

Online Consumer Behavior: Disclosure of Sensitive Customer Data in the Travel App Ecosystem

Online Consumer Behaviour: Pengungkapan Data Sensitif Pelanggan dalam Ekosistem Aplikasi Perjalanan

Harmi Widiana¹, Imanuella R. Andilolo², Sulaimiah³

Program Studi Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Mataram
¹hwidiana@unram.ac.id, ²irandilolo@unram.ac.id, ³sulaimiahmia65@gmail.com

Abstract

Background: In the digital age, various online platforms require users to provide personal data to provide personalised services. This change raises concerns about data privacy and security risks, especially since consumers often have difficulty understanding how their data is collected, stored, and used by service providers. **Purpose:** This study examines the impact of technical familiarity and trust on individuals' willingness to disclose sensitive data (health-related data, ethnicity data, and sexual orientation data) to Online travel agencies. **Methodology:** The research adopts a quantitative approach, surveying participants to assess their level of privacy literacy and its effect on their data-sharing intentions. **Findings:** Results indicate that individuals with higher technical familiarity are more cautious about sharing sensitive information, suggesting that privacy awareness plays a critical role in shaping user behaviour. Similarly, trust in digital platforms, where higher trust increases users' willingness to disclose data despite privacy concerns. **Implications:** These findings have practical implications for policymakers, healthcare providers, and digital platform developers in promoting safe and responsible data-sharing practices. **Originality:** This study emphasises the need for public education initiatives to improve privacy literacy and calls for transparent data governance policies to foster trust in the digital health ecosystem. **Keywords:** OTA, E-Commerce, Privacy, Behaviour.

Abstrak

Latar Belakang: Di era digital, berbagai platform online mengharuskan pengguna untuk memberikan data pribadi untuk memberikan layanan yang dipersonalisasi. Perubahan ini menimbulkan kekhawatiran tentang privasi data dan risiko keamanan, terutama karena konsumen sering kali mengalami kesulitan memahami bagaimana data mereka dikumpulkan, disimpan, dan digunakan oleh penyedia layanan. **Tujuan:** Penelitian ini mengkaji dampak literasi privasi online, khususnya keakraban teknis dan kepercayaan terhadap kemauan individu untuk mengungkapkan informasi sensitif (Data kesehatan, data etnis, data orientasi seksual) pada aplikasi perjalanan online. **Metodologi:** Penelitian ini menggunakan pendekatan kuantitatif, dengan mensurvei partisipan untuk menilai tingkat keakraban teknis mereka dan kepercayaan serta pengaruhnya terhadap niat berbagi data sensitif mereka. **Temuan:** Hasil penelitian menunjukkan bahwa individu dengan keakraban teknis yang lebih tinggi lebih berhati-hati dalam berbagi informasi, yang menunjukkan bahwa kesadaran privasi memainkan peran penting dalam membentuk perilaku pengguna. Begitu pula dengan kepercayaan pada platform digital, di mana kepercayaan yang lebih tinggi meningkatkan kemauan pengguna untuk mengungkapkan data meskipun ada masalah privasi. **Implikasi:** Temuan ini memiliki implikasi praktis bagi para pembuat kebijakan, penyedia layanan kesehatan, dan pengembang platform digital dalam mempromosikan praktik berbagi data yang aman dan bertanggung jawab. **Orisinalitas:** Studi ini menekankan perlunya inisiatif pendidikan publik untuk meningkatkan literasi privasi dan menyerukan kebijakan tata kelola data yang transparan untuk menumbuhkan kepercayaan dalam ekosistem kesehatan digital.

Kata Kunci: OTA, E-Commerce, Privacy, Behaviour.

1. Pendahuluan

Di era digital, kemampuan untuk melindungi informasi pribadi menjadi semakin penting, terutama saat konsumen menggunakan layanan daring. Agen perjalanan

daring (*Online Travel Agency* - OTA) mengharuskan pengguna untuk memberikan data sensitif, seperti detail paspor, informasi kartu kredit, dan preferensi pribadi, untuk memberikan layanan yang dipersonalisasi. Perubahan ini telah menimbulkan kekhawatiran tentang privasi data dan risiko keamanan. Di lain pihak, kemauan untuk mengungkapkan data tersebut sering kali bergantung pada pemahaman individu tentang privasi daring. Dalam konteks ini, literasi privasi daring, khususnya pemahaman teknis, memainkan peran penting dalam membentuk sikap dan perilaku pengguna. Konsumen dengan tingkat literasi yang lebih tinggi diharapkan menunjukkan kehati-hatian yang lebih tinggi saat membagikan data sensitif, sehingga mengurangi paradoks privasi, dimana individu mengungkapkan kekhawatiran privasi tetapi mengungkapkan informasi pribadi demi kenyamanan (Masur, 2020; Okditazeini & Irwansyah, 2018; Williams & Nurse, 2016)

