



Hubungan Antara Kesadaran Privasi Data Pribadi dan Penggunaan Layanan PayLater di Kalangan Pengguna E-commerce di Indonesia

M Sahlan

Universitas Islam Negeri Sumatera Utara Medan

Muhammad Irwan Padli Nasution

Fakultas Ekonomi dan Bisnis Islam UINSU

Korespondensi penulis: msahlan419@gmail.com

Abstract Pay later, atau metode pembayaran di kemudian hari, semakin populer di berbagai platform pembayaran. Dengan sistem ini, konsumen dapat membeli barang atau jasa tanpa membayar langsung, melainkan diberi jangka waktu tertentu untuk melakukan pembayaran. Namun, perkembangan ini juga menimbulkan kekhawatiran mengenai keamanan dan penggunaannya. Teknologi informasi dan komunikasi berperan penting dalam kehidupan sehari-hari. Tantangan utama dalam menjaga privasi data mencakup perlindungan terhadap pelanggaran data, penyalahgunaan data oleh pihak ketiga, dan kurangnya transparansi dalam pengelolaan data. Selain itu, perlu adanya penguatan regulasi dan kebijakan privasi data baik di tingkat lokal maupun global. Privasi data dan penggunaan pay later adalah dua aspek penting dalam ekosistem digital saat ini. Penggunaan pay later mengalami pertumbuhan pesat di berbagai platform pembayaran, mengubah cara konsumen berbelanja dan bertransaksi secara online. Namun, pertumbuhan ini juga membawa kekhawatiran tentang keamanan data pribadi konsumen. Oleh karena itu, artikel ini menekankan pentingnya mempertimbangkan keamanan privasi data dalam pengembangan dan penerapan model pembayaran pay later.
Kata kunci : Pay later, Privasi data, Keamanan data, Transparansi pengelolaan data, Platform pembayaran.

Abstrak Bayar nanti, atau metode pembayaran di kemudian hari, semakin populer di berbagai platform pembayaran. Dengan sistem ini, konsumen dapat membeli barang atau jasa tanpa membayar langsung, melainkan diberi jangka waktu tertentu untuk melakukan pembayaran. Namun perkembangan ini juga menimbulkan kekhawatiran mengenai keamanan dan kegunaan. Teknologi informasi dan komunikasi berperan penting dalam kehidupan sehari-hari. Tantangan utama dalam menjaga privasi data mencakup perlindungan terhadap pelanggaran data, perlindungan data oleh pihak ketiga, dan tidak mengizinkan transparansi dalam pengelolaan data. Selain itu, perlu adanya regulasi dan kebijakan privasi data baik di tingkat lokal maupun global. Perlindungan data dan penggunaan pembayaran nanti adalah dua aspek penting dalam ekosistem digital saat ini. Penggunaan pay later mengalami pertumbuhan pesat di berbagai platform pembayaran, mengubah cara berbelanja konsumen dan bertransaksi secara online. Namun, pertumbuhan ini juga membawa kekhawatiran tentang keamanan data pribadi konsumen. Oleh karena itu, artikel ini menekankan pentingnya mempertimbangkan keamanan privasi data dalam pengembangan dan penerapan model pembayaran paylater.
Kata kunci : Bayar nanti, Privasi data, Keamanan data, Transparansi pengelolaan data, Platform pembayaran.

PENDAHULUAN

Privasi data adalah hak seseorang untuk mengontrol dan menjaga keamanan data pribadi mereka. Data pribadi mencakup informasi seperti nama, alamat, nomor telepon, email, dan riwayat transaksi. Privasi data menjadi sangat penting di era digital karena data pribadi bisa disalahgunakan oleh pihak lain tanpa izin, mengganggu privasi individu, atau bahkan digunakan untuk tujuan yang tidak sah. Oleh karena itu, perlindungan data pribadi sangat penting untuk menjaga hak privasi individu dan mencegah penyalahgunaan data. Menurut Meutia (2015), privasi adalah hak kebebasan dalam melakukan sesuatu tanpa

gangguan, seperti pemantauan atau mata-mata. Privasi mencakup tiga aspek utama: perlindungan data, lokasi, dan identitas. Namun, seringkali orang mengabaikan privasi individu, terutama jika mereka sudah sangat akrab satu sama lain.

