



Keamanan Data Pribadi Dalam Sistem Pembayaran Via OVO Terhadap Ancaman dan Pengelabuan (Cybercrime)

**Edy Soesanto¹, Ayu Sri Utami², Jessy Angelliza Chantica³,
Raudita Andra Nabila⁴, Tania Septfani Ricki⁵**

Universitas Bhayangkara Jakarta Raya^{1,2,3,4,5}

e-mail : edy.soesanto@dsn.ubharajaya.ac.id

Abstract

Alternative free payment methods in some of the countries mentioned There are many ways to slow the growth of cash use, especially for payments for micro-retail. One of the e-money that is currently developing in Indonesia is OVO. OVO is a type of fintech (financial technology) innovation in the payment system used in online traffic or online motorcycle taxis. OVO can be used for Grab and Tokopedia services. In addition to the online motorcycle taxi program, OVO partners with several Indonesian MSME companies. OVO can be used to pay for purchases of goods from consumers to small and medium businesses participating in cooperation. Consumers must have an OVO balance to transact or pay with this electronic money. OVO credit is obtained through the Top up system. The rapid development of OVO transactions is because many people use OVO as an electronic money payment method. This is because of the advantages offered to OVO users. According to Bothun (Bothun et al., 2013) in his research there are several advantages that can make people choose mobile payments. Users benefit from a simple payment and savings process. Because companies make emoney users offer services that are offered with coupons or discounts.

Keywords: Money, OVO, Customer.

Abstrak

Metode pembayaran gratis alternatif di beberapa negara yang disebutkan Ada banyak cara untuk memperlambat pertumbuhan penggunaan uang tunai, terutama untuk pembayaran untuk ritel mikro. Salah satu e money yang berkembang di Indonesia saat ini adalah OVO. OVO adalah salah satu jenis inovasi fintech (financial technology) dalam sistem pembayaran yang digunakan dalam lalu lintas online atau ojek online. OVO dapat digunakan untuk layanan Grab dan Tokopedia. Selain program ojek online, OVO menggandeng beberapa perusahaan UMKM Indonesia. OVO dapat digunakan untuk membayar pembelian barang dari konsumen kepada usaha kecil dan menengah peserta kerjasama. Konsumen harus memiliki saldo OVO untuk bertransaksi atau membayar dengan uang elektronik ini. Kredit OVO diperoleh melalui sistem Top up. Pesatnya perkembangan transaksi OVO dikarenakan banyak masyarakat yang menggunakan OVO sebagai metode pembayaran uang elektronik. Ini karena keuntungan yang ditawarkan kepada pengguna OVO. Menurut Bothun (Bothun et al., 2013) dalam penelitiannya terdapat beberapa keuntungan yang dapat membuat masyarakat memilih mobile payment. Pengguna mendapat manfaat dari proses pembayaran dan tabungan yang sederhana. Karena perusahaan membuat pengguna emoney menawarkan layanan yang ditawarkan dengan kupon atau diskon.

Kata kunci: e- Money, OVO, Konsumen.

PENDAHULUAN

Perkembangan teknologi dan informasi di era Revolusi 4.0 terus mengalami percepatan. Perkembangan teknologi dan informasi telah menyebabkan perubahan yang sangat pesat di berbagai bidang, baik sosial, ekonomi, pendidikan dan budaya. Hal ini didukung dengan kemudahan penggunaan teknologi dan informasi dari berbagai belahan dunia. Teknologi dan informasi ini dapat digunakan oleh siapa saja, dimana saja melalui media online. Internet adalah jaringan komunikasi elektronik yang menghubungkan jaringan komputer terorganisir di seluruh dunia melalui satelit. Saat ini, internet menjadi hal yang tidak bisa dihindari oleh masyarakat di berbagai negara khususnya di Indonesia. Masyarakat bersikap positif terhadap perkembangan internet di Indonesia.

Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia 2019 (APJII, 2019), pertumbuhan pengguna internet meningkat sangat cepat dari tahun ke tahun. Pada tahun 2015 terdapat 110,2 juta pengguna internet di Indonesia, pada tahun 2016 terdapat 132,7 juta orang, pada tahun 2017 terdapat 143,26 juta orang dan pada tahun 2018 terdapat 171,17 juta orang. pengguna internet kadang-kadang Anda dapat mengakses internet tidak hanya dari komputer atau smartphone, tetapi juga dari kedua perangkat tersebut. Beberapa tahun yang lalu, Internet hanya digunakan untuk komunikasi online dan pencarian informasi. Namun dewasa ini perkembangan penggunaan internet benar-benar tak terbendung. Di Indonesia, penggunaan internet dalam sistem pembayaran telah berkembang. Sistem pembayaran dengan menggunakan uang tunai langsung (cash) kini berkembang menjadi pembayaran tanpa uang tunai. Perkembangan ini menyebabkan sebagian masyarakat lebih memilih membayar dengan ATM, kartu kredit, cek atau uang elektronik (e-money) daripada uang tunai. Hal ini mengarah pada budaya sosial cashless yang saat ini semakin menguat, khususnya terkait produk uang elektronik (e-money).

Bank Indonesia (Bank Indonesia, 2018) menyatakan bahwa uang elektronik adalah alat pembayaran dalam bentuk elektronik yang memungkinkan uang disimpan dalam suatu media elektronik tertentu. Media elektronik yang dapat digunakan untuk menyimpan nilai uang elektronik dapat berupa chip (berbasis chip) yang bentuknya seperti kartu ATM berbasis server yaitu. aplikasi yang dapat diunduh dari PlayStore. Banyak jenis uang elektronik yang saat ini sedang dikembangkan di Indonesia. Menurut data Bank Indonesia per 27 Mei 2020, terdapat 41 jenis uang elektronik yang beredar di Indonesia berdasarkan dukungan penyelenggara jasa berizin dan sistem pembayaran (Bank Indonesia, 2020). Kita ambil contoh nama uang elektronik yang berkembang di Indonesia, OVO. OVO (PT Visionet Internasional) adalah layanan dompet elektronik dengan fungsi penyimpanan uang elektronik dan transaksi pembayaran di Indonesia. Awalnya didirikan oleh Lippo Group, OVO mulai beroperasi pada tahun 2017 dan mendapat lisensi e-money dari Bank Indonesia pada 25

September 2017 untuk beroperasi sebagai perusahaan fintech di seluruh Indonesia.

OVO merupakan salah satu jenis inovasi fintech (financial technology) dalam sistem pembayaran yang digunakan dalam lalu lintas online atau ojek online. OVO dapat digunakan untuk layanan Grab dan Tokopedia. Selain layanan aplikasi ojek online, OVO menggandeng beberapa perusahaan UMKM Indonesia. OVO dapat digunakan untuk membayar pembelian barang dari konsumen kepada usaha kecil dan menengah peserta kerjasama. Konsumen harus memiliki saldo OVO untuk bertransaksi atau membayar dengan uang elektronik ini. Kredit OVO ditentukan oleh sistem Top Up. Top up yaitu mengisi saldo OVO dengan cara membeli atau menukarkan sejumlah uang tertentu agar dapat digunakan untuk bertransaksi. Jika seseorang tidak mengisi ulang saldo OVO, mereka tidak akan dapat melakukan transaksi melalui OVO meskipun memiliki aplikasi e-money. Isi ulang OVO dapat dilakukan dengan beberapa cara, yaitu isi ulang bank, isi ulang merchant, dan isi ulang ojek online.

Pesatnya perkembangan bisnis OVO dikarenakan banyak masyarakat yang menggunakan OVO sebagai metode pembayaran uang elektronik. Ini karena keuntungan yang ditawarkan kepada pengguna OVO. Menurut Bothun (Bothun et al., 2013) dalam penelitiannya terdapat beberapa keuntungan yang dapat membuat masyarakat memilih mobile payment. Pengguna mendapat manfaat dari proses pembayaran dan tabungan yang sederhana. Karena perusahaan menawarkan pengguna uang untuk layanan yang ditawarkan dengan kupon atau diskon. OVO yang kini terintegrasi dengan sistem QRIS. QRIS (Quick Response Code Indonesia Standard) adalah standar kode QR dalam sistem pembayaran Indonesia. QRIS merupakan produk Bank Indonesia yang dikembangkan bersama Asosiasi Sistem Pembayaran Indonesia (ASPI) sehubungan dengan implementasi GPN (Gerbang Pembayaran Nasional). , yang resmi diluncurkan pada 1 Januari 2020.

