

URGENSI PENGATURAN PERLINDUNGAN DATA PRIBADI PADA NASABAH DALAM MENANGGULANGI TINDAK PIDANA *SKIMMING*

I Dewa Gede Waisha Permana¹, Komang Octaviani Dewi²

¹Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia Bali,
E-mail:(waisha.permana@gmail.com)

Abstrak

Perlindungan hukum terhadap data pribadi pada nasabah di Indonesia masih belum optimal, hal tersebut dapat dilihat dari masih banyaknya penyalahgunaan data pribadi seseorang karena kurangnya pengawasan dari pihak-pihak pengguna data. Urgensi pemberian perlindungan hukum kepada data pribadi ini mulai diperhatikan seiring dengan meningkatnya kasus yang berkaitan dengan kebocoran data pribadi seseorang dan berakhir kepada aksi penipuan atau tindak kriminal *skimming*. Dengan tujuan memahami dan mengkaji pengaturan hukum yang berkaitan dengan perlindungan data pribadi nasabah dalam menanggulangi tindak pidana *skimming* dan menganalisis bentuk penyelesaian hukum tindak pidana *skimming* terkait dengan perlindungan data pribadi nasabah. Metode penelitian yang digunakan adalah yuridis normatif melalui pendekatan perundang-undangan, pendekatan konseptual. Pengaturan perlindungan hukum data pribadi pada nasabah secara khusus dan komprehensif yang berkaitan dengan perbankan ataupun hal lainnya belum ada, akan tetapi umumnya yang selalu dijadikan rujukan pengaturan hukum berkaitan dengan data pribadi adalah Undang-Undang Informasi dan Transaksi Elektronik. Penyelesaian hukum yang digunakan dalam perkara tindak pidana *skimming* sudah pasti menggunakan jalur litigasi (pengadilan) sehingga pelaku kejahatan *skimming* segera dijatuhkan hukuman atas perbuatan tindak pidana yang dilakukan dengan menggunakan Pasal 363 ayat 1 ke-4 dan ke-5 untuk pelaku kejahatan tindak pidana pencurian *skimming* dan Pasal 378 KUH Pidana untuk kasus tindak pidana penipuan *skimming*.

Kata Kunci: Perlindungan, Data Pribadi, *Skimming*

Abstract

Legal protection of personal data on customers in Indonesia is still not optimal, it can be seen from the number of misuses of personal data due to lack of supervision from parties using data. The urgency of providing legal protection to personal data is starting to be noticed along with the increasing number of cases related to the leakage of a person's personal data and ending in fraudulent acts or criminal acts of skimming. With the aim of understanding and reviewing legal arrangements relating to the protection of customers' personal data in tackling skimming crimes and analyzing forms of legal settlements for skimming crimes related to the protection of customers' personal data. The research method used is normative juridical through a statutory approach, a conceptual approach. There are no specific and comprehensive arrangements for legal protection of personal

data for customers related to banking or other matters, but generally, what is always used as a reference for legal arrangements relating to personal data is the Electronic Information and Transaction Law. The legal settlement used in the case of the crime of skimming is certain to use litigation (courts) so that the perpetrators of the crime of skimming are immediately sentenced for criminal acts committed using Article 363 paragraphs 1, 4 and 5 for the perpetrators of the crime of skimming theft. and Article 378 of the Criminal Code for cases of skimming fraud.

Keywords: Protection, Personal Data, Skimming

1. PENDAHULUAN

1.1. Latar Belakang Masalah

Media elektronik merupakan perkembangan teknologi informasi yang seringkali berkaitan dengan berbagai macam kegiatan baik itu kegiatan pemerintahan, transaksi bisnis dan komunikasi. Hal ini dilakukan secara *online* namun memiliki dampak yang beresiko apabila informasi tersebut disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Dengan adanya penyalahgunaan data pribadi, maka dapat terlihat adanya kelemahan sistem, kurangnya pengawasan, sehingga data pribadi dapat disalahgunakan dan mengakibatkan kerugian bagi pemilik data tersebut. Penyalahgunaan, pencurian, penjualan data pribadi merupakan suatu pelanggaran hukum dalam bidang teknologi informasi dan juga dapat dikategorikan sebagai pelanggaran atas hak asasi manusia, karena data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi

Data-data pribadi berkenaan dengan kependudukan dan demografis di sangat penting dilindungi agar tidak mudah dieksploitasi. Ada beberapa bentuk penyalahgunaan data seperti penjualan data, data profiling, tujuan pemasaran, penelitian. Penyalahgunaan data pribadi untuk tindak kriminal seperti pembuatan akun palsu, penipuan dalam jaringan, pencucian uang, pasar palsu dan juga transaksi ilegal. Oleh karena itu, diperlukan rangkaian pengamanan dan aturan yang komprehensif berkenaan dengan data pribadi.

Salah satu kasus yang berkaitan dengan penyalahgunaan data dan informasi adalah kasus *skimming* atau penyalinan data dan informasi kartu ATM nasabah yang kemudian pelaku

skimming melakukan penarikan dana dari tempat lain. Kamera pengintai sudah jarang digunakan seiring dengan semakin canggihnya alat *skimmer* yang digunakan para pelaku.¹

Skimming adalah teknik mengumpulkan informasi sebuah kartu kredit atau kartu ATM dengan cara menempatkan alat yang biasa disebut *skimmer*. Alat ini bertugas merekam jejak penggunaan sebuah kartu kredit atau kartu ATM. Jika alat ini dipasang dalam sebuah mesin ATM, otomatis semua kartu yang keluar masuk di mesin tersebut akan terekam data dan aktifitasnya.² Pelaku bisa mendapatkan data nomor kartu kredit atau debit korban menggunakan metode sederhana seperti halnya fotokopi, atau metode yang lebih canggih seperti menggunakan perangkat elektronik kecil (*skimmer*) untuk menggesek kartu lalu menyimpan ratusan nomor kartu kredit korban.³

Indonesia merupakan negara, dengan sistem dasar negara yang berpegang pada kedaulatan hukum yang pada hakikatnya bersumber dari Pancasila yang selaku sumber dari segala sumber hukum. Perlu dipahami bahwa Negara Indonesia merupakan suatu negara kesatuan yang berbentuk Republik yang berdasarkan atas

¹ Liputan6, *Begini Cara Kerja Skimming Kartu ATM*, diambil dari <http://www.liputan6.com/tekno/read/2049670/begini-cara-kerja-iskimmingi-kartu-atm>, diakses 12 Juli 2021.

² Sony Andes. (2018), *Pencegahan Kejahatan Skimming Perbankan*, <https://petrominer.com/pencegahan-kejahatan-skimming-perbankan/#>, diakses pada tanggal 25 Juni 2021.

³ Adi Suraji. (2019). *Pencurian melalui Skimming*, Universitas Gajah Mada, Jogjakarta, *Jurnal* Vol 6 No.4 .

hukum.⁴ Urgensi pemberian perlindungan hukum kepada data pribadi ini mulai diperhatikan seiring dengan meningkatnya jumlah pengguna media elektronik dan jumlah kasus yang muncul memiliki keterkaitan dengan kebocoran data pribadi seseorang yang berakhir kepada aksi penipuan atau tindak kriminal *skimming* menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi.

Berdasarkan uraian tersebut maka menarik untuk dikaji mengenai urgensi pengaturan perlindungan data pribadi pada nasabah dalam menanggulangi tindak pidana *skimming*. Adapun rumusan masalah yang akan dikaji yaitu: Bagaimanakah pengaturan perlindungan hukum data pribadi pada nasabah? Bagaimana penyelesaian hukum terhadap tindak pidana *skimming*?

Adapun tujuan yang ingin dicapai yaitu tujuan secara umum agar dapat mengembangkan ilmu pengetahuan hukum khususnya dibidang hukum pidana yang berkaitan dengan tindak pidana *skimming*. Dan tujuan secara khusus untuk memahami dan mengkaji pengaturan yang berkaitan dengan perlindungan data pribadi nasabah dalam menanggulangi tindak pidana *skimming* dan menganalisis bentuk penyelesaian hukum tindak pidana *skimming* terkait dengan perlindungan data pribadi nasabah.

