



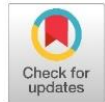
## Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit Dalam Tindak Pidana Di Bidang Perbankan

Galang Ramadhan Djokdja<sup>1</sup>, Sherly Adam<sup>2</sup>, Margie Gladies Sopacua<sup>3</sup>

<sup>1,2,3</sup> Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.

@ : galangrdj9@gmail.com

doi : xxxxxxxxxxxxxxxxx



### Info Artikel

#### Keywords:

Criminal Liability; Credit Card Burglary; Criminal Acts in the Banking Sector.

#### Kata Kunci:

Tanggung Jawab Pidana; Pembobolan Kartu Kredit; Tindak Pidana di Bidang Perbankan.

### Abstract

**Introduction:** There are many cases of fraud with credit cards at banks known as carding, but there is no new legal rule to ensnare the perpetrators so that the judges still use the old rules, namely the Criminal Code. Law enforcement in the banking sector includes regulatory issues in the field of information technology and other aspects are the ability of law enforcement officers, public legal awareness, and infrastructure that supports law enforcement, especially in reviewing criminal liability for perpetrators.

**Purposes of the Research:** Criminal liability for credit card burglary perpetrators in criminal acts in the banking sector.

**Methods of the Research:** The research method used is normative juridical with a problem approach in the form of a statutory approach, a conceptual analysis approach and a case approach. The legal materials used are primary and secondary legal materials. Data collection techniques are carried out through library research and processing techniques and analysis of legal materials through descriptions using qualitative methods.

**Results of the Research:** The results of the study indicate that the criminal law regulation of the crime of carding has been regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions and has been formulated in articles 362, 363 and 378 of the Criminal Code. namely about Theft and Fraud. Carding criminal liability can be carried out based on the ability of the perpetrator to be responsible; there is an error in the form of a deliberate act of the perpetrator as proven in accordance with the articles in paragraph; there is no excuse for his actions; and may be subject to sanctions for carding criminals.

### Abstrak

**Latar Belakang:** Marak terjadi kasus penipuan dengan kartu kredit dibank yang dikenal dengan istilah *carding* namun belum ada aturan hukum yang baru untuk menjerat pelaku sehingga para hakim masih memakai aturan yang lama yaitu KUHP. Penegakan hukum di bidang perbankan diantaranya masalah regulasi di bidang teknologi informasi dan aspek lainnya adalah kemampuan aparat penegak hukum, kesadaran hukum masyarakat, dan sarana prasarana yang mendukung penegakan hukumnya khususnya dalam mengkaji pertanggungjaban pidana pelaku.

**Tujuan Penelitian:** Pertanggungjawaban pidana pelaku pembobolan kartu kredit dalam tindak pidana di bidang perbankan.

**Metode Penelitian:** Metode penelitian yang digunakan adalah yuridis normative dengan pendekatan masalah berupa pendekatan perundang-undangan, pendekatan analisa konseptual dan pendekatan kasus. Bahan

hukum yang digunakan adalah bahan hukum primer dan sekunder. Teknik pengumpulan data dilakukan melalui studi kepustakaan dan teknik pengolahan dan analisa bahan hukum melalui cara deskripsi dengan menggunakan metode kualitatif.

**Hasil Penelitian:** Hasil penelitian menunjukkan bahwa pengaturan hukum pidana terhadap tindak pidana carding, telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta telah dirumuskan dalam pasal-pasal 362, 363 dan 378 KUHP yaitu tentang Pencurian dan Penipuan. Pertanggungjawaban pidana carding dapat dilakukan berdasarkan kemampuan bertanggung jawab pelaku; adanya kesalahan dalam bentuk kesengajaan pelaku yang dibuktikan sesuai pasal-pasal di atas; tidak ada alasan pemaaf atas perbuatannya; dan dapat dikenakan sanksi bagi pelaku tindak pidana carding.

## 1. Pendahuluan

Bank dan Lembaga Keuangan Non Bank merupakan bagian dari sistem keuangan dan sistem pembayaran suatu Negara<sup>1</sup>, bahkan pada era globalisasi sekarang ini, bank juga telah menjadi bagian dari sistem keuangan dan sistem pembayaran dunia.<sup>2</sup> Perbankan merupakan suatu lembaga badan hukum yang dibentuk dengan tujuan untuk membantu pemerataan pembangunan nasional. Hal tersebut didasarkan pada Pasal 4 Undang-Undang Nomor 7 Tahun 1992 jo Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, mengatur bahwa perbankan di Indonesia bertujuan menunjang pelaksanaan pembangunan nasional dalam rangka meningkatkan pemerataan pertumbuhan ekonomi dan stabilitas nasional ke arah peningkatan kesejahteraan rakyat banyak. Seiring dengan peran perbankan yang sangat strategis dalam menunjang perekonomian masyarakat, bidang perbankan pun tidak dapat dilepaskan dari tindak pidana yang juga banyak merugikan kepercayaan masyarakat.

Secara umum tindak pidana di bidang perbankan adalah suatu perbuatan yang melanggar ketentuan yang diatur dalam undang-undang perbankan maupun yang terdapat dalam ketentuan pidana sedangkan istilah kejahatan di bidang perbankan merupakan perbuatan yang dilakukan terkait industri perbankan yang menyalahi aturan hukum yang bisa melibatkan pihak perbankan maupun nasabahnya baik sebagai pelaku maupun korban. Padahal pengaturan terkait tindak pidana di bidang perbankan seperti pencurian uang, pemalsuan dokumen nasabah, pemusnahan pelaporan dan sebagainya memang didalamnya telah jelas diterangkan dalam Undang-Undang Nomor 10 Tahun 1998 tentang perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan yang (selanjutnya disebut UU Perbankan). Pada Pasal 47 hingga Pasal 59A menyebutkan mengenai sanksi pelaku tindak pidana perbankan.

---

<sup>1</sup> Muchtar Anshary Hamid Labetubun et al., "Sistem Keuangan Dan Lembaga Keuangan Di Indonesia," in *Lembaga Keuangan Bank Dan Non Bank (Sebuah Tinjauan Teori Dan Praktis)* (Bandung: Widina Bhakti Persada, 2021), h. 3.