Alasan pengembangan metode pembayaran QRIS adalah merchant menawarkan beberapa kode QR dari penyedia layanan pembayaran yang berbeda ketika pelanggan ingin menerima uang tanpa mengeluarkan uang, yang bertujuan untuk meningkatkan transaksi, mempercepat inklusi keuangan, meningkatkan pertumbuhan ekonomi untuk mempromosikan dan untuk Indonesia . Berdasarkan laporan tahunan BI hingga 5 November 2021, jumlah pengguna layanan QRIS meningkat menjadi 12,2 juta. Bisa dikatakan pada 22 Maret 2020, angka ini meningkat drastis menjadi 297,1%, hanya mencapai 3,08 juta pengguna, sejak 5 Maret. Per November 2021, jumlah merchant mikro yang terdaftar di QRIS adalah 7,53 juta, itu jumlah merchant yang sedikit. 3,2 juta dan 928 ribu usaha menengah.

Dilihat dari situasi saat ini, semakin banyak orang yang ingin menggunakan

sistem pembayaran QRIS dan mengikuti rencana metode pembayaran pemerintah, yang menunjukkan bahwa masyarakat sudah mulai memahami kemudahan, manfaat dan penggunaan metode pembayaran ini. Namun, dewasa ini banyak tindak pidana yang memanfaatkan perkembangan teknologi (cybercrime), misalnya. B. Meretas akun pengguna (hacking), phishing, penipuan (spoofing), dll., untuk mencuri informasi pribadi pengguna dan informasi pribadi yang terkandung di dalamnya. Informasi, kartu kredit, dan saldo rekening merupakan beberapa risiko yang dihadapi uang elektronik jika pengguna tidak hati-hati. Secara umum, data pribadi adalah informasi tentang identitas individu dan tidak boleh dibagikan. Data tersebut tidak boleh dibagikan tanpa persetujuan pemilik data, karena dapat disalahgunakan oleh orang yang tidak bertanggung jawab. Ini membuat orang mempertanyakan keamanan informasi pribadi mereka dan penuntutan kejahatan dunia maya yang merugikan masyarakat.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode deskriptif dengan penelitian kualitatif. Penelitian kualitatif adalah penelitian yang bertujuan untuk memahami suatu fenomena tentang apa yang dialami partisipan seperti perilaku, persepsi, motivasi, tindakan dan lain-lain. Dengan kata lain, penelitian kualitatif menyediakan data deskriptif dari partisipan yang relevan. Penelitian ini menggunakan metode deskriptif kualitatif dengan teknik pengumpulan data yaitu wawancara, kuesioner dan studi pustaka. Teknik pengumpulan data dilakukan dengan memberikan seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawab. Studi literatur adalah teknik pengumpulan data dengan melakukan studi telaah terhadap buku, literatur, catatan, dan laporan yang ada kaitannya dengan masalah yang sedang dipecahkan.

PEMBAHASAN

Keamanan Data

Keamanan data adalah kebijakan dan praktik yang mendukung teknologi yang melindungi data dari korupsi, pengubahan, dan pengungkapan data yang disengaja atau tidak disengaja. Lebih khusus lagi, keamanan data memungkinkan Anda mencegah akses yang tidak diinginkan ke komputer, database, atau situs web yang mencoba mengambil informasi digital pribadi. Pencurian data meluas dan memakan banyak korban. Berdasarkan data dari Cyber Insiden pencurian data meningkat setiap tahun selama lima tahun terakhir.

Pada tahun 2016 saja terdapat 20 laporan pencurian data, dan pada tahun 2020 jumlahnya meningkat menjadi 182 kasus. Oleh karena itu, penting untuk mengecek apakah layanan online yang digunakan sudah memiliki langkah pengamanan yang memadai atau belum. Keamanan data harus mencakup tiga

elemen penting termasuk kerahasiaan, integritas dan ketersediaan. Ketiga elemen ini disebut sebagai triad CIA. Dalam praktiknya, ada berbagai jenis keamanan yang dapat Anda gunakan dalam kehidupan sehari-hari, mulai dari autentikasi, tokenisasi, enkripsi, dll. Meskipun berbeda, jenis keamanan ini menawarkan manfaat yang sama dalam menjaga keamanan.

Enkripsi

Jenis keamanan data yang pertama adalah enkripsi. Jenis perlindungan ini menggunakan algoritme komputer yang membuat karakter teks tidak dapat dibaca menggunakan kunci enkripsi. Dengan kata lain, hanya beberapa orang yang berwenang yang dapat mengakses informasi yang dikandungnya.