2. METODE PENELITIAN

Sebuah penelitian hukum dilakukan sesuai dengan karakter

⁴ Abdul Wahid, Sunardi, dan Dwi Ari Kurniawati, (2019), *Membumi Konstitusi Indonesia sebagai Upaya Menjaga Hak Kebhinekaan, Yurispruden*, Vol. 2., No. 2. hlm. 186.

perspektif ilmu hukum untuk menentukan aturan-aturan hukum, prinsip-prinsip hukum dan juga doktrin-doktrin hukum sehingga dapat digunakan untuk menjawab isu hukum yang sedang dibahas.⁵ Penulisan mengenai Urgensi Pengaturan Perlindungan Data Pribadi Pada Nasabah Dalam Menanggulangi Tindak Pidana *Skimming* dikategorikan sebagai penelitian hukum normatif dengan menggunakan pendekatan perundang-undangan dan pendekatan konseptual.

Sumber bahan hukum yang digunakan dalam penulisan ini adalah data sekunder yang terdiri dari bahan hukum primer yang berupa peraturan dasar yang berkaitan dengan tindak pidana *skimming*. Bahan hukum sekunder merupakan penjelasan dari bahan hukum primer berupa hasil penelitian yang bersumber pada ilmu hukum. Serta bahan hukum tersier merupakan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder antara lain kamus dan ensiklopedia. Pengumpulan bahan hukum menggunakan studi dokumen dengan teknik analisis berupa deskripsi, interpretasi, sistematisasi, evaluasi, dan argumentasi hal-hal yang berkaitan dengan Urgensi Pengaturan Perlindungan Data Pribadi Pada Nasabah Dalam Menanggulangi Tindak Pidana *Skimming*.⁶

3. PEMBAHASAN

3.1. Pengaturan Perlindungan Hukum Data Pribadi pada Nasabah

Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama,

⁵ Marzuki, P.M. (2005), *Penelitian Hukum*, Jakarta: Prenada Media, hlm.35

⁶ Hartono, S., (2006), *Penelitian Hukum di Indonesia Pada Abad Ke – 20*, Bandung: PT.Alumni, hlm.134

umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.⁷ Menurut Jerry Kang, data pribadi mendeskripsikan suatu informasi yang erat kaitannya dengan seseorang yang dapat membedakan karakteristik masing-masing pribadi.⁸ Data dan informasi pribadi juga dapat dipahami bahwa data dan informasi itu berkenaan dengan kehidupan individu dan juga dekat kaitannya dengan konsep kerahasiaan atau hak privasi seseorang yang harus dijaga dan dilindungi oleh aturan perundang-undangan.

Di Indonesia terkait perlindungan hukum terhadap data pribadi pada nasabah masih dipandang belum optimal, hal tersebut dapat dilihat dari masih banyaknya penyalahgunaan data pribadi seseorang tanpa sepegetahuan dari pemiliknya yang diakibatkan kurang ketatnya pengamanan dan pengawasan dari pihak-pihak pengguna data. Contohnya mengisi aplikasi di Bank yang berkaitan dengan pembukaan rekening tabungan, pembuatan kartu ATM ataupun pembuatan kartu kredit yang dilakukan oleh nasabah secara tidak langsung nasabah dianggap telah menyetujui pengguna jasa dapat mengakses data pribadi kita. Akan tetapi sebagai nasabah dengan telah diberikannya data tersebut belum mendapatkan hak atau jaminan atas perlindungan kerahasiaan data pribadinya. Dan apabila terjadi

kebocoran data pribadi atau terjadi tindak pidana *skimming* seorang nasabah tidak mendapatkan perlindungan hukum yang berkaitan dengan hak-haknya. Aturan hukum berkaitan dengan perlindungan data pribadi di Indonesia juga masih bersifat umum karena aturannya dalam beberapa peraturan perundang-undangan yang terpisah dan hanya menggambarkan konsep perlindungan data pribadi secara general.

Hingga saat ini dapat dikatakan bahwa Indonesia tidak mempunyai kebijakan atau ketentuan yang mengatur tentang perlindungan data pribadi secara khusus, sampai sejauh ini masih termuat secara terpisah di beberapa peraturan perundang-undangan. Saat ini perlindungan data pribadi termuat di beberapa peraturan perundang-undangan, antara lain:

- Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan
- Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan
- Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
- Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Terkait dengan perlindungan hukum data pribadi pada nasabah tersebut tidak terlepas dari kendala yang akan dihadapi, misalnya kesulitan dalam melacak pelaku utamanya dan pembuktiannya sehingga menyebabkan

7

<http://kamusbahasaIndonesia.org/data%20pribadi/miripKamusBahasaIndonesia.org>. Diakses 12 Juli 2021.

⁸ Radian Adi Nugraha, (2012), *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Universitas Indonesia, hlm.. 31.

kesulitan dalam penanganannya. Boelewoekli berpandangan bahwa keterlibatan langsung pemerintah dan undang-undang dalam masalah data pribadi merupakan sesuatu yang dibutuhkan khususnya dalam menyelesaikan sengketa yang timbul dibidang telematika.⁹

Sampai saat ini undang-undang yang khusus secara komprehensif yang mengatur tentang perlindungan hukum data pribadi nasabah baik yang berkaitan dengan perbankan ataupun hal lainnya belum ada. Jika terjadi kasus, maka pengaturan hukumnya hanya akan merujuk pada undang-undang yang mengatur tentang penyalahgunaan data pribadi dan beberapa peraturan perundang-undangan lainnya, akan tetapi umumnya yang selalu dijadikan rujukan adalah Undang-Undang Informasi dan Transaksi Elektronik.¹⁰ Pengaturan mengenai perlindungan data pribadi diatur dalam beberapa Pasal di Undang-Undang Informasi dan Transaksi Elektronik. Namun dalam Undang-Undang Informasi dan Transaksi Elektronik memberikan pemahaman yang berkaitan dengan perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi. Perlindungan data pribadi dalam sebuah sistem elektronik di Undang-Undang Informasi dan Transaksi Elektronik meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh

penyelenggara sistem elektronik, dan perlindungan dari akses dan interferensi ilegal.

Perlindungan data pribadi dari penggunaan tanpa izin, Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik menyebutkan bahwa “penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan”. Dalam penjelasannya, Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik juga menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang. Sehingga penggunaan setiap data dan informasi di media elektronik yang terkait dengan data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan atau berdasarkan hukum positif (peraturan perundang-undangan).

Ketiadaan bentuk kepastian hukum yang jelas terhadap penyalahgunaan data pribadi nasabah khususnya nasabah perbankan akan berakibat terhadap keamanan keuangan yang berdampak kepada kesejahteraan masyarakat. Oleh sebab itu, perlindungan data pribadi menjadi tanggungjawab bersama, baik masyarakat, baik perorangan maupun badan hukum dan pemerintah. Karena tidaklah mungkin hanya mengandalkan sikap kehati-hatian masyarakat saja, tetapi harus ada peran pemerintah dalam membuat kebijakan hukum dengan tujuan agar dapat memberikan perlindungan kepada masyarakat. Upaya tersebut dapat melalui upaya preventif dan upaya represif. Upaya preventif dapat dilakukan dengan melalui kehati-hatian dalam memberikan data pribadi serta upaya

⁹ Aprilia, M. L., & Prasetyawati, E., (2017), *Perlindungan Hukum terhadap Data Pribadi Konsumen Pengguna Gojek*, Mimbar Keadilan, 90-105. <https://doi.org/10.30996/mk.v0i0.2202>, hlm. 93. Diakses tanggal 06 Juli 2021.

¹⁰ Natamiharja, R., & Mindoria, S., (2019), *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*. hlm. 1

pengawasan. Sedangkan upaya represif adalah memberikan suatu kepastian hukum diperlukan dan tidak dapat dikesampingkan dalam rangka penegakan hukum oleh setiap negara. Dengan adanya suatu kepastian hukum akan menetapkan dan menjamin hak tersebut dalam konstitusi dengan demikian, sudah waktunya negara Indonesia memiliki regulasi yang jelas berkaitan dengan pengaturan perlindungan hukum data pribadi seseorang.

3.2. Penyelesaian Hukum Terhadap Tindak Pidana *Skimming*

Canggihnya suatu teknologi, pelaku kejahatan siber (*cyber crime*) berevolusi menjadi berbagai jenis kejahatan baru dengan modus operandi yang baru juga. *Cybercrime* di Indonesia terutama di bidang perbankan banyak yang terjadi, misalnya pembajakan program komputer, *cracking*, penipuan penggunaan kartu kredit pihak lain secara tidak sah (*carding*), pembobolan bank (*banking fround*), pornografi, menduplikasi dan merekam data kartu ATM (*skimming* ATM), termasuk kejahatan terhadap nama domain (*domain name*).¹¹

Kasus tindak pidana *skimming* di Indonesia sering terjadi dan dunia perbankan di Indonesia memang cukup rawan menjadi sasaran aksi *skimming*. Perbuatan yang dilakukan pelaku *skimming* merupakan suatu perbuatan dengan cara mengakses komputer atau sistem elektronik milik orang lain dengan maksud untuk mengambil secara ilegal data-data pribadi yang terdapat pada komputer atau sistem elektronik tersebut.

Terhadap pihak nasabah sebagai korban tindak pidana *skimming* harus melaporkan tindak pidana tersebut kepada pihak bank dan kemudian melaporkan juga kepada pihak Kepolisian agar segera diproses melalui jalur hukum agar pelaku dapat dipidana. Tindak pidana *skimming* tersebut bisa dilakukan penangkapan atas pengaduan yang dilakukan nasabah yang mengaku uangnya di dalam rekening hilang secara tiba-tiba dan kemudian Polisi atau penyidik dapat melakukan penangkapan atas tindak pidana pencurian atau penipuan *skimming* yang dilakukan oleh pelaku kejahatan. Penyelesaian hukum yang digunakan dalam perkara tindak pidana *skimming* sudah pasti menggunakan jalur litigasi (pengadilan) sehingga pelaku kejahatan *skimming* segera dijatuhkan hukuman atas perbuatan tindak pidana penipuan yang dilakukan.

Perbuatan tindak pidana *skimming* tersebut, seseorang hanya dapat dipidana berdasarkan ketentuan Pasal 30 ayat (1) dan Pasal 46 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sehingga pelaku dapat dikenakan hukuman atas kejahatan tindak pidana *skimming*.

Tindak pidana pencurian *skimming* tersebut pada umumnya dilakukan oleh dua orang atau lebih. Dilihat dari proses pencurian *skimming* di mesin salah satu dari mereka yang memantau keadaan sekitar tempat mesin ATM, kemudian yang lain memasang alat *chip skimmer* serta kamera mini dan yang lainnya memproses atau menduplikasi data ke kartu yang kosong sehingga mereka bisa mendapatkan hasil dari pencurian tersebut sehingga

¹¹ Widodo, (2009), *Sistem Pemidanaan Dalam Cyber Crime*, Yogyakarta: Laksbang Mediatama. hlm. 29.

Pasal 363 ayat 1 ke-4 dan ke-5 bisa digunakan untuk menyerat pelaku kejahatan tindak pidana pencurian *skimming*. Dan apabila terdapat kasus tindak pidana penipuan *skimming* maka termasuk dalam Pasal 378 KUH Pidana

Penyelesaian hukum tindak pidana *skimming* dalam hukum acara pidana secara umum sama dengan penyelesaian perkara pidana lainnya, yaitu dengan adanya pelaku tindak pidana *skimming* yang tertangkap tangan dapat dilakukan pemeriksaan atas hasil laporan dan/atau pengaduan dengan ditemukan alat bukti dan barang bukti yang digunakan dalam melakukan tindak pidana. Sehingga dapat dilakukan proses peradilan di pengadilan serta diberikan hukuman yang sesuai atas perbuatan pelaku.