Meskipun OTA menawarkan kemudahan dan pengalaman yang disesuaikan, OTA juga menimbulkan kekhawatiran tentang keamanan dan penggunaan data pribadi. Konsumen harus mempertimbangkan manfaat personalisasi dan pemesanan yang lancar dengan risiko penyalahgunaan data, penipuan, dan pelanggaran privasi. Kompromi ini menciptakan proses pengambilan keputusan yang rumit, terutama saat individu tidak yakin tentang bagaimana data mereka akan digunakan atau dilindungi. Konsumen sering menerima diskon atau penawaran yang dipersonalisasi sebagai ganti data mereka tanpa sepenuhnya memahami risiko yang terlibat, sehingga menimbulkan pertanyaan kritis tentang efektivitas upaya literasi dan edukasi privasi (Sindermann et al., 2021). Namun, pemahaman tentang bagaimana literasi privasi daring memengaruhi keputusan ini masih terbatas—apakah peningkatan literasi memberdayakan konsumen untuk membuat pilihan yang lebih tepat atau sekadar menambah konflik internal mereka. Meskipun pemerintah berupaya untuk memperkuat kebijakan perlindungan data, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) Indonesia, asimetri informasi tetap ada antara penyedia layanan dan pengguna, yang berkontribusi pada praktik privasi yang buruk (Budiutono, 2023).

Mengingat pesatnya pertumbuhan industri perjalanan dan meningkatnya ketergantungan pada OTA, memahami dampak literasi privasi sangatlah penting. Studi ini bertujuan untuk mengeksplorasi bagaimana berbagai tingkat literasi privasi daring memengaruhi keinginan pengguna untuk mengungkapkan data sensitif saat memesan layanan melalui OTA. Secara khusus, penelitian ini akan memeriksa apakah tingkat literasi yang lebih tinggi menghasilkan perilaku berbagi data yang lebih hati-hati atau apakah konsumen masih cenderung mengungkapkan informasi sensitif demi nilai yang ditawarkan oleh OTA, seperti diskon atau layanan yang ditingkatkan.

Penelitian ini bertujuan untuk mengeksplorasi bagaimana literasi privasi daring dan kepercayaan memengaruhi keinginan konsumen Indonesia untuk mengungkapkan data sensitif kepada OTA. Dengan menyelidiki hubungan antara literasi privasi dan kepercayaan terkait perilaku pengungkapan data, penelitian ini berkontribusi pada pengetahuan baru tentang literasi privasi dan perilaku berbagi data dan menyoroti pentingnya menumbuhkan kesadaran privasi di dunia yang semakin saling terhubung.

2. Tinjauan Pustaka

Technical Familiarity Pada Platform Online

Literasi Privasi Daring (Online Privacy Literacy/OPL) merujuk pada pemahaman dan kesadaran individu mengenai bagaimana informasi pribadi mereka dikumpulkan, digunakan, dan dibagikan dalam lingkungan digital, serta kemampuan mereka dalam mengelola risiko privasi yang mungkin timbul (Bartsch & Dienlin, 2016; Trepte et al., 2015). Konsep ini mencakup dua aspek utama, yaitu pengetahuan (kesadaran) dan keterampilan (perilaku) yang berkaitan dengan perlindungan informasi pribadi di ranah digital (Prince et al., 2023). Seiring dengan meningkatnya keterlibatan pengguna dalam berbagai platform daring, tingkat literasi privasi yang dimiliki menjadi faktor penentu penting terhadap perilaku online mereka serta kapasitas mereka dalam melindungi data pribadi.

Penelitian-penelitian sebelumnya telah mengidentifikasi beragam dimensi dalam literasi privasi daring. Beberapa definisi menekankan pentingnya pemahaman terhadap risiko privasi serta tindakan-tindakan yang dapat diambil untuk memitigasinya (Lund, 2022), sementara definisi lain lebih menyoroti kesadaran terhadap praktik pengelolaan data oleh institusi serta kemampuan individu dalam mengevaluasi kebijakan privasi secara kritis (Desimpelaere et al., 2020). Salah satu komponen penting dalam OPL adalah keakraban teknis (*technical familiarity*), yang merujuk pada tingkat kenyamanan dan kemahiran individu dalam menggunakan teknologi digital dan alat-alat daring. Tingkat keakraban teknis yang lebih tinggi dapat memberdayakan pengguna untuk lebih memahami mekanisme teknis dalam pengumpulan dan perlindungan data, sehingga memengaruhi perilaku perlindungan privasi mereka serta keputusan terkait pengungkapan data pribadi. Dalam konteks ini, keakraban teknis juga berperan langsung terhadap kesediaan individu untuk mengungkapkan data pribadi secara online. Pemahaman teknis pengguna terhadap teknologi informasi dan komunikasi menjadi faktor penting dalam menentukan sejauh mana mereka merasa aman dan yakin untuk berbagi informasi pribadi.

