MANDUB: Jurnal Politik, Sosial, Hukum dan Humaniora
Volume 2, Nomor 4, Tahun 2024
e-ISSN: 2988-2273, p-ISSN: 2988-2281, Hal 189-197
DOI: https://doi.org/10.59059/mandub.v2i4.1760
Available Online at: https://journal.staiypiqbaubau.ac.id/index.php/Mandub

Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan dengan Mode *Skimming* Ditinjau dari Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik

Ludgardis Goo Nembo [1*], Bhisa Vitus Wilhelmus [2], Debi F.Ng. Fallo [3]
[1-3] Universitas Nusa Cendana, Indonesia

Alamat Kampus: Jln Adisucipto, Penfui, Kupang, Nusa Tenggara Timur
Korespondensi penulis:ludgardisnembo@gmail.com *

Abstract, *Banking is one of the financial services companies that has provided services to the community and businesses, Behind this development there are various legal problems related to information crime and electronic transactions in the banking sector, Skimming is the act of stealing debit or credit card information by accessing an independent cash machine and copying the information contained on the magnetic stripe of the debit card or credit belonging to the customer (victim) illegally to have control over the customer's (victim) account. The application of the law to the crime of ATM skimming is regulated in Article 362 of the Criminal Code (KUHP) regarding the crime of theft. This research is a type of normative judicial research supported by a normative approach by using primary legal materials, secondary legal materials and tertiary legal materials as data sources. This study uses a prescriptive method, which is an analysis method that provides an assessment (justification) about the object being researched whether it is true or false, or what should be according to the law. The results of the study show that (1) Skimming is a magnetic stripe crime that exists on ATM cards illegally to have control over the card or the account by duplicating the ATM card or by installing a hidden camera to find out the ATM PIN of the customer or victim. (2) Strategies to prevent unauthorized access and early detection of suspicious activities can be applied to reduce the incidence of criminal acts and effective cyber security is to strengthen the network and security system. This can include investing in cutting-edge security technologies, such as robust firewalls, active network monitoring, and security programs that can detect suspicious attacks. In addition, organizations also need to involve their employees in cybersecurity efforts.*

Keywords: *Legal Liability, Skimming, Legal Protection, Skimming Prevention Strategy*

Abstrak, Perbankan merupakan salah satu Perusahaan penyediaan jasa keuangan yang telah memberikan pelayanan kepada masyarakat dan bisnis, Dibalik perkembangan ini terdapat berbagai permasalahan hukum yang berkaitan dengan kejahatan informasi dan transaksi elektronik dibidang perbankan, *Skimming* adalah tindakan pencurian informasi kartu debit atau kredit dengan cara mengakses anjungan tunai mandiri dan menyalin informasi yang terdapat pada strip magnetik kartu debit atau kredit milik nasabah (korban) secara ilegal untuk memiliki kendali atas rekening nasabah (korban). Penerapan hukum terhadap tindak pidana kejahatan *Skimming* ATM diatur dalam Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) mengenai tindak pidana pencurian. Penelitian ini merupakan jenis penelitian yudiris normatif yang didukung pendekatan normatif dengan menggunakan bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier sebagai sumber data. Penelitian ini menggunakan metode preskriptif yaitu metode analisis yang memberikan penilaian (justifikasi) tentang obyek yang diteliti apakah benar atau salah, atau apa yang seyogyanya menurut hukum. Hasil Penelitian menunjukkan (1) *Skimming* adalah suatu kejahatan magnetic stripe yang ada pada kartu ATM dengan illegal untuk memiliki kendali atas kartu tersebut atau rekening tersebut dengan cara menggandakan kartu ATM ataupun dengan memasang hidden camera untuk mengetahui PIN ATM nasabah atau korban. (2) Strategi pencegahan akses tidak sah serta deteksi dini terhadap kegiatan mencurigakan dapat diterapkan untuk mengurangi insiden tindak pidana dan keamanan cyber yang efektif adalah dengan memperkuat jaringan dan sistem keamanan. Hal ini dapat mencakup investasi dalam teknologi keamanan yang mutakhir, seperti firewall yang kuat, pemantauan jaringan yang aktif, dan program keamanan yang dapat mendeteksi serangan yang mencurigakan. Selain itu, organisasi juga perlu melibatkan karyawan mereka dalam upaya keamanan *cyber*.