PayLater adalah layanan sepenuhnya digital yang berbeda dengan kartu kredit, yang memerlukan kartu fisik. Untuk mendapatkan kartu kredit, seseorang harus mengajukan permohonan di bank, sedangkan layanan PayLater dapat diaktifkan secara online. Batas transaksi layanan keuangan digital ini biasanya lebih rendah dibandingkan kartu kredit, seringkali hanya mencapai jutaan rupiah. Kartu kredit dapat digunakan untuk transaksi online maupun offline di berbagai tempat.

Sementara itu, PayLater hanya dapat digunakan pada aplikasi tertentu. Untuk menjaga privasi dan etika dalam manajemen SDM digital, organisasi perlu memiliki kebijakan dan prosedur yang jelas. Penggunaan data harus sesuai dengan peraturan privasi yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi. Selain itu, pelatihan dan peningkatan kesadaran karyawan mengenai privasi dan etika digital sangat penting untuk mencegah pelanggaran dan mendorong budaya kerja yang adil dan bertanggung jawab. Era digital juga membawa banyak perubahan dalam kehidupan manusia, terutama di bidang pendidikan (Amalia, SZ, 2019). Berikut beberapa strategi untuk mengelola identitas digital dan informasi pribadi dengan aman:

1. Gunakan sandi yang kuat dan kompleks untuk akun Anda. Hindari menggunakan informasi pribadi seperti tanggal lahir atau nama hewan peliharaan sebagai sandi, dan ubah sandi secara berkala.
2. Batasi akses ke data pribadi. Berikan izin akses hanya pada aplikasi dan situs yang benar-benar diperlukan. Hindari berbagi informasi pribadi secara luas di media sosial.
3. Aktifkan autentikasi dua faktor untuk akun-akun penting, yang memerlukan dua langkah verifikasi seperti kode yang dikirim ke ponsel saat login.
4. Lakukan backup data penting dan rahasia secara berkala untuk menghindari kehilangan data akibat kehilangan perangkat atau serangan siber. Gunakan penyimpanan cloud atau external drive.
5. Instal software anti-virus dan firewall terbaru, serta atur pembaruan otomatis untuk mendapatkan perlindungan terkini dari ancaman digital.
6. Berhati-hatilah terhadap phishing dan penipuan online lainnya. Hindari mengklik tautan mencurigakan atau membuka lampiran email dari sumber yang tidak dikenal.
7. Baca syarat dan ketentuan penggunaan situs sebelum mendaftar, dan berikan persetujuan yang bijak terkait penggunaan dan berbagi data pribadi.

8. Laporkan pelanggaran privasi dan kecurigaan kepada pihak berwenang yang terkait. Jangan diam saja dan ambil tindakan jika informasi pribadi Anda bocor atau disalahgunakan.

Berikut adalah beberapa strategi dasar untuk mengelola identitas digital dan informasi pribadi dengan aman dan bijak di era digital. Dengan disiplin menerapkan strategi-strategi ini, berbagai risiko terhadap privasi data dan keamanan siber dapat dihindari. Jika terjadi pelanggaran privasi data karyawan, perusahaan dapat menghadapi beberapa konsekuensi yang signifikan. Berikut adalah beberapa contoh:

1. Kerusakan Reputasi, Pelanggaran privasi data karyawan dapat merusak reputasi perusahaan, yang berdampak pada menurunnya kepercayaan pelanggan dan karyawan. Hal ini dapat mengakibatkan penurunan penjualan dan pendapatan.
2. Biaya Hukum, Perusahaan mungkin harus menghadapi biaya hukum yang signifikan jika karyawan mengajukan gugatan akibat pelanggaran privasi data. Biaya ini bisa meliputi biaya pengacara, biaya peralatan, dan biaya terkait lainnya.
3. Kerugian Karyawan: Pelanggaran privasi data dapat menyebabkan karyawan mengalami kerugian finansial, reputasi, atau bahkan psikologis. Perusahaan mungkin perlu memberikan kompensasi kepada karyawan yang terkena dampak.
4. Kerugian Bisnis, Pelanggaran privasi data karyawan dapat menyebabkan penurunan kepercayaan pelanggan, penurunan penjualan, atau bahkan penutupan bisnis.
5. Kerugian Reputasi Karyawan, Pelanggaran privasi data karyawan juga dapat merusak reputasi karyawan, yang dapat menyulitkan mereka dalam mencari pekerjaan di masa depan.
6. Biaya Pengawasan, Perusahaan mungkin perlu meningkatkan biaya pengawasan dan perlindungan data karyawan untuk mencegah insiden serupa di masa depan.
7. Penurunan Kualitas Karyawan, Pelanggaran privasi data karyawan dapat menurunkan kualitas karyawan, yang berdampak pada produktivitas dan efisiensi perusahaan.
8. Kerugian Kepemilikan, Pelanggaran privasi data karyawan dapat mengakibatkan kerugian kepemilikan perusahaan, seperti penurunan nilai perusahaan atau kerugian finansial.
9. Kerugian Kepastian, Pelanggaran privasi data karyawan dapat menyebabkan kerugian dalam hal keamanan data dan keamanan karyawan.
10. Kerugian Kepemimpinan, Pelanggaran privasi data karyawan dapat merusak kepercayaan karyawan dan pelanggan terhadap kepemimpinan perusahaan.

Berikut adalah beberapa contoh layanan PayLater yang sering digunakan oleh masyarakat umum:

1. Shopee PayLater

Jika kamu sering berbelanja di Shopee, pasti sudah familiar dengan fitur Shopee PayLater atau SPayLater. Shopee sering memberikan diskon besar bagi pengguna yang mengaktifkan dan bertransaksi menggunakan SPayLater. Pengguna juga bisa memilih tenor cicilan sesuai kemampuan mereka.

2. Gopay PayLater

Ingin pesan GoFood atau Gojek tapi belum gajian? Kamu bisa memanfaatkan fitur PayLater dari Gopay. Seperti fitur PayLater di aplikasi lainnya, pengguna harus melakukan aktivasi dan verifikasi data diri terlebih dahulu. Fitur Gopay PayLater ini bisa digunakan untuk semua layanan Gojek.

3. Traveloka PayLater

Sekarang, tidak hanya pembelian barang yang bisa dilakukan secara kredit, tetapi juga liburan. Kamu bisa menggunakan berbagai fitur di Traveloka dan membayarnya nanti. Mulai dari pemesanan tiket pesawat, kereta, bis, akomodasi, hingga atraksi hiburan.

4. Ovo PayLater

Sebagai aplikasi dompet digital, Ovo juga menyediakan metode pembayaran kredit. Tokopedia memudahkan transaksi penggunanya dengan berkolaborasi dengan Ovo, memungkinkan pengguna untuk bertransaksi di Tokopedia menggunakan Ovo PayLater.

5. Kredivo PayLater

Kredivo juga menyediakan fitur PayLater bagi penggunanya. Salah satu kelebihan fitur ini adalah dapat digunakan di berbagai platform yang bekerja sama dengan Kredivo, seperti Bukalapak, Lazada, dan Blibli.

Dalam beberapa kasus, perusahaan dapat menghadapi konsekuensi serius seperti tindakan hukum atau biaya besar untuk menangani insiden pencemaran privasi data karyawan. Oleh karena itu, perusahaan harus memastikan bahwa mereka memiliki sistem perlindungan data yang efektif dan mematuhi peraturan yang relevan untuk mencegah insiden serupa di masa depan.

Dalam era digital yang berkembang pesat, e-commerce telah menjadi metode transaksi yang populer bagi pelaku bisnis. Teknologi e-commerce memungkinkan pelaku bisnis untuk berhubungan dengan konsumen tanpa harus berinteraksi langsung, memperluas jaringan pemasaran mereka. Namun, pertumbuhan e-commerce juga membawa masalah kebocoran data pribadi yang perlu diperhatikan, yang sayangnya sering diabaikan oleh beberapa pihak.