Pemahaman teknis user terhadap teknologi informasi dan komunikasi memainkan peran penting dalam keputusan untuk mengungkapkan data pribadi secara online. Studi oleh Dwitha Yuniar & Fibrianto (2019) menunjukkan bahwa aspek teknis merupakan langkah awal bagi konsumen untuk menavigasi dan melindungi informasi pribadi mereka dari pelanggaran. Penelitian ini mengukur familiaritas konsumen dengan aspek teknis dan hubungannya dengan perilaku perlindungan konsumen dalam menggunakan e-commerce sebagai platform belanja online. Walaupun penyalahgunaan data pribadi menjadi salah satu masalah dalam berbelanja online (e-commerce) namun konsumen cenderung bersedia memberikan data pribadi melalui internet (Rahayu et al., 2023). Hal ini menunjukkan bahwa meskipun ada risiko penyalahgunaan data, tingkat familiaritas teknis dapat memengaruhi kesediaan konsumen untuk berbagi informasi pribadi.

Digital Trust Pada Platform Online

Kepercayaan terhadap platform digital telah diakui secara luas sebagai salah satu determinan utama dalam perilaku pengungkapan informasi pribadi di ranah daring. Dalam konteks ini, sejumlah penelitian menekankan bahwa kepercayaan memiliki peran krusial dalam mendorong keterlibatan pengguna, terutama ketika transaksi digital menuntut pengungkapan data pribadi dan finansial yang bersifat sensitif (Fathni et al., 2023; Zaki, 2023). Fathni et al. (2023) mengidentifikasi bahwa

kejelasan kebijakan privasi dan tingkat kepercayaan terhadap platform digital secara signifikan memengaruhi perilaku perlindungan privasi pengguna di Indonesia. Hasil ini menyoroti pentingnya transparansi informasi sebagai fondasi utama dalam membangun kepercayaan digital.

Sejalan dengan temuan tersebut, Zaki (2023) mengkaji dimensi etika dalam praktik pengumpulan data pribadi oleh organisasi dan perusahaan digital. Ia menekankan bahwa transparansi dalam pengelolaan data, bersama dengan upaya menjaga kepercayaan, merupakan elemen sentral dalam mendorong kesediaan individu untuk berbagi informasi pribadi. Perspektif ini menunjukkan bahwa kepercayaan tidak semata-mata bersifat teknis, tetapi juga dipengaruhi oleh penilaian moral dan persepsi etis pengguna terhadap niat dan integritas penyedia layanan digital.

Secara konseptual, kepercayaan dalam konteks daring dipahami sebagai keyakinan pengguna bahwa platform akan bertindak sesuai dengan kepentingan terbaik mereka, memenuhi komitmen, serta melindungi informasi pribadi yang mereka berikan (Gefen et al., 2003; McKnight et al., 2002). Dalam lingkungan digital yang diwarnai ketidakpastian dan asimetri informasi—seperti pada Online Travel Agencies (OTA)—kepercayaan menjadi komponen kunci dalam proses pengambilan keputusan (Chong et al., 2010). Berbagai studi literatur mengidentifikasi sejumlah faktor yang memengaruhi terbentuknya kepercayaan, termasuk reputasi platform, mekanisme keamanan, keterbukaan dalam pengelolaan data, dan kualitas pengalaman pengguna (Chen & Barnes, 2007; Beldad et al., 2010).

Dalam praktiknya, OTA menuntut pengguna untuk mengungkapkan informasi pribadi dan finansial guna menyelesaikan proses pemesanan. Ketika tingkat kepercayaan rendah, pengguna cenderung ragu, menghentikan transaksi, atau menolak memberikan data yang diperlukan. Sebaliknya, kepercayaan yang tinggi dapat mendorong partisipasi aktif serta kesediaan untuk berbagi informasi sensitif, dengan harapan memperoleh manfaat yang bersifat fungsional maupun kemudahan dalam penggunaan layanan (Flavián et al., 2006).