<sup>2</sup> Muchtar Anshary Hamid Labetubun et al., "Fungsi Dan Peranan Bank Indonesia Dan Bank Umum," in *Manajemen Perbankan (Sebuah Tinjauan Teori Dan Praktis)* (Bandung: Widina Bhakti Persada, 2021).

Pengaturan tindak pidana Carding dalam hukum pidana di Indonesia diatur dalam Pasal 263, Pasal 363 dan 378 KUHP dan Undang-Undang Diluar KUHP yaitu Undang-Undang Nomor 19 tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 28 tahun 2011 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) pada Pasal 30 dengan ancaman sanksinya diatur dalam Pasal 46, Pasal 32 dengan ancaman sanksinya diatur dalam Pasal 48, Pasal 34 dengan ancaman sanksinya diatur dalam Pasal 50 dan Pasal 35 dengan ancaman sanksinya diatur dalam Pasal 51 ayat (1). Namun sepanjang ini permasalahan *carding* di Indonesia baru dapat diatasi dengan regulasi lama ialah Pasal 362 KUHP serta Pasal 31 ayat (1) dan ayat (2) UU ITE.

Fenomena *cyber crime* di Indonesia merupakan perbincangan yang selalu menarik minat masyarakat, dari masyarakat pada umumnya dan masyarakat yang memiliki keterkaitan langsung dengan fenomena *cyber crime* yakni aparat penegak hukum, dan akademisi hukum, dalam dunia akademisi hukum, perbincangan bertambah menarik terkait dengan upaya pemerintah untuk menyusun peraturan perundang-undangan tentang *cyber crime*.<sup>3</sup> Kejahatan *cyber crime* yang dilakukan adalah tindak pidana *carding*. Tindak pidana *carding* adalah penipuan dengan menggunakan data kartu kredit. Tindak pidana *carding* yang dilakukan oleh para pelaku atau disebut *carder* dapat dikategorikan dalam 2 (dua) bentuk yaitu transaksi konvensional atau *off line* dan transaksi maya atau *on line*.<sup>4</sup>

Tindak pidana *carding* ini telah berkembang pesat di Indonesia, sementara itu sistem hukum di Indonesia masih memberikan celah dan lemahnya sistem pengawasan atas kejahatan ini. Perundang-undangan yang mengatur tentang *cyber crime* Indonesia termasuk negara yang tertinggal dalam pengembangan dan pemanfaatan teknologi informasi dalam merumuskan suatu terutama pengaturan tindak pidana *carding* dimana penegakan hukumnya masih sangat memprihatinkan.

## 2. Metode Penelitian

Penelitian yang digunakan ini merupakan penelitian hukum normatif. Penelitian hukum normatif adalah penelitian hukum yang meletakkan hukum sebagai sebuah bangunan sistem norma. Sistem norma yang dimaksud adalah mengenai asas-asas, norma, kaidah dari peraturan perundang-undangan, putusan pengadilan, perjanjian serta doktrin (ajaran). Peter Mahmud Marzuki menjelaskan bahwa penelitian hukum normatif adalah suatu proses untuk menemukan aturan hukum prinsip-prinsip hukum, guna menjawab permasalahan hukum, penelitian hukum normatif dilakukan untuk menghasilkan argumentasi, teori dan konsep baru sebagai preskripsi (penilaian) dalam masalah yang dihadapi.<sup>5</sup> Adapun sifat penelitian adalah deskriptif analisis, artinya dengan data yang ada diteliti dan dianalisis untuk dapat dipertegas pendirian dan digunakan pandangan para ahli serta pemikir-pemikir yuridis guna memperkuat teori sekaligus dapat ditarik beberapa kesimpulan dari permasalahan yang dikemukakan

---

<sup>3</sup> Sutarman, *Cyber Crime-Modus Operandi Dan Penanggulangannya* (Yogyakarta: LaksBang Pressindo, 2007), h. 5.

<sup>4</sup> F N Jovan, *Pembobol Kartu Kredit- Menyingkap Teknik Dan Cara Kerja Para Carder Di Internet* (Jakarta: Mediakita, 2006), h. 12.

<sup>5</sup> Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana, 2016), h. 141.

### 3. Hasil Dan Pembahasan

#### 3.1 Pengaturan Hukum Pidana Terhadap Pembobolan Kartu Kredit Dalam Tindak Pidana Di Bidang Perbankan

Tindak Istilah tindak pidana berasal dari istilah yang dikenal dalam hukum pidana Belanda yaitu *strafbaar feit*. Istilah ini terdapat dalam *Wetboek van Strafrecht* Negeri Belanda dan juga dalam *Wetboek van Strafrecht voor nederlandsch indie* (KUHP), tetapi tidak ada penjelasan resmi tentang apa yang dimaksud dengan *strafbaar feit*.<sup>6</sup>

Tindak pidana mempunyai pengertian yang abstrak dari peristiwa-peristiwa yang konkrit dalam lapangan hukum pidana, sehingga tindak pidana haruslah diberikan arti yang bersifat ilmiah dan ditentukan dengan jelas untuk dapat memisahkan dengan istilah yang dipakai sehari-hari dalam kehidupan masyarakat.<sup>7</sup>

Undang-Undang Perbankan membedakan sanksi pidana menjadi 2 (dua) bentuk, yaitu kejahatan dan pelanggaran. Pada Pasal 46, 47, 47A, 48 ayat (1), 49, 50, dan Pasal 50A merupakan tindak pidana yang tergolong bentuk kejahatan oleh karena itu sanksi yang diberikan lebih berat. Sedangkan tindak pidana perbankan yang termasuk dalam katagori pelanggaran terdapat pada Pasal 48 Ayat (2).

Terhadap tindak pidana Perbankan yang dilakukan oleh orang dalam terdapat beberapa undang-undang yang dapat dan biasanya diterapkan yaitu:

- 1) Kitab Undang-Undang hukum Pidana, Ketentuan KUHP yang biasa dipakai misalnya Pasal 263 (pemalsuan), Pasal 372 (penggelap dalam jabatan), 378 (penipuan). 362 (pencurian) Dll. Pasal-pasal KUHP diterapkan biasanya apabila bank menjadi korban dari suatu tindak pidana.
- 2) Undang-Undang Pemberantasan Tindak Pidana Korupsi. Diterapkan terhadap kasus-kasus yang menimpa bank pemerintah, Undang-Undang ini untuk mempermudah menjerat para pelaku, mengenakan hukuman yang berat dan memperoleh uang pengganti atas kerugian Negara.