Kata Kunci: Pertanggungjawaban Hukum, *Skimming*, Perlindungan Hukum, Strategi Pencegahan *skimming*

Received Oktober 03, 2024; Revised Oktober 29, 2024; Accepted November 30, 2024; Online Available Desember 02, 2024

1. LATAR BELAKANG

Perbankan merupakan salah satu Perusahaan penyediaan jasa keuangan yang telah memberikan pelayanan kepada masyarakat dan bisnis. Sebagai upaya meningkatkan pelayanan,perbankan telah menerapkan teknologi di berbagai bidang salah satunya pada anjungan tunai mandiri (ATM). ATM digunakan sebagai pengganti fungsi kasir dalam bertransaksi seperti penarikkan tunai serta proses transaksi lainnya.Munculnya modus operandi kejahatan pembobolan ATM ini, menjadi pemicu munculnya dampak yang ditimbulkan. Dampak atas kejahatan pembobolan ATM tersebut antara lain yang terjadi viktimisasi secara langsung dan tidak langsung kepada masyarakat. Kerugian secara material dan non material kepada sistem perbankan secara khusus dan sistem perekonomian secara umum.Kegiatan perbankan dengan electronic transaction (*e-banking*) melalui mesin ATM, telepon seluler (*phone banking*) dan jaringan internet (internet *banking*),merupakan beberapa contoh pelayanan transaksi perbankan dengan teknologi informasi.Dari sisikeamanan, penggunaaan teknologi dapat memberi perlindungan keamanan data dan transaksi.

Dibalik perkembangan ini terdapat berbagai permasalahan hukum yang berkaitan dengan kejahatan informasi dan transaksi elektronik dibidang perbankan,jika tidak diantisipasi dengan baik, tentu akan merugikan bank,masyarakat dan nasabah. Dalam tatanan implementasi ,teknologi informasi dan komunikasi layaknya pisau bermata dua.Satu sisi teknologi informasi memberikan manfaat yang tidak sedikit terhadap peningkatan sektor pelayanan baik public maupun pelayanan internal.Disisi lain teknologi informasi digunakan oleh orang-orang yang tidak bertangggungjawab dengan melakukan perbuatan yang sifatnya melawan hukum, yang menyerang berbagai kepentingan hukum orang banyak,masyarakat dan negara.

Skimming adalah tindakan pencurian informasi kartu debit atau kredit dengan cara mengakses anjungan tunai mandiri dan menyalin informasi yang terdapat pada strip magnetik kartu debit atau kredit milik nasabah (korban) secara ilegal untuk memiliki kendali atas rekening nasabah (korban). Penerapan hukum terhadap tindak pidana kejahatan *Skimming* ATM diatur dalam Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) mengenai tindak pidana pencurian. Untuk mengatur tata cara penggunaan teknologi informasi dan komunikasi di Indonesia, pemerintah mengeluarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Tindak pidana *Skimming* di dalam Undang-Undang ITE diatur dalam Pasal 30 ayat (1) jo Pasal 46 ayat (1) Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. jo Pasal 30 ayat (1) Undang-undang Nomor 1 Tahun 2024 tentang

Perubahan atas Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik.

Modus dalam aksi *Skimming* merupakan metode yang digunakan untuk mencuri informasi nasabah pada saat bertransaksi menggunakan *Automatic Teller Machine* (ATM). Komponen utama yang digunakan yaitu skimmer, hidden camera atau spy camera dan keypad.

Salah satu contoh kasus *skimming* yang terjadi yaitu pada rekening BNI 46 Cabang Kupang. Uang dalam rekening milik 69 nasabah Bank Negara Indonesia (BNI) 46 Cabang Kupang dikuras oknum tak bertanggung jawab. Uang dalam rekening nasabah itu diketahui ditarik tanpa sepengetahuan nasabah melalui penarikan tunai. Puluhan nasabah baru menyadari kondisi tersebut setelah mendapat notifikasi melalui SMS Banking BNI pada kurun waktu Rabu malam (12/9/2019) hingga Kamis pagi (13/9/2019).