Dengan demikian, literatur secara konsisten menegaskan bahwa kepercayaan merupakan elemen esensial dalam ekosistem digital, terutama dalam membentuk sikap dan niat pengguna terkait pengungkapan informasi pribadi. Oleh karena itu, kombinasi antara transparansi kebijakan, kompetensi teknis, dan integritas operasional menjadi syarat utama dalam menciptakan hubungan jangka panjang yang berbasis kepercayaan antara pengguna dan penyedia layanan digital.

Kesediaan Mengungkapkan Data Pribadi

Kesediaan untuk mengungkapkan data pribadi merujuk pada tingkat kesiapan individu untuk memberikan informasi pribadinya kepada suatu pihak, biasanya sebagai imbalan atas manfaat atau layanan yang dirasakan (Degutis et al., 2020). Kesediaan ini dipengaruhi oleh interaksi yang kompleks antara berbagai faktor, termasuk kekhawatiran terhadap individu. Dalam hal data yang bersifat sensitif – seperti informasi terkait kesehatan, etnis, atau orientasi seksual, Tingkat kesediaan untuk mengungkapkannya umumnya lebih rendah karena adanya potensi yang lebih tinggi terhadap penyalahgunaan, diskriminasi, atau pelanggaran privasi (Zhang et al., 2021).

Dalam konteks platform daring, pengguna sering melakukan *privacy calculus*, yaitu mempertimbangkan manfaat yang dirasakan dari pengungkapan informasi

seperti layanan yang dipersonalisasi, kemudahan penggunaan, akses ke fitur tertentu, dengan resiko yang dipersepsikan seperti misalnya pencurian identitas, pemasaran yang tidak diinginkan, diskriminasi (Herbert et al., 2021). Sifat data yang diminta juga memiliki pengaruh yang signifikan. Secara umum pengguna lebih enggan mengungkapkan informasi yang sangat sensitif dibandingkan dengan data yang kurang sensitif (Groeppe-Klein & Freichel, n.d.). Bagi OTA, memahami tingkat kesediaan ini sangat penting, mengingat beberapa data sensitif mungkin diperlukan untuk pengaturan perjalanan tertentu (misalnya data kesehatan untuk keadaan darurat medis, preferensi diet, atau kebutuhan aksesibilitas; data etnis untuk pertimbangan budaya atau pengalaman perjalanan khusus).

3. Metode

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei untuk menganalisis pengaruh literasi privasi online dan kepercayaan terhadap kesediaan pengungkapan data pribadi. Pendekatan ini dipilih karena mampu mengukur hubungan antar variabel secara sistematis dengan menggunakan data numerik yang diolah secara statistik.

Populasi dalam penelitian ini adalah individu pengguna internet yang aktif melakukan transaksi atau aktivitas booking online pada online travel agency (OTA) Traveloka. Sampel penelitian diambil menggunakan teknik purposive sampling dengan kriteria berusia 18 tahun ke atas, memiliki pengalaman dalam mengisi atau memberikan data pribadi pada platform Traveloka dan berdomisili di wilayah Indonesia.

Jumlah sampel pada penelitian ini adalah 100, di mana jumlah ini sudah memenuhi syarat untuk dilakukan analisis regresi logit. Instrumen penelitian berupa kuesioner terstruktur yang terdiri dari empat bagian utama, yaitu bagian pertama meliputi pertanyaan mengenai demografi responden yang meliputi usia, jenis kelamin, tingkat pendidikan, dan pengalaman penggunaan internet. Bagian kedua adalah pertanyaan mengenai *technical familiarity* yang diukur menggunakan skala Likert dengan lima ketukan, yaitu sama sekali tidak familiar (1), sedikit familiar (2), cukup familiar (3), familiar (4), dan sangat familiar (5). *Digital trust* juga diukur dengan skala Likert 5 poin yaitu sangat tidak setuju (1), tidak setuju (2), netral (3), setuju (4), dan sangat tidak setuju (5) yang diukur berdasarkan aspek rekomendasi orang terdekat, pengalaman pribadi, dan review pengguna. Bagian ketiga adalah pertanyaan mengenai kesediaan pengungkapan data pribadi yang diukur melalui pernyataan mengenai kesediaan berbagi informasi pribadi dalam konteks berbagi informasi terkait status kesehatan dan etnis.

Data dikumpulkan melalui survei daring (online survey) menggunakan platform Qualtrics untuk menjangkau responden secara lebih luas dan efisien. Link survei disebarkan melalui media sosial, email, dan komunitas daring yang relevan. Data yang terkumpul dianalisis menggunakan pendekatan statistik deskriptif untuk menggambarkan karakteristik demografi responden serta distribusi jawaban kuesioner.