Autentikasi

Otentikasi adalah proses memastikan identifikasi atau otentikasi. Sederhananya, autentikasi ini adalah metode keamanan yang biasanya mengidentifikasi pengguna secara akurat sebelum mengizinkan mereka mengakses informasi tersebut.

Tokenisasi

Tokenisasi adalah proses dimana informasi sensitif pemegang kartu diubah menjadi token atau kode dan bank mengubahnya kembali untuk memproses pembayaran. Dengan jenis keamanan data ini, semua informasi kartu dimiliki sepenuhnya oleh pihak bank. Oleh karena itu, informasi kartu kredit bersifat sensitif dan sangat rahasia, meskipun hanya sedikit informasi yang diketahui bank. Dengan demikian, kemungkinan kebocoran data rendah karena data tidak pernah terkirim ke pihak lain.

Kontrol akses data

Kontrol akses data (kontrol akses) adalah jenis tindakan keamanan yang membatasi akses fisik dan digital ke sistem dan informasi penting lainnya. Dalam praktiknya, kontrol akses ini membatasi pengguna yang memiliki akses ke data. Dengan demikian, jenis keamanan ini dapat mencegah pengguna atau penyusup mencoba mengakses data. Penyembunyian Data Penyembunyian data adalah konsep penting dalam pemrograman berorientasi objek. Objek kemudian menyembunyikan informasi internalnya dari kode di luar kelas tempatnya dibuat. Dengan demikian, hanya metode kelas yang dapat mengakses dan memodifikasi data internal objek.

Upaya Menjaga Keamanan Data Pelanggan

Sebagai platform pembayaran, penghargaan, dan layanan keuangan digital terkemuka di Indonesia, OVO menyadari potensi penyalahgunaan data pribadi. Sejalan dengan slogan #dataprivacymatter, OVO terus berupaya untuk memastikan dan meningkatkan keamanan data pribadi pengguna guna meningkatkan kepercayaan pelanggan untuk lebih lanjut menggunakan OVO

untuk bertransaksi. OVO selalu berusaha melindungi data pribadi seluruh penggunanya. Setiap aplikasi OVO dilengkapi dengan fitur kode keamanan dan verifikasi dua langkah setiap kali pengguna masuk ke aplikasi OVO. Selain itu, hingga saat ini, OVO telah meningkatkan langkah-langkah anti penipuan, termasuk Tim Keamanan Informasi (InfoSec) yang bertugas mencegah dan menghentikan pengungkapan informasi pribadi penggunanya. OVO juga memenuhi misinya sesuai dengan peraturan perundang-undangan yang berlaku dengan menyimpan informasi pribadi setiap pengguna di pusat data di Indonesia.

Penegakan hukum terhadap kejahatan cyber

Perkembangan ilmu pengetahuan dan teknologi saat ini tidak hanya berdampak positif, tetapi juga disalahgunakan sebagai instrumen kejahatan. Sangat penting untuk memprediksi kebijakan hukum agar kejahatan dunia maya yang muncul dapat ditindak secara pidana, dalam hal ini juga sistem penegakan hukum. Indonesia sendiri sudah memiliki regulasi kejahatan dunia maya yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, perubahan atas Undang-Undang Nomor 11 Tahun 2008. Penegakan hukum merupakan bagian dari penegakan hukum. Petugas polisi adalah petugas polisi yang berpartisipasi secara langsung atau tidak langsung dalam kegiatan kepolisian. Pada dasarnya, lembaga penegak hukum menggabungkan nilai, aturan, dan perilaku. Lembaga penegak hukum biasanya mengambil tindakan dan terus menerus berusaha untuk mencapai tujuan keadilan. Sikap anggota polisi dalam menjalankan tugasnya seringkali didasarkan pada penilaian, yang merupakan proses yang menentukan untuk mengatasi masalah yang timbul.