Berkenaan dengan pasal pasal mengenai tindak pidana perbankan, perubahan yang cukup signifikan yang terdapat dalam Undang-Undang Nomor 10 1998 tentang perubahan Undang-Undang Nomor 7 Tahun 1992 tentang perbankan adalah mengenai pengenaan sanksi yang jauh lebih berat dan ditetapkan minimum dan maksimum dalam hal terjadi tindak pidana di bidang perbankan.

Tidak semua pasal dari undang-undang perbankan dapat menjerat pelaku tindak pidana sebagai mana diatur Pasal 49 dan 50 Undang-Undang Nomor 10 tahun 1998, maka sepanjang tidak diatur oleh Undang-Undang ini dapat diterapkan KUHP. Seperti tindak pidana yang berkaitan dengan tindakan pemalsuan dokumen atau warkat, maka dapat diberlakukan ketentuan Pasal 263 atau Pasal 264 KUHP yang mengatur pemalsuan surat.

---

<sup>6</sup> Adami Chazawi, *Pelajaran Hukum Pidana (Stelsel Tindak Pidana, Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana)* (Jakarta: Raja Grafindo Persada, 2002), h. 67.

<sup>7</sup> Kartonegoro, *Diktat Kuliah Hukum Pidana* (Jakarta: Balai Lektor Mahasiswa, 1987), h. 62.

Atau penggelapan dapat dikenakan Pasal 372 KUHP yang mengatur tentang penggelapan, 378 (penipuan). 362 (pencurian).

Tindak pidana di bidang perbankan merupakan salah satu bentuk dari tindak pidana di bidang ekonomi. Tindak pidana di bidang ekonomi ini biasanya disebut juga kejahatan kerah putih (*white collar crime*). Seperti yang telah kita ketahui sebelumnya, tindak pidana ekonomi merupakan suatu tindak pidana yang mempunyai motif ekonomi yang dilakukan oleh orang-orang tertentu dan dapat merugikan masyarakat dan/atau negara.

Tindak pidana di bidang perbankan adalah segala jenis perbuatan melanggar hukum yang berhubungan dengan kegiatan dalam menjalankan usaha bank, baik bank sebagai sasaran maupun sebagai sarana.<sup>8</sup> Juga diartikan sebagai tindak pidana yang tidak hanya mencakup pelanggaran terhadap Undang-Undang Perbankan saja, melainkan mencakup pula tindak pidana lain sepanjang berkaitan dengan lembaga perbankan.<sup>9</sup>

Dimensi bentuk tindak pidana di bidang perbankan dapat berupa tindak pidana seseorang terhadap bank, tindak pidana bank terhadap bank lain, ataupun tindak pidana bank terhadap perorangan, sehingga bank dapat menjadi korban ataupun pelaku. Sedangkan dimensi ruang tindak pidana di bidang perbankan tidak terbatas pada suatu tempat tertentu, namun dapat melewati batas-batas teritorial suatu negara. Dengan demikian pula dimensi waktu tindak pidana di bidang perbankan dapat terjadi seketika, namun dapat pula berlangsung lama. Sementara itu, ruang lingkup terjadinya tindak pidana di bidang perbankan dapat terjadi pada keseluruhan lingkup kehidupan dunia perbankan atau yang sangat berkaitan dengan kegiatan perbankan dan mencakup dengan lembaga keuangan lainnya.<sup>10</sup>

Bentuk-bentuk Cyber crime pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum yaitu:

- 1) Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
  - a) *Illegal access* (akses secara tidak sah terhadap sistem komputer).
  - b) *Data interference* (mengganggu data komputer).
  - c) *System interference* (mengganggu sistem komputer).
  - d) *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer).
  - e) *Data Theft* (mencuri data).
  - f) *Data leakage and espionage* (membocorkan data dan memata-matai).
  - g) *Miss use of devices* (menyalahgunakan peralatan komputer).
- 2) Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan.
  - a) *Credit card fraud* (penipuan kartu kredit).
  - b) *Bank fraud* (penipuan terhadap bank).

---

<sup>8</sup> BPHN and Departemen Kehakiman, "Laporan Akhir Penelitian Masalah-Masalah Hukum Kejahatan Perbankan" (Jakarta, 1992), h. 18.

<sup>9</sup> *Ibid*, h. 12-13

<sup>10</sup> Ronald Pentury, "Tinjauan Kriminologi Terhadap Kejahatan Perbankan" (Universitas Pattimura, 2013), h. 35.



- c) *Service Offered fraud* (penipuan melalui penawaran suatu jasa).
  - d) *Identity Theft and Fraud* (pencurian identitas dan penipuan).
  - e) *Computer-related fraud* (penipuan melalui komputer).
  - f) *Computer-related forgery* (pemalsuan melalui komputer).
  - g) *Computer-related betting* (perjudian melalui komputer).
  - h) *Computer-related Extortion and Threats* (pemerasan dan pengancaman melalui komputer).
- 3) Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem computer.
- a) *Child pornography* (pornografi anak).
  - b) *Infringements Of Copyright and Related Rights* (pelanggaran terhadap hak cipta dan hak-hak terkait).
  - c) *Drug Traffickers* (peredaran narkoba).