Uji validitas dan reliabilitas menggunakan Cronbach's Alpha dilakukan untuk memastikan konsistensi internal instrumen penelitian.

Analisis Regresi Logistik

Untuk menguji pengaruh variabel *Technical Familiarity* dan *Digital Trust* terhadap kesediaan untuk mengungkapkan data sensitif, penelitian ini menggunakan analisis regresi logistik biner. Metode analisis ini dipilih karena variabel dependen (*willingness to disclose*) dapat dikategorikan menjadi dua kategori logis atau bersifat dikotomis, yaitu:

0 = tidak bersedia mengungkapkan data Sensitif; dan

1 = bersedia mengungkapkan data sensitif.

Dua model regresi logistik dikembangkan secara terpisah untuk masing-masing jenis data sensitif, yaitu data kesehatan dan data etnis. Variabel independen utama dalam model adalah *technical familiarity* (X1) dan *digital trust* (X2), sementara variabel demografis berupa usia, jenis kelamin, tingkat pendidikan, dan status pekerjaan dimasukkan sebagai variabel kontrol.

Pendekatan ini memungkinkan estimasi probabilitas kecenderungan individu dalam mengungkapkan data sensitif berdasarkan tingkat familiaritas teknis dan kepercayaan terhadap platform OTA, sekaligus mengendalikan pengaruh faktor demografis.

Model Regresi

Secara matematis, model regresi logistik biner yang digunakan dalam penelitian ini dapat dirumuskan sebagai berikut:

$$\text{Logit}(P) = \ln\left(\frac{P}{1-P}\right) = \beta_0 + \beta_1 TF + \beta_2 DT + \beta_3 AGE + \beta_4 GEN + \beta_5 EDU + \beta_6 JOB + \varepsilon$$

Keterangan:

P = Probabilitas pengguna bersedia mengungkapkan data sensitif.

β_0 = Konstanta

$\beta_1 - \beta_6$ = Koefisien regresi

TF = *Technical Familiarity*.

DT = *Digital Trust*.

AGE = Usia

GEN = Jenis Kelamin

EDU = Pendidikan

JOB = Status Pekerjaan

Model ini digunakan untuk mengestimasi kecenderungan pengungkapan data sensitif dalam konteks OTA, dengan mempertimbangkan aspek teknis dan kepercayaan, serta karakteristik demografis pengguna.

4. Hasil dan Pembahasan

Statistik Deskriptif Responden

Sebanyak 100 responden berpartisipasi dalam survei ini. Karakteristik responden adalah sebagai berikut:

Tabel 1. Karakteristik Responden

Karakteristik	Kategori	Jumlah	Persentase	Mean	SD
Usia	18 – 34	56	56%	0.56	0.701
	35 – 54	32	32%		
	55+	12	12%		

Jenis Kelamin	Perempuan	48	48%	1.52	0.502
	Laki – laki	52	52%		
Pendidikan	Pendidikan rendah (sampai dengan SMP)	2	2%	3.68	0.680
	Pendidikan Menengah (SMA, S1)	92	92%		
	Pendidikan Tinggi (Master, Doktor)	6	6%		
Status pekerjaan	Aktif Bekerja	77	77%	2.30	1.972
	Tidak aktif bekerja	23	23%		

Analisis regresi logistik biner dilakukan untuk menguji pengaruh variabel *technical familiarity*, *digital trust* dan faktor demografi (jenis kelamin, usia, pendidikan, dan pekerjaan) terhadap kesediaan responden untuk mengungkapkan data kesehatan (Willingness to Disclose Health Data) dan data etnis (Willingness to Disclose Ethnicity Data).

Variabel dependen dikodekan secara dikotomis, yaitu $0 = \text{Tidak Bersedia}$ dan $1 = \text{Bersedia}$. Seluruh data (N=100) memenuhi kriteria analisis tanpa adanya nilai hilang.

Kesediaan Mengungkapkan Data Kesehatan

Hasil *Omnibus Test of Model Coefficients* menunjukkan bahwa model regresi logistik secara simultan tidak signifikan (Chi Square = 6,011; df = 6; sig.= 0,422) , yang mengindikasikan bahwa kombinasi variabel independen belum mampu meningkatkan kecocokan model secara signifikan dibandingkan dengan *null model*.

Nilai *Hosmer and Lemeshow Test* menunjukkan hasil yang tidak signifikan (Chi Square = 6,655; df = 8; Sig. = 0,574), sehingga dapat disimpulkan bahwa model memiliki kecocokan yang baik (good fit) antara data observasi dan data yang diprediksi oleh model.