Akibatnya uang ratusan juta milik nasabah raib begitu saja. Pemimpin Cabang BNI 46 Kupang I Gede Wirata saat dikonfirmasi Liputan6.com membenarkan peristiwa tersebut. Dia mengatakan, para nasabah yang mengalami kondisi tersebut telah mengadukannya ke manajemen BNI 46 Cabang Kupang sejak Kamis pagi. Jadi teknik tersebut memungkinkan pelaku untuk mengirimkan data yang didapat dari skimmer ke komputer atau smartphone yang dipasang di lokasi tertentu, dan pelaku *skimming* dapat mengakses data dimana saja.

2. METODE PENELITIAN

Jenis penelitian ini merupakan penelitian dapat dilakukan dengan menggunakan pendekatan penelitian hukum normatif (*Yuridis Normatif*). Aspek-aspek yang menjadi fokus penelitian ini, yaitu pertanggungjawaban pidana bagi pelaku tindak pidana pencurian data nasabah perbankan dengan mode *skimming* ditinjau menurut undang-undang informasi dan transaksi elektronik serta strategi pencegahan akses tidak sah serta deteksi dini terhadap kegiatan mencurigakan dapat diterapkan untuk mengurangi insiden tindak pidana pencurian data nasabah perbankan.

Dalam penelitian hukum normatif atau kepustakaan teknik pengumpulan data dalam penelitian hukum normatif dilakukan dengan studi pustaka terhadap bahan-bahan hukum, baik bahan hukum primer, bahan hukum sekunder, maupun bahan hukum tersier dan atau bahan non hukum. Metode analisis untuk jenis penelitian hukum normatif menggunakan metode preskriptif dengan memberikan penilaian (justifikasi) tentang obyek yang diteliti apakah benar atau salah, atau apa yang seyogyanya menurut hukum.

3. HASIL DAN PEMBAHASAN

Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Mode *Skimming* Ditinjau Menurut Undang-Undang Informasi Dan Transaksi Elektronik

Udang-Undang Informasi dan Transaksi Elektronik mengatur berbagai aspek terkait penggunaan teknologi informasi dan transaksi elektronik, termasuk perlindungan data pribadi dan tindakan pidana yang terkait dengan topik teknologi informasi.Yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 pasal 30 dan pasal 32 Tentang Informasi dan Transaksi Elektronik. Pasal-pasal dalam Undang-Undang mencakup ketentuan mengenai pengakuan informasi elektronik sebagai alat bukti hukum, serta larangan terhadap tindakan-tindakan yang merugikan pihak lain, seperti pencurian data. Kemampuan bertanggung jawab bagi pelaku tindak pidana *skimming* dapat dilihat dari beberapa aspek, yaitu:

a. Aspek Hukum : Pelaku dapat dikenakan sanksi sesuai dengan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik, khususnya pada pasal-pasal yang mengatur tentang tindakan ilegal dalam penggunaan informasi elektronik. Misalnya, Pasal 30 yang mengatur tentang akses ilegal ke sistem elektronik
b. Aspek Pembuktian : Dalam konteks hukum, informasi elektronik yang diperoleh melalui tindakan *skimming* dapat digunakan sebagai alat bukti. Undang-Udang Informasi dan Transaksi Elektronik menetapkan bahwa dokumen elektronik memiliki kekuatan hukum yang sama dengan dokumen fisik, selama memenuhi persyaratan tertentu.
c. Aspek Tanggung Jawab : Menurut Undang-Undang Informasi dan Transaksi Elektronik , pelaku tindak pidana bertanggung jawab atas segala akibat hukum dari tindakan mereka. Jika pencurian data menyebabkan kerugian bagi nasabah atau bank, pelaku dapat dikenakan sanksi pidana dan perdata.

Sanksi pidana merupakan hukuman yang dikenakan oleh negara terhadap seseorang yang dinyatakan bersalah karena melakukan tindak pidana (kejahatan atau pelanggaran hukum). Tujuan utama sanksi pidana adalah untuk menghukum pelaku, mencegah tindak pidana lebih lanjut, memperbaiki perilaku pelaku, dan memberikan efek jera kepada masyarakat.

Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi dan Elektronik yang diubah pertama kali dengan Undang-Undang Nomor 19 Tahun 2016 dan diubah kedua kalinya dengan Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik pasal 30 ayat 2 menyataan bahwa pelanggaran terhadap pasal ini diancam dengan sanksi pidana, sebagaimana diatur dalam Pasal 46 ayat (2) UU ITE, pelaku dapat

dipidana dengan pidana penjara paling lama 7 tahun dan/atau denda paling banyak Rp700.000.000,00. Ini menunjukkan betapa seriusnya hukum memandang tindakan pencurian data melalui akses ilegal ke sistem elektronik, ayat 3 menyatakan bahwa pelanggaran terhadap pasal ini dapat dikenakan sanksi pidana yang lebih berat dibandingkan dengan akses ilegal biasa. Berdasarkan ketentuan yang ada, pelaku dapat dijatuhi hukuman penjara hingga 8 tahun dan/atau denda hingga Rp800.000.000,00, sesuai dengan Pasal 46 UU ITE.

Pemberian sanksi ini bertujuan untuk memberikan efek jera bagi pelaku kejahatan Cyber serta melindungi hak-hak pemilik data elektronik yang disimpan dalam sistem elektronik agar tidak disalahgunakan atau dirusak oleh pihak yang tidak berhak dan juga sebagai langkah preventif untuk menjaga keamanan transaksi elektronik dan perlindungan data pribadi masyarakat.

Salah satu contoh tindak pidana pencurian data nasabah melalui Metode *skimming* ialah yang terjadi pada tahun 2019,di BNI (Bank Negara Indonesia) 46 cabang kupang dimana uang dalam rekening 69 nasabah dikuras oleh orang tak bertanggung jawab namun berdasarkan berita yang beredar keberadaan pelaku tidak diketahui keberadaannya .Menanggapi keluhan para nasabah yang terdampak atas kejadian ini pihaknya bekerja cepat dan berkoordinasi dengan Kantor Pusat BNI 46 di Jakarta untuk melakukan investigasi internal terhadap kondisi tersebut. Dari investigasi tim kantor pusat, diketahui bahwa memang itu adalah tindak kejahatan *skimming*, yang dilakukan oleh pihak yang tidak bertanggung jawab. Pihak BNI juga langsung menjelaskan perihal *skimming* dan menangani masalah tersebut dengan menanggung seluruh kerugian para nasabah yang melakukan komplain ke rekening mereka masing-masing,sesuai jumlah saldo yang tercatat.

Berdasarkan contoh kasus diatas peneliti melihat bahwa terjadi pergeseran peretanggungjawaban. Dimana dalam hukum pidana, pertanggungjawaban pidana dibebankan kepada pelaku yang melakukan tindak pidana. Namun dalam kasus tertentu, pertanggung jawaban dapat bergeser kepada instansi atau badan hukum. Pertanggungjawaban pidana bisa berpindah ke instansi atau pihak lain dalam situasi di mana pelaku utama kabur dan ada bukti kelalaian atau kesalahan dari pihak yang seharusnya bertanggung jawab. Pertanggungjawaban pidana dapat berpindah ke instansi lain jika terdapat hubungan kewenangan, bukti kelalaian atau kesalahan dalam pengawasan, serta adanya pelanggaran hukum yang jelas berdasarkan beberapa syarat salah satunya unsur kesalahan (mens rea) yang harus dibuktikan dalam konteks hukum pidana.

Strategi Pencegahan Akses Tidak Sah Serta Deteksi Dini Terhadap Kegiatan Mencurigakan Dapat Diterapkan Untuk Mengurangi Insiden Tindak Pidana

1. Langkah-Langkah Keamanan Fisik

Keamanan fisik sangat penting untuk mencegah pencurian data nasabah, terutama dalam lingkungan perbankan dan perusahaan yang menangani informasi sensitif. Berikut adalah beberapa langkah keamanan fisik yang bisa diambil untuk melindungi data nasabah dari akses ilegal atau pencurian:

a) Kontrol Akses ke Lokasi Fisik
b) Pengawasan di Area Sensitif Penggunaan Kamera Pengawas (CCTV)
c) Proteksi Perangkat Keras
d) Pengelolaan Arsip dan Dokumen Fisik
e) Keamanan pada Perangkat Mobile
f) Pelatihan Karyawan
g) Audit dan Pemeliharaan Rutin
h) Backup Data dan Pemulihan Bencana

2. Monitoring Dan Analisis Data Dalam Kegiatan Transaksi Dan Pola Transaksi Yang Mencurigakan

Monitoring dan analisis data dalam kegiatan transaksi dan pola transaksi yang mencurigakan merupakan bagian penting dari upaya pencegahan pencucian uang, pendanaan terorisme, serta aktivitas penipuan dalam sistem keuangan. Proses ini umumnya dilakukan dengan mengidentifikasi pola yang tidak normal atau mencurigakan yang mungkin menunjukkan adanya aktivitas ilegal.

Lembaga keuangan diwajibkan untuk melakukan pemantauan terhadap aktivitas transaksi nasabah. Proses ini meliputi:

a) Pemantauan Rekening
b) Analisis Data Transaksi
c) Pelaporan kepada PPATK

Monitoring dan analisis data dalam kegiatan transaksi dan pola transaksi yang mencurigakan merupakan bagian penting dari upaya pencegahan pencucian uang, pendanaan terorisme, serta aktivitas penipuan dalam sistem keuangan.

3. Kolaborasi dengan penegak hukum

Kolaborasi antara bank dan penegak hukum dalam mencegah akses tidak sah serta *skimming* sangat penting untuk menjaga keamanan sistem perbankan. Melalui peningkatan

keamanan, edukasi publik, sistem pelaporan yang efisien, analisis data transaksi, investigasi bersama, dan perlindungan hukum, langkah-langkah ini dapat membantu mengurangi risiko kejahatan cyber dan melindungi nasabah dari kerugian finansial, beberapa aspek penting mengenai kolaborasi dengan penegak hukum sebagai berikut:

a) Peningkatan Sistem Keamanan
b) Pendidikan dan Kesadaran Masyarakat
c) Pelaporan dan Tindak Lanjut
d) Analisis Data Transaksi
e) investigasi Bersama
f) Perlindungan Hukum

4. KESIMPULAN DAN SARAN

Kesimpulan

1. *Skimming* adalah suatu kejahatan magnetic stripe yang ada pada kartu ATM dengan illegal untuk memiliki kendali atas kartu tersebut atau rekening tersebut dengan cara menggandakan kartu ATM ataupun dengan memasang hidden camera untuk mengetahui PIN ATM nasabah atau korban.
2. Strategi pencegahan akses tidak sah serta deteksi dini terhadap kegiatan mencurigakan dapat diterapkan untuk mengurangi insiden tindak pidana dan keamanan cyber yang efektif adalah dengan memperkuat jaringan dan sistem keamanan. Hal ini dapat mencakup investasi dalam teknologi keamanan yang mutakhir, seperti firewall yang kuat, pemantauan jaringan yang aktif, dan program keamanan yang dapat mendeteksi serangan yang mencurigakan. Selain itu, organisasi juga perlu melibatkan karyawan mereka dalam upaya keamanan *cyber*. Mengedukasi karyawan mengenai praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat dan tidak membuka email atau lampiran yang mencurigakan, dapat membantu mencegah serangan *cyber*. Selain itu, organisasi juga harus memperhatikan kebijakan dan prosedur keamanan

Saran

1. Mengembangkan strategi keamanan *cyber* yang efektif adalah kunci untuk melindungi bisnis dan individu dari ancaman kejahatan *cyber*. Ini mencakup penilaian terhadap jenis data yang disimpan, ancaman potensial, dan potensi dampaknya.
2. Respons cepat dapat membantu mencegah kerugian lebih lanjut. Sertakan rencana pemulihan keamanan yang rinci untuk mengatasi serangan dan memulihkan operasi

secepat mungkin. Ini dapat mencakup aturan keamanan untuk penggunaan perangkat pribadi, kebijakan sandi yang kuat, dan hak pengguna.

3. Identifikasi dan perbaiki kelemahan yang mungkin ditemukan selama audit. Dengan menggabungkan langkah-langkah ini, organisasi dan individu dapat mengembangkan strategi keamanan cyber yang komprehensif dan adaptif untuk melindungi diri dari ancaman yang terus berkembang.