Penegakan hukum terhadap kejahatan cyber

Perkembangan ilmu pengetahuan dan teknologi saat ini tidak hanya berdampak positif, tetapi juga disalahgunakan sebagai instrumen kejahatan. Sangat penting untuk memprediksi kebijakan hukum agar kejahatan dunia maya yang muncul dapat ditindak secara pidana, dalam hal ini juga sistem penegakan hukum. Indonesia sendiri sudah memiliki regulasi kejahatan dunia maya yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, perubahan atas Undang-Undang Nomor 11 Tahun 2008. Penegakan hukum merupakan bagian dari penegakan hukum. Petugas polisi adalah petugas polisi yang berpartisipasi secara langsung atau tidak langsung dalam kegiatan kepolisian. Pada dasarnya, lembaga penegak hukum menggabungkan nilai, aturan, dan perilaku. Lembaga penegak hukum biasanya mengambil tindakan dan terus menerus berusaha untuk mencapai tujuan keadilan. Sikap anggota polisi dalam menjalankan tugasnya seringkali didasarkan pada penilaian, yang merupakan proses yang menentukan untuk mengatasi masalah yang timbul. Di Indonesia, lembaga penegak hukum yang menangani kasus peretasan cybercrime dibagi menjadi tiga kelompok:

Pengadilan

Peran pengadilan sebagai lembaga resmi pemerintah adalah melakukan penyidikan, memberikan keadilan melalui adjudikasi, mengambil keputusan, dan menyelesaikan pertanyaan atau masalah yang diajukan oleh masyarakat.

Kejaksaan

Kejaksaan Agung memainkan peran utama dalam penegakan hukum dalam sistem peradilan pidana Indonesia. Tentang tugasnya untuk memenuhi penegakan hukum dan sebaliknya. Kejaksaan merupakan satu-satunya lembaga yang hanya dimiliki oleh kejaksaan dan bukan lembaga penegak hukum lainnya.

Kepolisian

Dalam kasus pidana, polisi biasanya segera melakukan penyelidikan, meskipun sebelumnya tidak ada pengaduan atau pengaduan yang diajukan. Namun, ini membutuhkan pertimbangan lain sebelumnya. Tindakan penyidikan tersebut merupakan tanggung jawab kepolisian menurut Pasal 14 (1) lit.g, dimana menurut Undang-undang Hukum Acara Pidana, kepolisian berwenang untuk menyidik tindak pidana yang didahului dengan tindakan penyidikan.

Perlindungan Terhadap Keamanan Data

Data pribadi adalah data pribadi tertentu yang disimpan, dijaga dan dilindungi karena alasan kebenaran dan kerahasiaan. Perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap pengumpulan, pengumpulan, pemrosesan, analisis, penyimpanan, tampilan, pemberitahuan, transmisi, penyebaran, dan pemusnahan data pribadi. Perlindungan data pribadi dalam sistem elektronik harus didasarkan pada prinsip perlindungan data pribadi. (Kominfo 2016). Hak tersebut diatur dalam Pasal 26, yaitu:

1. Dia berhak atas perlindungan rahasia atas data pribadinya; sehubungan dengan penyelesaian sengketa data pribadi, mengajukan pengaduan kepada Menteri bahwa penyelenggara sistem elektronik tidak merahasiakan data pribadinya; Memiliki akses atau kemampuan untuk mengubah atau memperbaharui informasi pribadi tanpa mengganggu sistem pengelolaan informasi pribadi, kecuali sebagaimana diwajibkan oleh peraturan perundang-undangan; Akses atau kemungkinan memperoleh informasi historis tentang data pribadi yang disampaikan kepada penyelenggara sistem elektronik, sambil memenuhi persyaratan hukum dan meminta pemusnahan data pribadi tertentu miliknya dalam sistem elektronik yang diselenggarakan oleh penyedia layanan dilakukan. ke sistem elektronik, kecuali peraturan perundang-undangan menentukan lain.
2. Pengelola sistem elektronik wajib melakukan sertifikasi terhadap sistem elektronik yang dikelolanya, sesuai dengan ketentuan peraturan perundang-undangan

3. Menjaga kebenaran, validitas, kerahasiaan, akurasi, relevansi, dan kesesuaian pengumpulan, pengumpulan, pemrosesan, analisis, penyimpanan, tampilan, publikasi, transfer, distribusi, dan pemusnahan informasi pribadi.
4. memberitahukan secara tertulis kepada pemilik data pribadi apabila kerahasiaan data pribadi tersebut tidak dilindungi dalam sistem elektronik yang dikelolanya, Mereka memiliki aturan internal untuk perlindungan data pribadi menurut hukum.
5. Menyediakan audit trail untuk seluruh kegiatan operasional sistem elektronik yang dikelolanya.
6. memberikan pilihan kepada pemilik data pribadi mengenai data pribadi yang dikelolanya, pihak ketiga mana yang dapat menggunakan dan/atau memperlihatkan/menunjukkan/dapat memperlihatkan kepada pihak ketiga dengan seizinnya, dengan tetap terkait dengan tujuan pengumpulan dan pengumpulan data pribadi tersebut. memberikan akses kepada pemilik data pribadi atau kemampuan untuk mengubah atau memperbarui data pribadi mereka tanpa mengganggu sistem untuk mengelola data pribadi, kecuali undang-undang dan peraturan menentukan lain.
7. Pemusnahan data pribadi sesuai dengan ketentuan Keputusan Menteri
8. Ini atau ketentuan peraturan perundang-undangan lainnya yang diatur masing-masing otoritas pengawas dan regulator industri secara terpisah untuk tujuan ini.
9. menunjukkan orang penghubung yang kepadanya data pribadi dapat dengan mudah menyerahkan pemrosesan data pribadinya.

Profil Perusahaan OVO

Sejarah

OVO awalnya didirikan oleh Lippo Group sebagai aplikasi keuangan digital terintegrasi yang terintegrasi dengan beberapa perusahaan di bawah LippoX, sebuah perusahaan pembayaran digital di dalam Lippo Group. Didirikan pada tahun 2017, OVO bertujuan untuk memenuhi berbagai kebutuhan terkait pembayaran tunai dan mobile (dailysocial.id 2016) dan memperoleh lisensi e-money dari Bank Indonesia pada 25 September 2017 untuk beroperasi sebagai perusahaan fintech yang beroperasi di seluruh Indonesia. pada Desember 2017, Tokyo Century Corporation menginvestasikan sekitar \$116 juta untuk mengakuisisi 20 persen saham di startup tersebut.

Produk dan Layanan

OVO telah memperluas bisnisnya ke layanan keuangan seperti pinjaman, investasi, dan asuransi. Untuk layanan peminjaman, OVO membeli layanan P2P bernama Taralite pada 2019. Di penghujung 2020, OVO menghadirkan OVO hingga layanan pasar Suojaus yang menawarkan produk asuransi di aplikasi

OVO bekerja sama dengan mitra. Kemudian, di awal tahun 2021, OVO meluncurkan layanan OVO Invest yang berfokus pada produk investasi. OVO adalah aplikasi berbasis uang elektronik yang harus diunduh pengguna sebelum melakukan pembayaran, seperti membayar pedagang, membeli pulsa, dan mentransfer uang. Model bisnis OVO didasarkan pada tiga pilar utama: pembayaran digital, poin loyalitas, dan layanan keuangan.

Visi Misi OVO

OVO memiliki visi untuk menjadi aplikasi keuangan yang berkelanjutan dan berfokus pada misi sosial yang ingin dikembangkan OVO, OVO bertekad melalui aplikasi pembayaran yang praktis ingin mendukung program pemerintah terkait Gerakan Non Tunai (GNT).

Risk Assasment OVO

Dalam implementasinya, selain banyak aspek positif dan peluang besar untuk implementasi dan pengembangan OVO lebih lanjut, ada juga faktor risiko yang tidak boleh diabaikan dan dapat dianalisis dengan menggunakan metode berikut:

Failure Modes and Effects Analysis

FMEA atau Failure Modes and Effects Analysis (Casadai, 2007) yang dikutip oleh Nurlailah (2016) merupakan prosedur terstruktur untuk mengidentifikasi dan mencegah sebanyak mungkin mode kegagalan. Jenis kegagalan dalam konteks ini meliputi kesalahan atau cacat desain, kondisi di luar batas spesifikasi yang ditentukan atau perubahan produk yang dapat mempengaruhi pengoperasian produk. Tujuan FMEA adalah untuk menghilangkan mode kegagalan dan dengan demikian meningkatkan keandalan produk dan layanan serta meningkatkan kepuasan konsumen dengan produk atau layanan tersebut. FMEA berguna untuk mengidentifikasi cacat potensial dan dampaknya terhadap operasi produk dan untuk menentukan langkah-langkah untuk memecahkan masalah ini. Dengan bantuan FMEA, kemungkinan kesalahan dalam sistem pembayaran digital OVO dapat diidentifikasi. Potensi kerentanan sistem atau kegagalan sistem terjadi untuk mencegah risiko operasional dari kelemahan sistem dan sumber daya platform karena ketidakmampuan platform untuk menyediakan layanan yang optimal. Memberikan layanan yang kurang optimal dapat menimbulkan risiko reputasi karena aplikasi OVO diturunkan karena kegagalan sistem. Pencegahan risiko Risiko penipuan internal seperti pencucian uang atau pembobolan data, penipuan yang dapat menimbulkan risiko hukum yaitu potensi tuntutan hukum nasabah.