Nilai *Nigelkerke R Square* sebesar 0,087 menunjukkan bahwa variabel-variabel independen dalam model hanya mampu menjelaskan sekitar 8,7% variasi kesediaan responden dalam mengungkapkan data kesehatan, sedangkan sisanya dipengaruhi oleh faktor lain di luar model penelitian ini.

Tabel klasifikasi menunjukkan bahwa model mampu mengklasifikasikan data dengan akurasi keseluruhan sebesar 75,0%. Model sangat baik dalam memprediksi kategori bersedia (98,7%), namun kurang optimal dalam memprediksi kategori tidak bersedia (0,0%).

Hasil uji parsial (*Wald test*) menunjukkan bahwa tidak terdapat satu pun variabel independen yang berpengaruh signifikan secara statistik terhadap kesediaan responden dalam mengungkapkan data kesehatan ($p > 0,05$).

Meskipun variabel *digital trust* menunjukkan arah koefisien regresi positif ($\text{Exp}(B) = 2,506$), pengaruh tersebut tidak signifikan secara statistik (sig. = 0,109), sehingga temuan ini hanya mengindikasikan adanya kecenderungan probabilistik, bukan hubungan kausal yang konklusif.

Variable *Technical Familiarity* dan faktor demografi (jenis kelamin, usia, pendidikan, dan pekerjaan) juga menunjukkan nilai signifikansi di atas 0,05, dengan confidence interval $\text{Exp}(B)$ yang mencakup nilai 1. Hal ini menunjukkan bahwa secara parsial, seluruh variabel tersebut belum terbukti berpengaruh signifikan terhadap probabilitas kesediaan responden dalam mengungkapkan data kesehatan.

Rata-rata probabilitas prediksi kesediaan responden untuk mengungkapkan data kesehatan adalah sebesar 0,76 (SD = 0,105), dengan nilai minimum 0,48 dan maksimum 0,94. Hal ini menunjukkan bahwa secara umum responden memiliki kecenderungan yang relatif tinggi untuk bersedia mengungkapkan data kesehatan, meskipun kecenderungan tersebut belum dapat dijelaskan secara kuat oleh variabel-variabel dalam model penelitian ini.

Kesediaan Mengungkapkan Data Etnis

Hasil *Omnibus Test Model Coefficients* menunjukkan bahwa model regresi logistik tidak signifikan secara statistik (Chi Square = 3,882; df = 2; sig. = 0,144). Hal ini mengindikasikan bahwa variabel *technical familiarity* dan *digital trust* secara simultan belum mampu meningkatkan kemampuan model dalam memprediksi kesediaan responden untuk mengungkapkan data etnis dibandingkan dengan model dasar (*null model*).

Meskipun demikian, hasil uji *Hosmer Lemeshow* menunjukkan nilai signifikansi sebesar 0,400 ($p > 0,05$), yang menandakan bahwa model memiliki kecocokan yang memadai antara nilai yang diobservasi dan nilai yang diprediksi oleh model regresi logistik.

Nilai *Nagelkerke R Square* sebesar 0,051 menunjukkan bahwa variabel independen dalam model hanya mampu menjelaskan sekitar 5,1% variasi kesediaan responden dalam mengungkapkan data etnis. Nilai ini mengindikasikan bahwa sebagian besar variasi perilaku pengungkapan data etnis dipengaruhi oleh faktor lain di luar model penelitian ini.

Berdasarkan *classification table*, model memiliki akurasi klasifikasi keseluruhan sebesar 55,0%. Model mampu mengklasifikasikan dengan benar 67,3% responden yang bersedia mengungkapkan data etnis, namun hanya mampu mengklasifikasikan dengan benar 40,0% responden yang tidak bersedia. Temuan ini menunjukkan bahwa kemampuan prediksi model tergolong rendah hingga moderat, khususnya dalam membedakan responden yang bersedia mengungkapkan data etnis.

Hasil uji parsial (*Wald test*) menunjukkan bahwa tidak terdapat variabel independen yang berpengaruh signifikan secara statistik terhadap kesediaan responden untuk mengungkapkan data etnisitas ($p > 0,05$).

Variable *digital trust* memiliki koefisien regresi positif ($B = 0,525$) dengan nilai *odds ratio* sebesar 1,691. Hal ini mengindikasikan bahwa peningkatan tingkat kepercayaan cenderung meningkatkan peluang responden untuk bersedia mengungkapkan data etnis. Namun demikian, pengaruh tersebut tidak signifikan secara statistik (sig. = 0,259), sehingga belum dapat disimpulkan sebagai faktor penentu utama dalam pengambilan keputusan pengungkapan data etnisitas.

Variable *technical familiarity* juga menunjukkan arah pengaruh positif ($B = 0,311$; $\text{Exp}(B) = 1,365$), yang berarti bahwa peningkatan familiaritas teknis cenderung meningkatkan peluang kesediaan pengungkapan data etnis. Akan tetapi, pengaruh ini juga tidak signifikan secara statistik (sig. = 0,300), dengan rentang confidence interval

yang mencakup nilai 1 (satu), sehingga pengaruhnya belum dapat dibuktikan secara empiris.

Distribusi probabilitas prediksi menunjukkan bahwa model menghasilkan variasi probabilitas yang cukup lebar antara responden yang bersedia dan tidak bersedia mengungkapkan data etnisitas. Namun, tidak ditemukan outlier ekstrem dalam model, yang menandakan bahwa estimasi parameter relatif stabil dan tidak dipengaruhi oleh kasus-kasus tertentu secara berlebihan.

Pembahasan

Penelitian ini mengkaji faktor-faktor yang memengaruhi kesediaan individu dalam mengungkapkan data pribadi yang bersifat sensitif, khususnya data kesehatan dan data etnis, dengan menitikberatkan pada peran keakraban teknis dan kepercayaan. Hasil analisis regresi logistik menunjukkan bahwa pada kedua model, variabel-variabel independen belum menunjukkan pengaruh yang signifikan secara statistik, baik secara simultan maupun secara parsial.

Pada kedua model, variabel digital trust menunjukkan arah koefisien yang positif terhadap kesediaan responden untuk mengungkapkan data kesehatan maupun data etnis. Meskipun demikian, pengaruh tersebut tidak signifikan secara statistik. Temuan ini secara konseptual sejalan dengan kerangka *privacy calculus theory*, yang menyatakan bahwa individu akan mempertimbangkan manfaat dan risiko sebelum memutuskan untuk membagikan data pribadi (Fernandes & Pereira, 2021; Gouthier et al., 2022; Paspatis et al., 2023). Kepercayaan terhadap penyedia layanan digital merupakan salah satu manfaat psikologis utama yang dapat menurunkan persepsi risiko.

Namun, hasil penelitian ini menunjukkan bahwa dalam konteks data yang sangat sensitif, seperti data kesehatan dan data etnis, kepercayaan saja belum cukup kuat untuk mendorong perilaku pengungkapan data pada media digital. Sejumlah penelitian setelah tahun 2018 menegaskan bahwa sensitivitas data memoderasi peran kepercayaan (Gouthier et al., 2022; Li et al., 2023). Pengguna cenderung tetap bersikap hati-hati meskipun memiliki tingkat kepercayaan yang relatif tinggi, karena meningkatnya kesadaran risiko kebocoran data, diskriminasi, serta penyalahgunaan informasi oleh pihak ketiga.

Dalam konteks data etnis, ketidaksignifikanan pengaruh kepercayaan menjadi semakin relevan. Literatur mutakhir menunjukkan bahwa data etnis dan ras sering dikaitkan dengan isu diskriminasi sosial, eksklusifitas, dan stigma, sehingga individu cenderung menahan diri untuk mengungkapkan informasi tersebut meskipun mereka mempercayai platform penyedia layanan (Goldshstein et al., 2024; Nong et al., 2022). Dengan demikian, temuan ini memperkuat argumen bahwa tingkat sensitivitas dan implikasi sosial dari jenis data berperan penting dalam menentukan efektivitas dan implikasi sosial dari jenis data dalam menentukan efektivitas kepercayaan sebagai pendorong pengungkapan data pribadi.

Hasil penelitian menunjukkan bahwa *technical familiarity* tidak berpengaruh signifikan terhadap kesediaan pengungkapan data, baik pada model data kesehatan maupun data etnis. Temuan ini memberikan kontribusi penting terhadap literatur terkini yang menunjukkan bahwa familiaritas teknologi memiliki sifat ambivalen.

Penelitian-penelitian awal banyak menekankan bahwa peningkatan literasi dan pengalaman teknologi dapat meningkatkan rasa aman dan kenyamanan pengguna. Namun, studi-studi terbaru setelah tahun 2019 menunjukkan bahwa pengguna yang

semakin familiar dengan teknologi justru cenderung lebih sadar akan risiko privasi, praktik pengumpulan data, serta potensi eksploitasi informasi pribadi. Dalam konteks ini, peningkatan familiaritas tidak otomatis meningkatkan kesediaan untuk berbagi data sensitif, melainkan dapat memperkuat sikap kehati-hatian (Han et al., 2026; Herriger et al., 2025; Li et al., 2023).