Shopee adalah salah satu platform e-commerce yang sangat digunakan di Indonesia. Menurut survei data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2019 – 2020, Shopee menduduki peringkat pertama dalam penggunaan e-

commerce oleh masyarakat, dengan persentase 27,4%. Menurut databoks.katadata.co.id (2021), Shopee dan Tokopedia (Gopay) paylater adalah dua layanan paylater yang paling sering digunakan pada tahun 2021. Shopee paylater menjadi aplikasi yang paling populer di Indonesia pada tahun 2021, dengan 78,4% pengguna. Tokopedia (Gopay) berada di peringkat kedua dengan 33,8% pengguna, dan di peringkat ketiga ada Kredivo dengan 23,2% pengguna yang menggunakan fitur paylater.

Di balik kemudahan yang ditawarkan, layanan digital seperti PayLater juga membawa risiko terhadap kebocoran data pribadi. Mengingat tingginya penggunaan layanan PayLater dan pentingnya privasi data, perlu dipahami bagaimana kesadaran privasi data pribadi berhubungan dengan penggunaan layanan PayLater. Pemahaman ini penting untuk meningkatkan perlindungan privasi dan mengurangi risiko penyalahgunaan data pribadi.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kuantitatif dengan pendekatan korelasional, artinya penelitian menggunakan sebuah metode penelitian yang bertujuan untuk memahami hubungan antara dua variabel atau lebih. Menurut Gay dalam Emzir (2009:38) Penelitian korelasional ialah penelitian yang berusaha menafsirkan hubungan antar variabel. Penelitian korelasional umumnya digunakan pada bidang sosial, ekonomi, juga pendidikan. Menurut Suharsimi (2010:313), mengutarakan jika penelitian korelasi adalah penelitian yang bertujuan untuk menemukan ada atau tidak hubungan dan apabila ada, berapa eratnya hubungan tersebut, serta berarti atau tidak hubungan itu. Pendekatan ini bertujuan untuk mengeksplorasi dan memahami hubungan antara variabel kesadaran privasi data pribadi dan penggunaan layanan PayLater di kalangan pengguna e-commerce di Indonesia. Desain korelasional dipilih karena sesuai untuk mengidentifikasi tingkat hubungan atau asosiasi antara dua variabel atau lebih tanpa berusaha menentukan hubungan sebab-akibat. Penelitian korelasional membantu kita memahami apakah dan bagaimana dua hal berhubungan. Meskipun tidak bisa memastikan sebab-akibat, penelitian ini memberikan informasi penting yang bisa digunakan untuk penelitian lebih lanjut atau keputusan berdasarkan data.

HASIL DAN PEMBAHASAN

Hasil yang di dapatkan dapat di jabarkan ialah, Penggunaan paylater semakin populer, hal ini juga menimbulkan kekhawatiran terkait keamanan dan privasi data pribadi konsumen. Adapun tantangan utama mencakup:

- Penyalahgunaan data oleh pihak-pihak yang tidak berwenang dapat menimbulkan dampak negatif bagi konsumen.
- Penyalahgunaan data oleh pihak ketiga dapat merugikan konsumen, seperti pencurian identitas, penipuan, atau penggunaan data untuk kepentingan pribadi.
- Kurangnya transparansi dari penyedia layanan paylater dalam menjelaskan bagaimana data pribadi konsumen akan dikelola dan dijaga keamanannya.