SWOT(Strength,Weaknesses,Opportunities,and Threats)

Analisis ini didasarkan pada asumsi bahwa strategi yang efektif akan memaksimalkan kekuatan dan peluang OVO serta meminimalkan kelemahan dan ancamannya. Diimplementasikan dengan benar, asumsi

sederhana ini dapat berdampak signifikan pada perencanaan strategis dan analisis lingkungan bisnis yang berhasil dan memberikan informasi penting untuk mengidentifikasi peluang dan ancaman dalam perusahaan. Tujuan dan strategi tersebut ditetapkan dengan tujuan memanfaatkan kekuatan internal perusahaan dan mengatasi kelemahan yang ada. Oleh karena itu, berikut adalah analisis SWOT perusahaan OVO:

1. Strength (kekuatan)

Kekuatan adalah faktor internal yang mengacu pada sumber daya, kemampuan, atau keunggulan lain dibandingkan pesaing dan tuntutan pasar yang dapat ditanggapi oleh perusahaan. Kekuatan ini memberi perusahaan keunggulan kompetitif khusus di pasar. Praktis dan simpel, pembayarannya benar dan tepat.

2. Weaknesses (kelemahan)

Membutuhkan infrastruktur teknologi, dukungan infrastruktur seperti kekuatan sinyal internet adalah kebutuhan terpenting yang mengurangi target pasar, hanya pengguna pintar yang memiliki akses Internet.

3. Opportunitties (potensi)

Bertambahnya merchant baru yang menggunakan platform digital dan kemudahan berbisnis dengan pembayaran digital menambah jumlah merchant baru.

4. Threats (Ancaman)

Keamanan pembayaran digital rentan terhadap pencurian data dan juga dapat dibobol oleh oknum yang tidak bertanggung jawab dengan menggunakan teknik seperti penipuan, phishing, dan penipuan.

Assesment Sekuriti OVO

OVO berupaya untuk mengantisipasi dan memperbarui kebutuhan pelanggan serta memberikan penyelesaian yang cepat dan tepat atas keluhan pelanggan. Misalnya contact center OVO yang selalu siap 24 jam sehari, 7 hari seminggu untuk customer support melalui berbagai saluran seperti telepon dan media sosial. dan surel. Pengalaman pelanggan yang mengutamakan kenyamanan seperti ini mungkin tampak kecil, tetapi sebenarnya mewakili nilai nyata bagi pelanggan OVO.

KESIMPULAN

Keamanan data adalah praktik dan kebijakan berbasis teknologi yang melindungi data dari kerusakan, pengubahan, dan pengungkapan data yang disengaja atau tidak disengaja. OVO sering menyarankan pengguna untuk tidak membagikan PIN/Password/OTP mereka kepada siapa pun, bahkan kepada perwakilan layanan pelanggan OVO. OVO juga merekomendasikan agar semua pengguna memperbarui atau mengubah kata sandi OVO mereka secara berkala. Sistem wajib. Indonesia sendiri sudah memiliki undang-undang kejahatan dunia maya yang diatur dalam UU No 19 tahun ini 2016 tentang

informasi dan transaksi elektronik, yaitu. H. Amandemen Perda No. 11 Tahun 2008. OVO (PT Visionet Internasional) adalah platform dompet elektronik yang memungkinkan pengguna menyimpan uang.

Memproses dan melakukan transaksi pembayaran secara elektronik di Indonesia. OVO awalnya didirikan oleh Lippo Group sebagai aplikasi keuangan digital terintegrasi yang terintegrasi dengan beberapa perusahaan di bawah LippoX, sebuah perusahaan pembayaran digital di dalam Lippo Group. Dalam hal implementasi, selain beberapa aspek positif dan peluang besar untuk implementasi dan pengembangan, OVO juga memiliki faktor risiko yang tidak boleh diabaikan dan dapat dianalisis menggunakan mode kegagalan dan analisis efektif serta metode SWOT.

Informasi pribadi pengguna, seperti nama, alamat email, nomor telepon, dan informasi keuangan, harus dilindungi dengan sangat hati-hati untuk mencegah ancaman dan penipuan (cybercrime). Anda dapat menggunakan metode berikut:

1. Mengaktifkan fitur keamanan aplikasi OVO dan tidak berbagi informasi pribadi dengan orang lain.
2. Perbarui aplikasi dan sistem operasi secara rutin, hindari mengakses OVO melalui jaringan Wi-Fi publik.
3. Menggunakan kata sandi yang kuat dan berbeda pada Aplikasi.
4. Mempelajari jenis kemungkinan kejahatan dunia maya (cybercrime)

DAFTAR PUSTAKA

- Alijoyo, Antonius. (2016) *Failure Mode Effect Analysis* Teknik Penilaian Risiko Berbasis Iso 31010 Analisis Modus Kegagalan Dan Dampak (CSRM: Jakarta)
- Arisandy, Yogi Oktafian (2020) Penegakan Hukum Terhadap Cyber Crime Hacker Indonesian, *Journal Of Criminal Law And Criminology (IJCLC)* 1(2), , 162-169.
- Astuti, Anissa Mayang, Indri Shinta Ratnawati, (2020). Analisis SWOT Dalam Menentukan Strategi Pemasaran, *Jurnal Ilmu Manajemen*, 17, (2).
- Badariah. Nurlailah,, Dedy Sugiarto , Chani Anugerah, (2016), Penerapan Metode Failure Mode And Effect Analysis (FMEA) Dan Expert System (SISTEM PAKAR), *Seminar Nasional Sains Dan Teknologi Fakultas Teknik Universitas Muhammadiyah Jakarta*
- Bank Indonesia (2020) Apa Itu Uang Elektronik diakses 20 Maret 2023 pada <https://www.bi.go.id/id/edukasi/pages/apa-itu-uang-elektronik.aspx>

Fernando, Roki Iwan Krisnadi, (2020) Analisis Fungsi Pembayaran Digital Saat Masa Pandemi Covid-19 Di Indonesia, *Jurnal Magister Manajemen Telekomunikasi, Universitas Indonesia*

Kominfo, (2016) Indonesia Sudah Memiliki Aturan Soal Perlindungan Data Pribadi diakses 31 Maret 2023 pada https://www.kominfo.go.id/content/detail/8621/Indonesia-Sudah-Miliki-Aturan-Soal-Perlindungan-Data-Pribadi/0/Sorotan_Media

Nababan, Roida, Nelson Persada Sinaga, (2021) Perlindungan Hukum Bagi Konsumen Yang Data Pribadinya Diperjual Belikan Di Aplikasi Fintech Peer-Topeer Lending, *Jurnal Magister Hukum Program Pascasarjana Universitas HKBP Nommensen* 02 (02) 156-167

Randi Eka (2016), OVO Dan Evolusi Layanan Pembayaran Mobile Diakses 31 Maret 2023 Dari <https://dailysocial.id/post/ovo-dan-evolusi-layanan-pembayaran-mobile>

Riyanti Teresa Tedja (2019), Risiko Penggunaan Fintech diakses pada 31 Maret 2023 pada <https://sis.binus.ac.id/2019/10/19/risiko-penggunaan-fintech/>

Safitri, Rizka, Miftah Andriansyah. (2020) Analisis Penerimaan Teknologi Keuangan (Fintech) Terhadap Penggunaan Aplikasi Fintech OVO, *JMM Online* 4(4) 542

Septiana Ayu Estri Maharani (2019) Profil Digital Payment Di Indonesia Peluang Dan Resiko diakses pada 31 Maret 2023 http://repository.unisba.ac.id/bitstream/handle/123456789/26753/Fulltext_Ppr_Mahani_Oin_2019-2.Pdf?Sequence=1&Isallowed=Y

Universitas Stekom Pusat (2022), OVO (Pembayaran), Diakses 31 Maret 2023 Dari [https://p2k.stekom.ac.id/ensiklopedia/ovo_\(pembayaran\)](https://p2k.stekom.ac.id/ensiklopedia/ovo_(pembayaran)).