*Carding* atau disebut *Card Not Present Transaction* adalah bentuk kejahatan menggunakan nomor kartu kredit orang lain untuk dibelanjakan (*non face to face transaction*) tanpa sepengetahuan pemiliknya yang sah. Transaksi lazimnya dilakukan secara elektronik. *Carding* sendiri merupakan tindak pidana yang bersifat *illegal interception* atau menyadap data nasabah atau pemilik kartu kredit secara fisik artinya untuk belanja di toko *online* (*forgery*).<sup>11</sup> *Carding* merupakan suatu tindak pidana yang berhubungan dengan kartu kredit dan metode kejahatan ini menggunakan jaringan komputer atau internet untuk mendapatkan data dari pemilik kartu kredit tanpa sepengetahuan pemilik kartu kredit tersebut.<sup>12</sup> Sebagai akibat dari perkembangan teknologi informatika berbasis internet, dengan sendirinya teknologi informatika juga telah mengubah perilaku masyarakat dan peradaban manusia secara global. Teknologi informatika menyebabkan perubahan sosial secara signifikan yang berlangsung dengan cepat.<sup>13</sup>

Teknologi informatika saat ini telah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum, dengan kata lain terjadinya perbuatan-perbuatan melawan hukum tersebut maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut. Dampak negatif selain kemudahan dan kenyamanan layanan internet itu, ada ancaman yang sangat merisaukan, yakni sisi keamanannya. Pengamanan sistem informasi berbasis internet perlu diperhatikan, karena jaringan informasi yang bersifat publik dan global sangat rentan dari berbagai bentuk kejahatan. Ancaman timbul manakala seseorang mempunyai keinginan memperoleh akses ilegal ke dalam jaringan komputer, sehingga lahirnya perilaku-perilaku

<sup>11</sup> Kristoforus Laga Kleden, "Pisau Analisis Kriminologi Prostitusi Online," *DiH: Jurnal Ilmu Hukum* 15, no. 1 (2019): 68-78, <https://doi.org/10.30996/dih.v15i1>.

<sup>12</sup> Tomy Michael, "The HE Inhited Conditions In The Draft Regulation of Surabaya Mayor About The Procedur of Choosing The Management of Community Empowerment of Village Institusion, Citizen Association And Neighborhood Association," *Jurnal Hukum Magnum Opus* 2, no. 2 (2019): 174-84.

<sup>13</sup> Tony Yuri Rahmanto, "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik," *Jurnal Penelitian Hukum De Jure* 19, no. 1 (2019): 31-52, <https://doi.org/10.30641/dejure.2019.V19.31-52>.

me nyimpang dengan memanfaatkan teknologi canggih sebagai alat untuk mencapai tujuan dengan melakukan kejahatan. Kejahatan-kejahatan ini dikenal sebagai kejahatan dunia maya atau *cyber crime*.<sup>14</sup>

*Cyber crime* yang menggunakan media komunikasi dan komputer, kendati berada di dunia lain dalam bentuk maya tetapi memiliki dampak yang sangat nyata. Penyimpangan dan kerugian besar telah terjadi dan dirasakan oleh masyarakat di berbagai penjuru dunia. Kerugian berdampak luas kepada sektor-sektor lain di bidang ekonomi, perbankan, moneter dan sektor lain yang menggunakan jaringan komputer. Fenomena *cyber crime* di Indonesia merupakan perbincangan yang selalu menarik minat masyarakat.

Berbicara tindak pidana *carding* tidak terlepas dari 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 *cyber (cyber crime)* dengan tindak kejahatan komputer, dan ada ahli yang membedakan diantara keduanya.

Meskipun belum ada kesepakatan mengenai definisi kejahatan teknologi informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer. Secara umum yang dimaksud dengan kejahatan komputer atau kejahatan di dunia *cyber (cyber crime)* adalah “upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut”. Tindak pidana *carding* sendiri merupakan salah satu bentuk dari kejahatan *cyber crime* yang terjadi saat ini, akibat dari kemajuan teknologi informasi.<sup>15</sup>

Perkembangan teknologi dengan berbagai bentuk kecanggihan informasi, komunikasi dan transportasi membuat modus kejahatan semakin marak dilakukan oleh pelaku-pelaku kejahatan, diantaranya kejahatan yang menggunakan komputer dan internet sebagai alat bantu untuk melakukan kejahatan di bidang kartu kredit atau yang dikenal dengan tindak pidana *carding*. Kartu kredit merupakan salah satu kartu yang diterbitkan oleh bank atau dikenal sebagai bank card. Bank card merupakan “uang plastik” yang dikeluarkan oleh bank.<sup>16</sup>

Kebijakan pengaturan tindak pidana *carding* terdapat di dalam UU ITE yaitu yang berkaitan dengan perbuatan menggunakan dan atau mengakses kartu kredit orang lain secara tanpa hak. Ketentuan Pasal 51 UU ITE hanya dapat menjangkau pelanggaran pada tahapan *card embossing and delivery (courier/recipient or customer) dan usage*. Tidak semua modus operandi dalam tahapan tersebut dapat terjangkau, karena ketentuan Pasal 51 jo Pasal 34 UU ITE hanya mengatur perbuatan yang dilakukan oleh orang yang menggunakan

---

<sup>14</sup> Rezy Januar Wilyana, Imam Budi Santoso, and Oci Senjaya, “Pembuktian Bukti Elektronik Di Persidangan,” *Singaperbangsa Law Review* 1, no. 1 (2020): 164–83.

<sup>15</sup> Adam Bastian Mardhatillah and Ahmad Mahyani, “Bukti Tidak Langsung Sebagai Dasar Hakim Menjatuhkan Pidana (Putusan Nomor: 777/ Pid.B/ 2016/ PN.JKT.PST),” *Mimbar Keadilan* 12, no. 1 (2019): 59–66, <https://doi.org/10.30996/mk.v12i1.2167>.

<sup>16</sup> D. Gumilang, Otto Yudianto, and Erny Herlin Setyorini, “Legalitas Surat Kuasa Yang Diterbitkan Seorang Buron,” *Jurnal Hukum Magnum Opus* 2, no. 2 (2019): 125–36, <https://doi.org/10.30996/jhmo.v2i2.2497>.

kartu kredit tetapi tidak termasuk pedagang atau pengelola yang juga dapat menjadi pelaku tindak pidana *carding*.