Penggunaan layanan pembayaran digital seperti PayLater telah menjadi semakin populer di kalangan konsumen e-commerce di Indonesia. Layanan ini menawarkan kemudahan dan fleksibilitas dalam berbelanja, karena konsumen dapat membeli barang sekarang dan membayar nanti. Namun, meskipun memiliki banyak manfaat, penggunaan layanan PayLater juga membawa tantangan signifikan terkait keamanan dan privasi data pribadi konsumen. Salah satu isu utama yang muncul adalah perlindungan terhadap pelanggaran data. Dalam menggunakan layanan PayLater, konsumen harus mempercayakan data pribadi mereka kepada penyedia layanan. Data ini mencakup informasi identitas seperti nama, alamat, dan nomor telepon, serta riwayat pembayaran dan preferensi belanja mereka. Kepercayaan ini membawa risiko serius jika terjadi kebocoran atau pelanggaran data. Kebocoran data dapat menyebabkan masalah serius seperti pencurian identitas, di mana pihak yang tidak berwenang dapat menggunakan informasi pribadi konsumen untuk melakukan penipuan atau kejahatan lainnya. Selain itu, data yang bocor juga dapat digunakan untuk tujuan yang merugikan konsumen, seperti spam atau phishing.

Selain risiko kebocoran data, terdapat juga kekhawatiran akan penyalahgunaan data oleh pihak ketiga yang tidak memiliki wewenang untuk mengakses dan memanfaatkan informasi konsumen. Data pribadi konsumen bisa dieksploitasi oleh pihak ketiga untuk berbagai tujuan yang tidak sesuai dengan kepentingan konsumen, seperti pemasaran yang agresif, di mana konsumen dibanjiri dengan iklan yang tidak diinginkan, atau bahkan dijual ke pihak lain tanpa persetujuan konsumen. Penyalahgunaan data ini dapat mengakibatkan konsumen merasa terganggu dan kehilangan kepercayaan terhadap layanan yang mereka gunakan.

Masalah lain yang menjadi perhatian adalah kurangnya transparansi dari penyedia layanan PayLater dalam mengelola data konsumen. Konsumen seringkali tidak memiliki informasi yang jelas dan rinci mengenai bagaimana data pribadi mereka akan digunakan, disimpan, dan dilindungi oleh penyedia layanan. Kurangnya transparansi ini dapat menimbulkan kebingungan di kalangan konsumen, yang pada akhirnya dapat menyebabkan ketidakpercayaan. Tanpa pemahaman yang jelas tentang bagaimana data mereka diperlakukan, konsumen mungkin merasa tidak aman dan enggan menggunakan layanan PayLater, meskipun mereka mungkin tertarik pada manfaat yang ditawarkannya.

Untuk mengatasi tantangan-tantangan tersebut, diperlukan upaya yang komprehensif dari penyedia layanan PayLater untuk memastikan keamanan dan privasi data konsumen. Pertama, penyedia layanan harus menerapkan standar keamanan yang ketat dalam pengelolaan data. Ini mencakup adopsi teknologi keamanan terkini yang dapat melindungi data konsumen dari ancaman cyber dan pelanggaran data. Selain teknologi, prosedur dan kebijakan keamanan yang ketat juga harus diterapkan untuk memastikan bahwa data pribadi konsumen dilindungi dengan baik.

Transparansi juga menjadi kunci dalam mengatasi kekhawatiran konsumen. Penyedia layanan harus menyediakan kebijakan privasi yang jelas dan mudah dipahami oleh konsumen, menjelaskan bagaimana data pribadi mereka akan digunakan, disimpan, dan dilindungi. Informasi yang transparan ini harus dikomunikasikan secara proaktif kepada konsumen, termasuk setiap perubahan yang terjadi dalam kebijakan privasi dan pengelolaan data. Dengan demikian, konsumen dapat merasa lebih aman dan percaya bahwa data mereka dikelola dengan cara yang bertanggung jawab.

Selain itu, edukasi dan pemberian kontrol yang memadai kepada konsumen atas data mereka sangat penting. Penyedia layanan harus memberikan edukasi kepada konsumen mengenai pentingnya privasi data dan cara melindungi informasi pribadi mereka. Konsumen juga harus diberikan kontrol yang memadai atas data mereka, termasuk opsi untuk mengakses, mengubah, dan menghapus data pribadi mereka jika diperlukan. Dengan memberikan kontrol ini, konsumen dapat merasa lebih berdaya dan memiliki keyakinan bahwa mereka memiliki kendali atas informasi pribadi mereka.