4. PENUTUP

4.1. Kesimpulan

Pengaturan perlindungan hukum data pribadi pada nasabah secara khusus dan komprehensif yang berkaitan dengan perbankan ataupun hal lainnya belum ada. Jika terjadi kasus, maka pengaturan hukumnya hanya akan merujuk pada undang-undang yang mengatur tentang penyalahgunaan data pribadi dan beberapa peraturan perundang-undangan lainnya, akan tetapi umumnya yang selalu dijadikan rujukan adalah Undang-Undang Informasi dan Transaksi Elektronik.

Penyelesaian hukum yang digunakan dalam perkara tindak pidana *skimming* sudah pasti menggunakan jalur litigasi (pengadilan) sehingga pelaku kejahatan *skimming* segera dijatuhkan hukuman atas perbuatan tindak pidana yang dilakukan dengan menggunakan Pasal 363 ayat 1 ke-4 dan ke-5 untuk pelaku kejahatan tindak

pidana pencurian *skimming* dan Pasal 378 KUH Pidana untuk kasus tindak pidana penipuan *skimming*.

4.2. Saran

1. Pemerintah Indonesia diharapkan untuk segera membahas Rancangan Undang-Undang Perlindungan Data Pribadi sehingga Indonesia akan lebih siap menghadapi tantangan ekonomi digital juga dapat memberikan jaminan keamanan terhadap data pribadi masyarakat serta dapat memberikan sanksi yang tegas terhadap pihak yang menyalahgunakan data pribadi pihak lain.na
2. Agar pihak Bank dan/atau pihak-pihak yang berkaitan dengan jasa perbankan agar melakukan pemeriksaan secara berkala dengan tujuan meningkatkan keamanan dan kenyamanan nasabah.

DAFTAR PUSTAKA

BUKU

- Hartono, S., (2006), *Penelitian Hukum di Indonesia Pada Abad Ke – 20*, Bandung: PT.Alumni
- Marzuki, P.M., (2005), *Penelitian Hukum*, Jakarta: Prenada Media
- Natamiharja, R., & Mindoria, S., (2019), *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*.
- Nugraha, Radian Adi, (2012), *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Universitas Indonesia
- Widodo, (2009), *Sistem Pidanaaan Dalam Cyber Crime*,

Yogyakarta: Laksbang
Mediatama

JURNAL:

- Abdul Wahid, Sunardi, dan Dwi Ari Kurniawati, 2019, “*Membumi Konstitusi Indonesia sebagai Upaya Menjaga Hak Kebhinekaan*”, *Yurispruden*, Vol. 2., No. 2
- Adi Suraji, 2019. “*Pencurian melalui Skimming*”, Universitas Gajah Mada, Jogjakarta, *Jurnal* Vol 6 No.4 .

INTERNET:

- Aprilia, M. L., & Prasetyawati, E., 2017, “*Perlindungan Hukum terhadap Data Pribadi Konsumen Pengguna Gojek*”, *Mimbar Keadilan*, 90-105. <https://doi.org/10.30996/mk.v0i0.2202>, hlm. 93. Diakses tanggal 06 Juli 2021.
- <http://kamusbahasaindonesia.org/data%20pribadi/miripKamusBahasaIndonesia.org>. Diakses 12 Juli 2021.
- Liputan6, “*Begini Cara Kerja Skimming Kartu ATM*”, diambil dari <http://www.liputan6.com/teknoread/2049670/begini-cara-kerja-iskimmingi-kartu-atm>, diakses 12 Juli 2021.
- Sony Andes., 2018., “*Pencegahan Kejahatan Skimming Perbankan*”, <https://petrominer.com/pencegahan-kejahatan-skimming-perbankan/#>, diakses pada tanggal 25 Juni 2021.