Fitur hukum positif paling utama KUHP telah dimiliki Indonesia, tetapi peraturan itu masih belum lumayan sanggup menjerat pelaku tindak pidana di Internet. Pasal 1 KUHP disebutkan “tidak terdapat perbuatan pidana bila tadinya tidak dinyatakan dalam sesuatu syarat undang undang (*nullum delictum noela poena siena praveia legi poenali*)”. Maksudnya, pasal itu menegaskan jika pelaku kejahatan cyber crime paling utama tindak pidana *carding* belum pasti bisa dikenakan sanksi pidana. Tidak hanya berbenturan dengan Pasal 1 KUHP, kesusahan bisa mempertanggungjawabkan pelaku tindak pidana *carding* yang dicoba baik secara *offline* ataupun *online* berkaitan dengan permasalahan pembuktian. Hukum positif mewajibkan terdapatnya perlengkapan fakta, saksi, petunjuk, penjelasan pakar dan tersangka dalam pembuktian. Sebaliknya dalam perihal kejahatan terpaut dengan teknologi data susah dicoba pembuktiannya.<sup>17</sup>

Pengaturan hukum pidana terhadap tindak pidana pembobolan kartu kredit atau kejahatan *carding* diatur dalam Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, pengaturan hukum selain dalam Undang-Undang Informasi dan Transaksi Elektronik kejahatan *carding* dapat dirumuskan dalam KUHP dengan menggunakan metode interpretasi ekstensif terhadap pasal-pasal yang terdapat dalam KUHP yaitu Pasal 362, 363 dan 378 KUHP yaitu tentang pencurian dan penipuan. Menurut modus operandinya diatur dalam undang-undang khusus diluar KUHP yaitu Undang-Undang nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai *lex specialis* diantaranya diatur pada Pasal 30 jo Pasal 46 sebagai pasal tentang pencurian, Pasal 34 ayat (1) jo Pasal 50 sebagai pasal tentang pencurian dilakukan dengan kerjasama oleh dua orang atau lebih, Pada Pasal 35 jo Pasal 51 ayat (1) atau Pasal 32 jo Pasal 48 sebagai pasal tentang penipuan. Peran pemerintah dalam melakukan pengaturan secara jelas dan detail terhadap tindak pidana pembobolan kartu kredit atau *Carding* yang dapat diterapkan bagi pelaku tindak pidana pembobolan kartu kredit atau *Carding*.

### **3.2 Pertanggungjawaban Pidana Pelaku Pembobolan Kartu Kredit Dalam Tindak Pidana Di Bidang Perbankan**

Undang-Undang Nomor 7 Tahun 1992 *jo* Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, dapat ditemukan beberapa aspek tindak pidana perbankan, antara lain dikemukakan di bawah ini berupa:<sup>18</sup>

- a) Menghimpun dana tanpa izin usaha perbankan,
- b) Kejahatan tentang rahasia perbankan,
- c) Kejahatan menyangkut catatan pembukuan dan laporan bank,
- d) Kejahatan penyalahgunaan kewenangan jabatan,

---

<sup>17</sup> Gert Jan van Hardeveld, Craig Webber, and Kieron O'Hara, “Discovering Credit Card Fraud Methods in Online Tutorials,” in *Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention*, vol. 1, 2016, 1-5, <https://doi.org/10.1145/2915368.2915369>.

<sup>18</sup> Kasmir, *Bank Dan Lembaga Keuangan Lainnya* (Jakarta: Raja Grafindo Persada, 2014), 117.



- e) Tindak pidana tidak melaksanakan langkah-langkah untuk pematuhan peraturan bank.
- f) Penyalahgunaan kartu kredit,
- g) Tindak pidana oleh pihak terafiliasi.

*Cyber crime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. *Cyber crime* memiliki beberapa karakteristik yaitu perbuatan yang dilakukan secara ilegal, perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet, perbuatan tersebut mengakibatkan kerugian materiil atau immateriil dan pelaku adalah orang yang menguasai penggunaan internet beserta aplikasinya, di mana perbuatan tersebut sering dilakukan secara transnasional.<sup>19</sup>

*Cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Pada *cyber crime* terdapat dua tipe kejahatan di mana tipe yang pertama adalah kejahatan di mana komputer menjadi target aktivitas kriminal, sedangkan tipe yang kedua adalah kejahatan yang menggunakan komputer sebagai alatnya.<sup>20</sup>

Fenomena *cyber crime* di bidang perbankan memiliki karakteristik tersendiri dibandingkan dengan kejahatan konvensional lainnya di mana siapa pun bisa menjadi korban dari kejahatan ini. Pelaku tidak menetapkan target korban, sehingga kejahatan ini perlu di waspadai oleh setiap pengguna jasa layanan internet, hal ini disebabkan sifat internet global yang memungkinkan *cyber crime* dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan, sementara sistem informasi perbankan mutlak memerlukan layanan internet.

Beberapa bentuk perkembangan *cyber crime* dalam kegiatan perbankan antara lain:

- a) *Typo site*, yaitu membuat nama domain dan alamat situs yang mirip dengan situs resmi di mana pelaku memanfaatkan kekeliruan dari pengguna internet dalam pengetikan alamat situs yang dicari.<sup>21</sup>
- b) *Keylogger keystroke recorder* di mana kegiatan ini dilakukan dengan menggunakan *software* atau program *keylogger* dan cara kerja dari *keylogger* ini adalah dengan mencatat segala aktivitas yang dilakukan oleh pengguna internet melalui huruf-huruf yang diketikkan pada *keyboard* di mana dalam berselancar di dunia maya, pengguna internet mungkin saja memasukkan nomor identitas dan *password* yang dapat dimanfaatkan oleh pelaku. Kejahatan ini biasanya terjadi pada tempat umum yang digunakan untuk mengakses internet seperti warung internet, restoran, bandara dan tempat umum lainnya yang menyediakan komputer yang di dukung dengan fasilitas internet.

---

<sup>19</sup> Budi Suhariyanto, *Tindak Pidana Teknologi Informasi* (Jakarta: Rajawali Pers, 2012), h. 13.

<sup>20</sup> Abdul Wahid and Mohammad Labib, *Kejahatan Mayantara* (Bandung: Refika Aditama, 2005), h. 40.

<sup>21</sup> Muhammad Khairul Faridi, "Kejahatan Siber Dalam Bidang Perbankan," *Cyber Security Dan Forensik Digital* 1, no. 2 (2018): 57-61.

- c) *Sniffing* adalah cara yang digunakan oleh pelaku dengan mengamati paket data internet yang digunakan oleh pengguna untuk mendapatkan nomor identitas dan *password* yang bersangkutan.<sup>22</sup>
- d) *Brute force attacking* yaitu upaya pencurian nomor identitas dan *password* melalui mencoba kemungkinan atas kombinasi yang dibuat.
- e) *Web deface system exploitation*, yaitu eksploitasi sistem dengan mengganti tampilan awal dari sebuah situs resmi.
- f) *Email spamming*, yakni dengan mengirimkan email kepada pemilik akun dengan menawarkan produk-produk atau menyatakan bahwa pemilik akun telah memenangkan suatu undian.
- g) *Denial of service*, yaitu pelumpuhan sistem elektronik dengan membanjiri akun atau sistem elektronik dengan data dalam jumlah yang besar.
- h) *Virus, worm, trojan* yaitu penyebaran virus komputer dilakukan untuk menyerang sistem komputer, memperoleh data, memanipulasi data atau tindakan lain yang dilakukan secara melawan hukum.
- i) *Malware* merupakan singkatan dari *malicious software* yang artinya *software* yang tidak diinginkan dalam sistem komputer, biasanya malware dibuat untuk mencuri data informasi yang bahkan dapat merusak sebuah sistem komputer.
- j) *Carding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain yang diperoleh secara ilegal, biasanya dengan mencuri data di internet, dimana sebutan pelakunya adalah *carder* dan sebutan lain untuk kejahatan jenis ini adalah *cyberfroud* alias penipuan di dunia maya.
- k) *Skimming* merupakan metode yang digunakan untuk mencuri informasi nasabah pada saat bertransaksi menggunakan anjungan tunai mandiri.<sup>23</sup>

Ekses negatif yang diahirkan dari perkembangan bentuk-bentuk *cybercrime* ialah berkembangnya modus operandi dari kejahatan tradisional yang mempergunakan ruang virtual dalam melakukan kejahatan. Dalam fokus *cybercrime* pada penelitian ini terletak pada bentuk kejahatan tradisional yang memasuki ruang virtual dengan bantuan peralatan komputer dan teknologi internet. Contoh *cybercrime* dalam transaksi perbankan yang menggunakan sarana Internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan *online* (*online banking*).

Adapun cara Kerja Modus Pencurian Data Kartu kredit / credit card sebagai berikut:<sup>24</sup>

- 1) Membeli data nasabah dari oknum Bank.
- 2) Kemudian si pelaku menelpon satu persatu nasabah kartu kredit dengan mengatas namakan pihak bank dengan alasan penawaran upgrade paket.
- 3) Kemudian apabila si korban sudah setuju maka mereka akan mendatangkan kurir ke pihak korban.
- 4) Kemudian setelah kurir datang mereka akan meminta data lengkap, seperti KTP, dan kartu kredit yang nantinya akan di scan atau bahasa umumnya di foto copy secara bolak balik ktp dan kartu kredit.

---

<sup>22</sup> *Ibid*, h. 59.

<sup>23</sup> *Ibid*, h. 59.

<sup>24</sup> Toto Haryanto, "Modus Baru Pencurian Kartu Kredit Terungkap," *Totoharyato.Com* (Jakarta, 2015).

- 5) Kemudian setelah selesai si pelaku akan membuat duplikat kartu kredit anda dan mereka akan datang kembali kepada anda dan memberikan kartu kredit yang baru dengan datang ke tempat anda tinggal, dan si pelaku akan datang dan mengunting kartu kredit anda agar anda terlihat lebih percaya.
- 6) Apa yang mereka gunting itu adalah kartu kredit yang palsu dan yang asli sudah mereka kantong.

Defenisi *fraud* dalam kartu kredit, adalah *Fraud* berarti tindakan melanggar hukum yang dilakukan seseorang atau sekelompok orang untuk mendapatkan keuntungan finansial dari penggunaan kartu kredit yang bukan menjadi hak miliknya, dan salah satu tindakan kejahatan yang umum dilakukan adalah pencurian data kartu kredit, atau yang biasa disebut dengan istilah *phishing*. Orang atau komplotan yang melakukan *phishing* biasanya mengincar 4 digit nomor di belakang kartu kredit, dan nomor PIN-nya. Informasi ini kemudian digunakan oleh pelaku untuk bertransaksi atas nama nasabah, terdapat empat teknik yang umum atau sering dilakukan pelaku pencurian data kartu kredit, yaitu sebagai berikut:

- 1) Menelpon untuk memperbaharui data diri kartu kredit  
Pelaku akan menelpon dan mengaku sebagai perwakilan dari pihak Bank atau surveyor yang ingin memperbaharui data kartu kredit. Modus ini juga bisa dilakukan via E-Mail, dimana pelaku menanyakan hal yang sama seperti diatas.
- 2) Transaksi di toko online palsu  
Modus lain yang sering digunakan adalah membuat situs belanja online palsu. Karena apabila melakukan pembayaran kartu kredit pada situs online yang tidak terpercaya, kemungkinan tujuan mereka adalah mencuri data kartu kredit.
- 3) *Skimming*  
Teknik *skimming* dilakukan dengan menggunakan alat penyalin informasi. Umumnya, alat ini ditempelkan pada mesin ATM Bank. Namun juga dapat dilakukan pada mesin EDC kartu kredit dengan metode yang sama.
- 4) Menggunakan koneksi *Wi-Fi* palsu  
Pelaku menggunakan sebuah alat seperti reuter internet, yang dapat menciptakan koneksi internet *Wi-Fi* palsu di gadget calon korban. Ketika calon korban telah terkoneksi dengan koneksi ini, si pelaku dapat dengan mudah melihat informasi yang tersimpan dalam *browsing history* korban. Salah satu informasi yang biasanya dicari pelaku adalah informasi transaksi kartu kredit.

Modus ini dapat terjadi akibat lemahnya sistem otentikasi yang digunakan dalam memastikan identitas pemesanan barang di toko *online*. Mengingat tindak pidana *carding* ini menggunakan sarana komputer dan atau jaringan komputer maka dapat menjadi salah satu jenis kejahatan yang dapat dimasukkan dalam legislasi kejahatan dunia maya (*cyber crime law*).