KESIMPULAN

Penelitian ini menemukan hubungan negatif yang signifikan antara kesadaran privasi data pribadi dan penggunaan layanan PayLater di kalangan pengguna e-commerce di Indonesia. Temuan ini menunjukkan bahwa privasi data adalah faktor penting yang mempengaruhi keputusan pengguna dalam memanfaatkan layanan digital. Penyedia layanan perlu meningkatkan upaya perlindungan data untuk membangun kepercayaan di kalangan pengguna yang sadar privasi.

Penggunaan layanan pembayaran digital seperti PayLater di kalangan konsumen e-commerce di Indonesia menunjukkan tren yang terus meningkat karena menawarkan kemudahan dan fleksibilitas dalam berbelanja. Namun, popularitas layanan ini juga membawa tantangan signifikan terkait dengan keamanan dan privasi data pribadi konsumen. Konsumen yang menggunakan PayLater harus mempercayakan data pribadi mereka, termasuk informasi identitas, riwayat pembayaran, dan preferensi belanja, kepada penyedia layanan. Risiko kebocoran data dapat mengakibatkan pencurian identitas, penipuan, dan

penggunaan data untuk kepentingan yang merugikan konsumen. Selain itu, penyalahgunaan data oleh pihak ketiga yang tidak berwenang dapat menyebabkan pemasaran yang agresif, penjualan data, atau aktivitas ilegal lainnya.

Kurangnya transparansi dari penyedia layanan dalam pengelolaan data konsumen menambah kekhawatiran ini. Konsumen sering tidak mendapatkan informasi yang jelas mengenai bagaimana data pribadi mereka akan digunakan, disimpan, dan dilindungi, yang menyebabkan kebingungan dan ketidakpercayaan. Untuk mengatasi tantangan ini, penyedia layanan PayLater perlu mengadopsi pendekatan yang komprehensif dalam melindungi keamanan dan privasi data konsumen. Langkah-langkah ini mencakup penerapan standar keamanan yang ketat, meningkatkan transparansi dalam pengelolaan data, serta memberikan edukasi dan kontrol yang memadai kepada konsumen atas data pribadi mereka.

Dengan memperhatikan isu-isu privasi dan keamanan data ini, penyedia layanan PayLater dapat membangun kepercayaan konsumen, memastikan perlindungan data yang efektif, dan mendukung adopsi layanan yang lebih luas dan berkelanjutan di kalangan konsumen e-commerce di Indonesia. Keberhasilan dalam mengatasi tantangan ini akan memungkinkan layanan PayLater untuk terus berkembang dan memberikan manfaat maksimal bagi konsumen dan penyedia layanan.

DAFTAR PUSTAKA

- Amalia, S. Z. (2019). Implementasi manajemen sumber daya manusia di era digital: Studi kasus di MTs Nurul Jadid. Al-Idarah. Jurnal Kependidikan Islam. Vol 9. No 1.
- Rabbani, A., Noormansyah, N., Zufira, R.A., Firdaus, F.P., & Rakhmawati, N.A. (2020). Studi Empiris Peraturan Daerah Mengenai Cctv Terkait Privasi Data Di Kota-Kota Jawa Timur. Vol 17. No 1
- S. W. Putra, "Aspek Cybercrime dalam Paylater," vol. 4, pp. 1–22, Mar. 2021.
- I. Saputra, G. M. A. Sasmita, and A. Wiranatha, "Pengembangan Sistem Keamanan untuk ECommerce," Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi), vol. 5, no. 1, p. 17, 2017.
- Nanang Widayanto, dkk, Maret 2022. Analisis Keamanan Data Pribadi pada Shopee Paylater Menggunakan Metode Hybrid
- Khairina F. Hidayati, Sep 2023. PayLater: Definisi, Contoh, dan Tips Bijak Menggunakannya (<https://glints.com/id/lowongan/paylater/>)
- Raynaldi Fatih Amanullah, dkk. Maret 2019. Pengamanan Pesan Menggunakan Kombinasi Metode Kriptografi Rsa, Vigenere Cipher, Dan Hill Cipher Dengan Metode Steganografi Least Significant Bit
- Tia Deja Pohan, Muhammad Irwan Padli Nasution. Sep 2023. Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce