baik melalui pencurian data, penipuan, atau kebocoran data. Modus operandi *Carding* ini dimungkinkan karena sistem pengecekan identitas dan keabsahan kartu kredit di toko *online* seringkali tidak cukup kuat atau tidak cukup ketat. Oleh karena itu, pelaku dapat dengan mudah menggunakan data kartu kredit yang dicuri untuk berbelanja secara ilegal. [81]

Pasal 56 KUHP tentang penyertaan digunakan untuk menjerat pelaku tidak langsung seperti dalam kasus ini, namun kembali lagi bahwa penjatuhan pidana berdasarkan peran pembantu cenderung lebih ringan dibanding pelaku utama. Hal ini menjadi kendala serius karena dalam praktiknya, pelaku seperti Kingditho justru menjadi penghubung utama dan fasilitator yang mempermudah transaksi ilegal terjadi. UU ITE juga masih terbatas dalam memberikan pengaturan menyeluruh terhadap skema pertanggungjawaban pidana kolektif dalam jaringan kejahatan siber. Kejahatan *Carding* tidak dilakukan secara individu, melainkan melibatkan kelompok terorganisir lintas negara, dengan pembagian peran seperti *hacker*, penjual data, pembeli, dan perantara transaksi, dalam sistem hukum Indonesia, belum ada mekanisme khusus untuk menjerat jaringan atau organisasi kejahatan siber secara holistik. Akibatnya, pengadilan hanya mengadili individu berdasarkan peran tunggal, terpisah dari konteks jaringan yang lebih besar. [82]

Tidak ada upaya lebih lanjut untuk menelusuri, menyita hasil kejahatan, atau mengembangkan kasus terhadap pelaku utama pemilik data curian. Kendala

[81] *Ibid.,* halaman 54
[82] *Opt cit*., Diyu Sulaeman and Anyelir Puspa Kemala, halaman 54

teknis lainnya adalah kurangnya alat dan kapasitas penyidikan yang memadai dalam menghadapi bukti elektronik. Meskipun barang bukti berupa laptop, ponsel, dan rekening bank ditemukan, namun dalam praktiknya proses penyidikan terhadap jejak digital, pelacakan IP *address*, dan identifikasi jaringan komunikasi *online* sering kali terbentur dengan keterbatasan sumber daya teknologi di kepolisian. padahal dalam tindak pidana seperti pencurian dan penipuan, keberadaan korban dan kerugian nyata sangat penting untuk menguatkan aspek moral dan hukum dari pertanggungjawaban pidana. [83]

Pertimbangan hakim yang lebih meringankan juga mencerminkan kendala dari sudut ideologis dan sosiologis hukum. Dalam banyak kasus, pelaku *Carding* masih dianggap sebagai pelaku "kejahatan tanpa korban langsung", yang artinya tidak menyebabkan penderitaan fisik atau sosial secara kasat mata. Karena itu, pidana yang dijatuhkan sering kali bersifat lunak, dengan dalih pemuda, tidak bekerja, atau baru pertama kali melakukan. Dalam kasus ini, fakta bahwa terdakwa sudah menjalani peran sebagai rekber sejak 2017 tidak membuat hukuman menjadi lebih berat, melainkan seolah dianggap sebagai masa lalu yang tidak terlalu membahayakan. Hal ini menunjukkan bahwa sistem pemidanaan belum melihat kejahatan digital sebagai bentuk kejahatan serius dengan efek destruktif jangka panjang terhadap sistem keuangan dan hukum. Kendala lainnya yang tak kalah penting adalah absennya harmonisasi antara UU ITE dengan Kitab Undang-Undang Hukum Pidana (KUHP). Padahal, jika tindak pidana *Carding*ini dimaknai secara analogi sebagai pencurian data dengan niat memperoleh

[83] *Opt cit*., Diyu Sulaeman and Anyelir Puspa Kemala, halaman 54.

keuntungan ekonomi, maka Pasal 362 KUHP tentang pencurian atau Pasal 378 KUHP tentang penipuan bisa digunakan sebagai dasar kumulatif dalam penuntutan. Dengan pendekatan ini, pertanggungjawaban pidana tidak akan lagi terbatas pada soal "pemindahan informasi elektronik", tetapi mencakup pula pengambilan keuntungan dari milik orang lain tanpa hak yang dalam KUHP sudah memiliki struktur pembuktian dan ancaman pidana yang lebih mapan. [84]

Ketiadaan instrumen sanksi tambahan seperti pencabutan hak akses internet, penutupan akun media sosial, atau larangan menggunakan alat komunikasi untuk jangka waktu tertentu juga merupakan hambatan dalam memberikan efek jera. Dalam kasus ini, terdakwa menggunakan akun *Facebook*, rekening bank, dan berbagai alat elektronik untuk menjalankan transaksi ilegal, namun setelah vonis pidana, tidak ada satu pun ketentuan yang mengatur pelarangan penggunaan kembali alat atau sarana tersebut pasca hukuman dijalani. Akibatnya, potensi pengulangan kejahatan tetap terbuka karena pelaku tidak dibatasi secara teknis.

[84] *Opt cit*., Diyu Sulaeman and Anyelir Puspa Kemala, halaman 54.

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Berdasarkan studi kasus No. 845/Pid.Sus/2020/PT SBY, perbuatan pelaku *Carding*yang mencuri dan memanfaatkan data kartu kredit orang lain melalui media elektronik memenuhi unsur tindak pidana dalam Pasal 30 jo. Pasal 46 dan Pasal 32 jo. Pasal 48 UU ITE. Perbuatan tersebut dikualifikasikan sebagai akses ilegal dan manipulasi data elektronik yang mengakibatkan kerugian bagi pemilik data maupun pihak penerbit kartu kredit..

2. Tanggung jawab hukum terhadap pelaku tindak pidana pencurian kartu kredit (*Carding*) dalam Putusan Nomor 845/Pid.Sus/2020/PT SBY telah memenuhi unsur pidana sebagaimana diatur dalam Pasal 30 jo. Pasal 46 dan Pasal 32 jo. Pasal 48 UU ITE, yang mengkualifikasikan perbuatan pelaku sebagai akses ilegal dan manipulasi data elektronik. Namun, sanksi yang dijatuhkan, yaitu delapan bulan penjara, menunjukkan bahwa penerapan hukum belum mencerminkan prinsip proporsionalitas dan keadilan, karena jauh di bawah ancaman pidana maksimal. Hal ini menegaskan bahwa penegakan hukum terhadap *Carding* masih lemah dalam memberikan efek jera serta belum sepenuhnya melindungi kepentingan korban maupun stabilitas sistem keuangan *digital*..

3. Penegakan hukum terhadap tindak pidana *Carding*masih menghadapi kendala normatif, teknis, dan struktural. Secara normatif, belum terdapat

pengaturan yang komprehensif mengenai jaringan kejahatan siber lintas negara dalam UU ITE. Secara teknis, pembuktian digital memerlukan keahlian forensik yang lebih kuat. Secara struktural, koordinasi antar lembaga penegak hukum belum optimal.

B. Saran

1. DPR RI seharusnya melakukan revisi UU ITE untuk memperjelas unsur tindak pidana *Carding*, menyesuaikan ancaman pidana agar proporsional, dan mengatur mekanisme penindakan yang dapat menjangkau jaringan kejahatan siber lintas negara.. Hal ini penting untuk mendorong pemidanaan yang lebih setara antara kejahatan digital dan pencurian konvensional.
2. Mahkamah Agung dan Kejaksaan Agung seharusnya menetapkan pedoman pemidanaan khusus bagi tindak pidana *Carding* sehingga hukuman yang dijatuhkan lebih seragam, konsisten, dan mampu menimbulkan efek jera bagi pelaku. Dengan pendekatan kumulatif ini, jaksa dan hakim dapat melihat kejahatan *Carding* tidak hanya sebagai pelanggaran terhadap sistem elektronik, tetapi juga sebagai bentuk nyata dari pengambilan kekayaan orang lain.
3. Perlu adanya penguatan kapasitas aparat penegak hukum, khususnya penyidik kepolisian dan jaksa, dalam bidang forensik digital, pelacakan jaringan siber, serta peningkatan kerja sama internasional. Hal ini penting mengingat tindak pidana Carding bersifat transnasional, melibatkan

banyak pihak, serta menggunakan teknologi yang kompleks, sehingga tanpa dukungan keahlian teknis dan kolaborasi lintas negara, proses pembuktian dan pengungkapan jaringan pelaku akan selalu menghadapi hambatan serius.

DAFTAR PUSTAKA

BUKU

Jonaedi Efendy, Johnny Ibrahim, (2018), Metode Penelitian Hukum, Depok: Prenamedia Group

Muhaimin, (2020), Metode penelitian Hukum, Mataram University Press,. Mataram

Solikin, Nur. (2019). *Masyarakat, dan Penegakan Hukum*. Pasuruan, Qiara Media

Yuhelson, (2018), *BUKU HUKUM PERBANKAN DI INDONESIA*, Gorontalo: IDEA Publishing

Candra, Marli, and others, (2017) *VICTIM PRECIPITATION DALAM TINDAK PIDANA PENCURIAN (SEBUAH PENDEKATAN VIKTIMOLOGI)*, Bekasi: Duta Media Publishing,

Hamid, Abd Haris, (2022) *Hukum Tindak Pidana Pencurian & Kekerasan*, Makassar: Chakti Pustaka Indonesia

Edrisy, Fikma, (2019) *Pengantar Hukum Siber*, Bandar Lampung: Sai Wawai Publishing,

Nurul Ichsan Hasan, (2014) *Pengantar Perbankan Syariah*, *Jakarta: Gaung Persada Press Group*

Krista Yitawati, Anik Tri Haryani, Sigit Sapto Nugroho, (2017), *Hukum Dam Teknologi*, Solo: Perum Gumpang Baru

Ichwan Kurnia, (2024) Hukum Pidana Siber, Jawa Tengah: CV. Eureka Media Aksara.

Husammudin MZ, (2024), Hukum Acara Pidana & Pidana Cyber, Medan: PT Media Penerbit Indonesia

Sahat Maruli Situmeang, (2020), Cyber Law, Bandung: Cakra

Maskun, (2013), Kejahatan Siber, Jakarta: Kencana

Simon Nahak, (2021), Hukum Siber Di Indonesia, Jakarta: Inteligensia Media.

Sosial, Mengenal Media, and Tak Menyesal, *Kementerian Pendidikan Dan*

Kebudayaan Badan Pengembangan Dan Pembinaan Bahasa Bacaan Untuk Anak Tingkat SD Kelas 4, 5, Dan 6

Yusrizal, (2018), Penegakan Hukum Tindak Pidana Cyber, Malang: Media Nusa Creative

JURNAL & KARYA ILMIAH

Asliani Harahap. 2024. "Legal Protection Against Rape Victims Based On Victimology". Jurnal kepangkatan dosen UMSU

Aditama, Prigel, Elisabeth Aprilia Sinaga, and Citra Anjelika Putri, 'Perbandingan Hukum Pidana Cyber Crime Dan Pengaruhnya Dalam Penegakan Hukum Antara Indonesia Dan Amerika Comparison of Cyber Crime Criminal Law and Its Impact on Law Enforcement Between Indonesia and America', *Jurnal Kompilasi Hukum*,

Aldo, Dasril, 'Pengaruh Cyber Attack Terhadap Kebijakan Cyber Security Amerika Serikat', *Journal of International Relations*, 4.3 (2018), pp. 393–401

Arifin, Ridwan, Hartini Atikasari, and Waspiah, 'The Intersection of Criminal Law, Technology and Business Commercial Law on *Carding*as Cyber Fraud', *Jurnal Hukum Novelty*.

Artika, R. Mas Repati, 'PENCURIAN ANTAR ORANG YANG PUNYA HUBUNGAN KELUARGA TERTENTU SEBAGAI DELIK ADUAN RELATIF MENURUT PASAL 367 AYAT (2) KUHP', *Lex Privatum*, 8.4 (2020), pp. 239–46)

Denata, Brigita Cynthia Liwandra, and Aju Putrijanti, 'Perlindungan Hukum Bagi Pemegang Kartu Kredit Atas Tagihan Yang Tidak Benar', *Notarius*.

Dewi Maesyaroh, 'Peran Digital Forensik Terhadap Pencurian Data Pribadi Sektor Perbankan Digital', *Datin Law Jurnal*, 2024.

Diansah, Hendri, and others, 'Kebijakan Hukum Pidana Terhadap Tindak Pidana Carding', 3.2 (2022), pp. 15–30

Diyu Sulaeman, and Anyelir Puspa Kemala, 'Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia', *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, 3.2 (2025).

Durham, Cole, ‘Amicus Curiae’, *Revista Latinoamericana de Derecho y Religión*, 1.NE (2022),.

Endang, Elisabeth, and others, ‘Globalisasi Dan Identitas : Mencari Keseimbangan Dalam Keragaman Budaya Indonesia’, 3.1 (2025), pp. 354–6

Faridi, Muhammad Khairul, ‘Kejahatan Siber Dalam Bidang Perbankan’, *Cyber Security Dan Forensik Digital*, 1.2 (2019), pp. 57–61.

Ginanjar Laksana, Tri, and Sri Mulyani, ‘Key Determinants Of Cybercrimes Targeting The Human Population’, *Maret*, 11.2 (2024), p. 2024.

Ginara, I Gede Krisna, I Made Minggu Widyantara, and Ni Komang Arini Styawati, ‘Kriminalisasi Terhadap Kejahatan *Carding*Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia’, *Jurnal Preferensi Hukum*, 3.1 (2022).

Habibi, Miftakhur Rokhman, and Isnatul Liviani, ‘Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia’, *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, 23.2 (2020).

Hapsari, Rian Dwi, and Kuncoro Galih Pambayun, ‘ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis’, *Jurnal Konstituen*, 5.1 (2023).

Hendri diansah, usman, yulia monita, ‘Dasar Pertimbangan Hakim Dalam Putusan Pengadilan Negeri Palembang Kepada Sanksi Tindak PidanaTerhadap Pelaku Penangkapan Ikan Menggunakan Bahan Peledak Dalam Putusan Nomor: 1/Pid.Sus-PRK/2018/PN.Plg’, *Jurnal of Cryminal Law*, 6.1 (2022).

Idris Balaka, Kemal, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany, ‘Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital’, *Yustitiabelen*, 10.2 (2024).

Izzati, Rania Nur, and Atika Puspita Marzaman, ‘Analisis Strategi Amerika Serikat Dan Tiongkok Dalam Menanggulangi Cyber Crime Pasca-Pandemi’, *Triwikrama: Jurnal Ilmu Sosial*, 9.2 (2025), pp. 1–14

Kaimuddin Haris, Oheo, Sabrina Hidayat, and Riski Dwitasari, ‘Kejahatan *Carding*Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia *Carding*Crime as a Form of Cyber Crime in Indonesian Criminal Law’, *Halu Oleo Legal Research* |, 5.2 (2023).

Kewarganegaraan, Jurnal, and others, ‘Cyber Crime Dalam Sudut Pandang Hukum Pidana’, 6.1 (2022), pp. 2169–75

Kurniawan, N A, 'Pencegahan Kejahatan *Carding*Sebagai Kejahatan Transnasional Menurut Hukum Internasional', *Jurnal Mahasiswa Fakultas Hukum Universitas Brawijaya*, 2014, pp. 1–14

Maghfirah, Nurul, and Abshoril Fithry, 'ANALISIS TINDAK PIDANA TERHADAP KERUSAKAN PROGRAM DAN DATA KOMPUTER (Studi Kasus Perlindungan Sistem Hukum Informatika)', *Prosiding SNAPP : Sosial Humaniora, Pertanian, Kesehatan Dan Teknologi*, 2.1 (2024).

Mahardika, Agung, 'PERTIMBANGAN HAKIM ATAS PENCURIAN DENGAN MODUS *CARDING*BERDASARKAN PASAL362 KUHP JO UNDANG-UNDANG NOMOR 19 TAHUN 2016 ATAS PERUBAHAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK STUDI KASUS PUTUSAN NOMOR.155/PID.SUS/2018/PN', *Tjyybjb.Ac.Cn*, 27.2 (2021), pp. 635–37

Muharam, Novi, and Azis Budianto, '*Carding*Crime Analysis as A Form of Cyber Crime in Indonesia's Criminal Law', 01.01 (2022).

Nur Luthiya, Adik, Benny Irawan, and Rena Yulia, 'Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi', *Jurnal Hukum Pidana Dan Kriminologi*, 2.2 (2021).

Pansariadi, Rafi Septia Budianto, and Noenik Soekorini, 'Tindak Pidana Cyber Crime Dan Penegakan Hukumnya', *Binamulia Hukum*, 12.2 (2023).

Pramuhadi, R Nurcahya, 'Gaya Hidup Penggunaan Kartu Kredit Masyarakat Urban Di Surabaya', *Jurnal Sosiologi Dialektika*, 15.2 (2020).

Pribadi, Deny Slamet, 'Aspek Hukum Penggunaan Kartu Kredit Sebagai Alat Jaminan', *Risalah Hukum*, 2005, pp. 8–10

Pribadi, Insan, 'Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana', *Jurnal Lex Renaissance*, 3.1 (2018).

Putusan, Direktori, Mahkamah Agung, and Republik Indonesia, 'Nomor 845/PID.SUS/2020/PT SBY DEMI KEADILAN BERDASARKAN KETUHANAN YANG MAHA ESA', 2020

Qammaddin, Qammaddin, Sulfikar Sallu, and Ahmad Fathoni, 'Implementasi Teknik Forensik Dalam Cybercrime (Carding)', *Remik*, 7.1 (2023).

Rifai, Hasan Hiawatha, and Asmak U I Hosnah, 'Tinjauan Yuridis Terhadap Tindak Pidana Pencurian Identitas Di Bawah Ketentuan KUHP', *Jurnal Pendidikan Tambusai*, 8.2 (2024).

Rofikah, 'Model Penanggulangan Carding', *Yustisia*, no. 90 (2014), pp. 82–88

Saputra, R. Prayuda, 'PERKEMBANGAN TINDAK PIDANA PENCURIAN DI INDONESIA', *Jurnal Pahlawan*, 2.2 (2019), pp. 45–52

Saragih, Deardo Pieter, and others, 'Transnational *Carding*Crime Analysis Is Reviewed From International Criminal Law', *Jurnal Hukum Dan HAM Wara Sains*, 1.02 (2022), pp. 108–20

Siregar, K. Manahan, 'PENGARUH UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (ITE) TERHADAP HUBUNGAN MASYARAKAT DENGAN PEMERINTAH DI KOTA PADANGSIDIMPUAN.', *Jah (Jurnal Analisis Hukum)*, 7.2 (2021), pp. 217–40

Suseno, Sigid, and n Syarif A. Barmawi, 'Kebijakan Pengaturan *Carding*Dalam Hukum Pidana Di Indonesia', *Jurnal Ilmu - Ilmu Sosial Dan Humaniora*, Vol. 6 (2004), pp. 254–55

Syalendro, Oky, Arief Fahmi Lubis, and R. Yusak Andri Ende Putra, 'Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Dan Penanganan Kasus Tindak Pidana Cyber Crime', *Aurelia: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia*, 4.1 (2025), pp. 335–47

Taroreh, Erwin, and others, 'Tinjauan Yuridis Terhadap Pelaku Peretasan Kartu Kredit *(Carding)* Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik', 2024, pp. 8878–83

Yanuar, Adams Pratama, 'Cyber War : Ancaman Baru Keamanan Nasional Dan Internasional', *Jurnal Keamanan Nasional*, 7.1 (2021).

Zuraida, Mehda, 'Credit Card Fraud (Carding) Dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia', *Jurnal Analisis Hubungan Internasional*, 4.1 (2024), pp. 1627–42

UNDANG-UNDANG

Undang-Undang Nomor 1 tahun 2024 tentang informasi dan transaksi elektronik

Agung, Mahkamah, *Putusan Nomor 845/PID.SUS/2020/PT SBY*, 2020

INTERNET

Rinanda, H. Meilisa, 'Pelaku Spamming Dan *Carding* Di Bekuk Bobol Kartu

Kredit Rp500 Juta', *Detiknews.Com*, 2018