Adanya jenis kejahatan baru memaksa pemerintah membentuk regulasi baru guna menangani kejahatan yang terjadi. UU ITE merupakan undang-undang pertama yang dirumuskan oleh pemerintah Indonesia dalam menghadapi kejahatan-kejahatan yang dilakukan dengan menggunakan teknologi, dalam artian undang-undang tersebut merupakan tumpuhan utama dalam menegakkan hukum atas hal-hal yang berkaitan

dengan *cyber rcrime*. Namun dengan adanya undang-undang ini tidak sepenuhnya menghentikan kejahatan *carding*, sebab terlalu banyak celah yang dimanfaatkan *carder* untuk melakukan aksinya.<sup>25</sup>

Terjadinya kasus kejahatan *carding* memiliki cara dengan berbagai modus. Mengenai penanganannya terhadap kasus tersebut masih terdapat banyak hambatan, salah satunya mengenai rendahnya kesadaran nasabah akan pentingnya data pribadi seperti identitas, nomor pin, kode OTP. Disinilah letak permasalahan yang semakin hari semakin banyak terjadi, sehingga hal tersebut membahayakan pihak nasabah dan juga pihak perbankan.

Menangani kasus *carding* diterapkan Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi. Kemudian setelah lahirnya UU No. 8 Tahun 2011, khusus kasus *carding* dapat dijerat dengan menggunakan Pasal 31 ayat (1) dan (2) UU No. 11 tahun 2008 yang membahas tentang hacking. Karena dalam salah satu langkah untuk mendapatkan nomor kartu kredit *carder* sering melakukan hacking ke situs-situs resmi lembaga penyedia kartu kredit untuk menembus sistem pengamannya.

Sepanjang ini permasalahan *carding* di Indonesia baru dapat diatasi dengan regulasi lama ialah Pasal 362 KUHP serta Pasal 31 ayat (1) dan ayat (2) UU ITE. Penanggulangan permasalahan *carding* membutuhkan regulasi yang spesial mengendalikan tentang kejahatan *carding* supaya kasus-kasus semacam ini dapat menurun serta apalagi tidak terdapat lagi. Namun tidak hanya regulasi spesial pula wajib didukung dengan pengamanan sistem baik aplikasi ataupun hardware, guidelines buat pembuat kebijakan yang berhubungan dengan *computer-related crime* serta dukungan dari lembaga khusus.<sup>26</sup>

Tindak pidana *carding* tidak terlepas dari pertanggungjawaban pelaku dan penerapan sanksinya terhadap pertanggungjawaban pidana tindak pidana *carding* menggunakan teori Moeljatno dimana kesalahan tersebut terdiri dari kesengajaan (*dolus*) dimana kesengajaan atau *dolus* ditentukan dalam 3 (tiga) bentuk yaitu kesengajaan dengan maksud (*dolus directus*), kesengajaan dengan kepastian (*opzet bijt zekerheids bewotzjin*) dan kesengajaan dengan kemungkinan (*dolus eventualis*) sedangkan kealpaan (*culpa*), terdiri dari kealpaan dengan kesadaran (*bewuste schuld*) dan kealpaan tanpa kesadaran (*onbewuste schuld*). Adalah kealpaan yang tidak dikehendaki. Artinya sanksi terhadap pelanggaran norma pidana yang dilakukan lebih ringan pidananya, dikarenakan kealpaan atau *culpa* adalah perbuatan yang merupakan tindak pidana yang tidak ada dasar niat untuk melakukan kejahatan tetapi karena kecerobohan atau kurang hati-hatinya yang mengakibatkan terjadinya kejahatan.

Untuk melihat pertanggungjawaban pidana didalam tindak pidana penyalahgunaan

---

<sup>25</sup> Khoirotn Nisa, "Urgensi Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik Dalam Penanganan Atas Kejahatan Carding Di Bank X," *Journal of Islamic Business Law* 4, no. 3 (2020): 1-11.

<sup>26</sup> Michael Donegan, "Crime Script for Mandate Fraud," *Journal of Money Laundering Control* 22, no. 4 (2019): 770-81, <https://doi.org/10.1108/JMLC-03-2019-0025>.

kartu kredit milik orang lain baik itu pemalsuan, pencurian dan penipuan dapat dilakukan sebagai berikut:

- 1) Kemampuan Bertanggung Jawab  
Pengguna yang bertanggung jawab dalam tindak pidana penyalahgunaan kartu kredit, baik melakukan pemalsuan, penipuan dan pencurian. Hal ini di bebankan kepada pengguna bukan kepada pemilik, karena pengguna yang menggunakan kartu kredit untuk bertanggung jawab terhadap tindak pidana yang dilakukannya.ada kemampuan, artinya pelaku kejahatan Artinya penyalahgunaan kartu kredit dipandang mampu bertanggung jawab yang didasarkan kepada sehat jasmani dan rohani.
- 2) Kesalahan  
Unsur kesalahan pada tindak pidana penyalahgunaan kartu kredit milik orang lain harus dibuktikan bahwa pengguna sengaja melakukan tindak pidana tersebut. Hal ini dijelaskan oleh pasal-pasal yang dapat dikenakan kepada pengguna, seperti pasal 263, 362 dan 378 yang terdapat kata sengaja pada pasal-pasal tersebut. Adanya kesalahan (dalam hal ini kesengajaan), artinya perbuatan dari pelaku kejahatan penyalahgunaan kartu kredit memang terdapat kesalahan yang sengaja dibuatnya
- 3) Tidak Ada Alasan Pemaaf  
Berdasarkan uraian diatas pengguna mampu mempertanggung-jawabkan perbuatannya sehat jasmani dan rohani, ia melakukan perbuatan itu tidak dalam keadaan terpaksa atau tertekan maupun bukan untuk melakukan pembelaan darurat yang melampaui batas. Perbuatan tersebut dilakukan dengan sengaja dan dalam keadaan normal. Perbuatan pengguna bukan dilakukan karena perintah jabatan sehingga dapat disimpulkan dia melakukan atas kehendak sendiri. Maka pengguna dalam hal ini tidak memiliki alasan pemaaf atas perbuatannya. tidak ada alasan pemaaf, artinya perbuatan pelaku tersebut tidak memiliki dasar untuk dimaafkan akan tetapi harus dihukum.

#### 4. Kesimpulan

Pengaturan hukum pidana terhadap tindak pidana pembobolan kartu kredit atau tindak pidana carding diatur dalam Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, pengaturan hukum selain dalam Undang-Undang Informasi dan Transaksi Elektronik kejahatan carding dapat dirumuskan dalam KUHP dengan menggunakan metode interpretasi ekstensif terhadap pasal-pasal yang terdapat dalam KUHP yaitu Pasal 362, 363 dan 378 KUHP yaitu tentang pencurian dan penipuan. Menurut modus operandinya diatur dalam Undang-Undang nomor 19 tahun 2016 pada Pasal 30 jo Pasal 46 sebagai pasal tentang pencurian, Pasal 34 ayat (1) jo Pasal 50 sebagai pasal tentang pencurian dilakukan dengan kerjasama oleh dua orang atau lebih, Pada Pasal 35 jo Pasal 51 ayat (1) atau Pasal 32 jo Pasal 48 sebagai pasal tentang penipuan. Pertanggungjawaban pidana pelaku pembobolan kartu kredit dapat dilakukan berdasarkan kemampuan bertanggung jawab pelaku, adanya kesalahan dalam bentuk kesengajaan pelaku yang dibuktikan sesuai Pasal 362, 363 dan 378 KUHP, tidak ada alasan pemaaf atas perbuatannya



dan dapat dikenakan sanksi bagi pelaku tindak pidana pembobolan kartu kredit.

## Daftar Referensi

- BPHN, and Departemen Kehakiman. "Laporan Akhir Penelitian Masalah-Masalah Hukum Kejahatan Perbankan." Jakarta, 1992.
- Chazawi, Adami. *Pelajaran Hukum Pidana (Stelsel Tindak Pidana, Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana)*. Jakarta: Raja Grafindo Persada, 2002.
- Donegan, Michael. "Crime Script for Mandate Fraud." *Journal of Money Laundering Control* 22, no. 4 (2019): 770–81. <https://doi.org/10.1108/JMLC-03-2019-0025>.
- Faridi, Muhammad Khairul. "Kejahatan Siber Dalam Bidang Perbankan." *Cyber Security Dan Forensik Digital* 1, no. 2 (2018): 57–61.
- Gumilang, D., Otto Yudianto, and Erny Herlin Setyorini. "Legalitas Surat Kuasa Yang Diterbitkan Seorang Buron." *Jurnal Hukum Magnum Opus* 2, no. 2 (2019): 125–36. <https://doi.org/10.30996/jhmo.v2i2.2497>.
- Hardeveld, Gert Jan van, Craig Webber, and Kieron O'Hara. "Discovering Credit Card Fraud Methods in Online Tutorials." In *Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention*, 1:1–5, 2016. <https://doi.org/10.1145/2915368.2915369>.
- Haryanto, Toto. "Modus Baru Pencurian Kartu Kredit Terungkap." *Totoharyato.Com*. Jakarta, 2015.
- Jovan, F N. *Pembobol Kartu Kredit- Menyingkap Teknik Dan Cara Kerja Para Carder Di Internet*. Jakarta: Mediakita, 2006.
- Kartonegoro. *Diktat Kuliah Hukum Pidana*. Jakarta: Balai Lektur Mahasiswa, 1987.
- Kasmir. *Bank Dan Lembaga Keuangan Lainnya*. Jakarta: Raja Grafindo Persada, 2014.
- Kleden, Kristoforus Laga. "Pisau Analisis Kriminologi Prostitusi Online." *DiH: Jurnal Ilmu Hukum* 15, no. 1 (2019): 68–78. <https://doi.org/10.30996/dih.v15i1>.
- Labetubun, Muchtar Anshary Hamid, Esther Kembauw, Supiah Ningsih, Surya Putra, Siti Epa Hardiyanti, Ahmad Bairizki, Binti Mutafarida, et al. "Fungsi Dan Peranan Bank Indonesia Dan Bank Umum." In *Manajemen Perbankan (Sebuah Tinjauan Teori Dan Praktis)*. Bandung: Widina Bhakti Persada, 2021.
- Labetubun, Muchtar Anshary Hamid, Atika Zahra Maulida, Diana Triwardhani, Husain, Christina Bagenda, Lucky Nugroho, Titin Hargyatni, et al. "Sistem Keuangan Dan Lembaga Keuangan Di Indonesia." In *Lembaga Keuangan Bank Dan Non Bank (Sebuah Tinjauan Teori Dan Praktis)*. Bandung: Widina Bhakti Persada, 2021.
- Mardhatillah, Adam Bastian, and Ahmad Mahyani. "Bukti Tidak Langsung Sebagai Dasar Hakim Menjatuhkan Pidana (Putusan Nomor: 777/ Pid.B/ 2016/ PN.JKT.PST)." *Mimbar Keadilan* 12, no. 1 (2019): 59–66. <https://doi.org/10.30996/mk.v12i1.2167>.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2016.

- Michael, Tomy. "The HE Inhited Conditions In The Draft Regulation of Surabaya Mayor About The Procedur of Choosing The Management of Community Empowerment of Village Institusion, Citizen Association And Neighborhood Association." *Jurnal Hukum Magnum Opus* 2, no. 2 (2019): 174-84.
- Nisa, Khoirotun. "Urgensi Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik Dalam Penanganan Atas Kejahatan Carding Di Bank X." *Journal of Islamic Business Law* 4, no. 3 (2020): 1-11.
- Pentury, Ronald. "Tinjauan Kriminologi Terhadap Kejahatan Perbankan." Universitas Pattimura, 2013.
- Rahmanto, Tony Yuri. "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik." *Jurnal Penelitian Hukum De Jure* 19, no. 1 (2019): 31-52. <https://doi.org/10.30641/dejure.2019.V19.31-52>.
- Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi*. Jakarta: Rajawali Pers, 2012.
- Sutarman. *Cyber Crime-Modus Operandi Dan Penanggulangannya*. Yogyakarta: LaksBang Pressindo, 2007.
- Wahid, Abdul, and Mohammad Labib. *Kejahatan Mayantara*. Bandung: Refika Aditama, 2005.
- Wilyana, Rezy Januar, Imam Budi Santoso, and Oci Senjaya. "Pembuktian Bukti Elektronik Di Persidangan." *Singaperbangsa Law Review* 1, no. 1 (2020): 164-83.