DAFTAR REFERENSI

Adam Chazawi. (2015). *Tindak Pidana Informasi Dan Transaksi Elektronik.* Malang: Media Nusa Crative.

Ade Arthesa dan Edia Handiman. (2009,). *Bank dan Lembaga Bukan Bank Edisi 3,*. Jakarta:: Indeks.

Chazawi., A. (2021.). *Kejahatan Terhadap harta Benda.* Malang:: MNC Publishing.

Dian Ekawati, (. 1.-u. (2018). "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan,". *Unnes Law Review 1, no. 2*, hal. 159. Diambil kembali dari https://review-unes.com/index.php/law/article/view/24/15.

Dr.Neni Sri Imaniyati, S. (2020). *Pengantar Hukum Perbankan Indonesia.* Bandung: PT. Refika Aditama.

Enrick, M. (2022). "Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dengan Pengajuan Restitusi,". *Jurnal Jurist Diction, Vol. 1 Nomor 2, Agustus 2022*, 124-133.

Ida Hanifah, d. (2018). *Pedoman Penulisan Tugas Akhir Mahasiswa.* Medan: CV Pustaka Prima.

Ilhami Bisri. (2005). *Sistem Hukum Indonesia.* Cet. II; Jakarta:: PT Raja Grafindo Persada.

Kitab Undang-Undang Hukum Pidana

Mahesa Jati Kusuma, ,. (2017,). *Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan ITE di Bidang PerBankan.* Bandung:: Nusa Media,.

Melania Karsa MR. (2022). *Pedoman Penulisan Tugas Akhir.* Kupang: FH.

Muladi dan Barda Nawawi Arief. (1998). *Teori-Teori dan Kebijakan Pidana.* Bandung: Alumni,.

Nugroho, J. L. A., Manafe, D. R. C., & Dima, A. D. (2024). Penegakan Hukum Pidana terhadap Pelaku Tindak Pidana Penjual Pangan Kedaluwarsa di Tinjau dari Undang-Undang Nomor 18 Tahun 2012 tentang Pangan di Kelurahan Lasiana, Kecamatan Kelapa Lima, Kota Kupang. *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora*, *2*(4), 25-37.

Pawit M. Yusup dan Priyo Subekti. (2010). *Teori dan Praktek Penelusuran Infomasi (Informasi Retrieval)* . (Cet. I; Jakarta: ,): Kencana Prenada Media Group.

Raida L. Tobing. (2010)). *"Penelitian Hukum Tentang Efektivitas UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik", Laporan Akhir.* (Jakarta:: Badan Pembinaan Hukum Nasional,.

Roeslan Saleh, L. (Loc.Cit.). *Loc.Cit.* Loc.Cit.: Loc.Cit.

Sinlaeloe, L. I., Medan, K. K., & Manafe, D. R. C. (2024). PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI PEMINJAM DALAM LAYANAN APLIKASI PINJAMAN ONLINE (STUDI KASUS DI KOTA KUPANG). *Petitum Law Journal*, *1*(2), 584-595.

Shaikh Aijaz Ahmed dan Shah Syed Mir Muhammad. (2012). Auto Teller Machine (ATM) Fraud – Case Study of a Commercial Bank in Pakistan, International Journal of Business and Management.

Sri Redjeki Hartono, H. A. (2001). *Hukum Asuransi dan Perusahaan Asuransi.* Jakarta: Sinar Grafika.

Supromono, G. (2014). *Hukum Uang Indonesia.* Dyokarta: Gramata Publishing.

Undang-Undang ITE

Undang-Undang Perbankan

Undang-undang RI Tahun 1945

Victoria Linggoharjo, M. H.-t.-j.-k.-p.-m. (2020). Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming,". *Magister Hukum Arumentum 7, no. 1*. Diambil kembali dari https://media.neliti.com/media/publications/339486-tanggung-jawab-kejahatan-perbankan-melal557e7cc7.pdf

Yulies Tiena Masriani. (2017). *Pengantar Hukum Indonesia* . Jakarta: Sinar Grafika.

Zaidan., A. (2015). *Menuju Pembaruan Hukum Pidana.* Jakarta : Sinar Grafika.