Temuan penelitian ini mendukung pandangan tersebut, khususnya dalam konteks data kesehatan dan etnis yang memiliki konsekuensi personal dan sosial jangka panjang. Dengan demikian, familiaritas teknologi lebih berperan sebagai faktor yang meningkatkan kesadaran risiko dibandingkan dengan pendorong langsung pengungkapan data.

Integrasi hasil dari kedua model menunjukkan bahwa jenis data menjadi faktor kontekstual yang sangat penting. Meskipun kedua model sama-sama menunjukkan kecocokan model yang baik berdasarkan uji *Hosmer and Lemeshow*, kemampuan variabel independen dalam menjelaskan model relatif rendah, yaitu 8,7% untuk data kesehatan dan 5,1% untuk data etnis.

Perbedaan ini mengindikasikan bahwa kesediaan untuk mengungkapkan data etnisitas cenderung lebih sulit dijelaskan oleh variabel kepercayaan dan familiaritas teknis dibandingkan dengan data kesehatan. Literatur terkini menjelaskan bahwa data etnisitas termasuk dalam kategori *immutable and socially sensitive attributes*, sehingga keputusan pengungkapannya lebih banyak dipengaruhi oleh faktor struktural, seperti norma sosial, konteks budaya, dan kekhawatiran akan diskriminasi, dibandingkan dengan faktor individual semata.

5. Kesimpulan

Penelitian ini bertujuan untuk menganalisis pengaruh *technical familiarity* dan *digital trust* terhadap kesediaan konsumen dalam mengungkapkan data pribadi yang bersifat sensitif, khususnya data kesehatan dan data etnis, dalam konteks penggunaan aplikasi perjalanan daring. Dengan menggunakan pendekatan regresi logistik biner, penelitian ini memberikan pemahaman empiris mengenai faktor-faktor yang memengaruhi keputusan konsumen dalam menghadapi dilema privasi di ekosistem platform digital.

Hasil analisis menunjukkan bahwa baik *technical familiarity* maupun *digital trust* tidak berpengaruh signifikan secara statistik terhadap kesediaan responden dalam mengungkapkan data kesehatan maupun data etnis. Meskipun demikian, arah koefisien regresi pada kedua variabel menunjukkan kecenderungan positif, terutama pada *digital trust*, yang mengindikasikan bahwa peningkatan kepercayaan terhadap platform berpotensi meningkatkan probabilitas pengungkapan data. Namun, pengaruh tersebut belum cukup kuat untuk membentuk hubungan kausal yang konklusif, terutama dalam konteks data yang sangat sensitif.

Selain itu, *technical familiarity* juga tidak terbukti berpengaruh signifikan, yang menunjukkan bahwa peningkatan literasi dan keakraban teknologi tidak secara otomatis mendorong perilaku berbagi data. Sebaliknya, familiaritas teknis justru berpotensi meningkatkan kesadaran risiko dan sikap kehati-hatian pengguna. Temuan ini menegaskan bahwa perilaku pengungkapan data sensitif merupakan fenomena kompleks yang dipengaruhi oleh berbagai faktor di luar dimensi kepercayaan dan kemampuan teknis, termasuk norma sosial, nilai budaya, serta persepsi risiko jangka panjang.

Secara teoretis, hasil penelitian ini menunjukkan keterbatasan model *privacy calculus* dalam menjelaskan perilaku pengungkapan data sensitif pada platform digital. Oleh karena itu, penelitian selanjutnya disarankan untuk memasukkan variabel tambahan, seperti *perceived privacy risk*, *perceived control*, *institutional assurance*, serta faktor budaya dan sosial. Dari sisi praktis, temuan ini mengimplikasikan perlunya strategi perlindungan data yang lebih transparan, akuntabel, dan komunikatif oleh penyedia platform, khususnya dalam pengelolaan data yang sangat sensitif, guna meningkatkan kepercayaan dan kenyamanan pengguna dalam ekosistem digital.

6. Daftar Pustaka

- Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147–154. <https://doi.org/10.1016/j.chb.2015.11.022>
- Budiutono, S. (2023). *saiful,+39.+8692+Budiutono. VII(2)*.
- Degutis, M., Urbonavicius, S., Zimaitis, I., Skare, V., & Laurutyte, D. (2020). Willingness to disclose personal information: How to measure it? *Engineering Economics*, 31(4), 487–494. <https://doi.org/10.5755/j01.ee.31.4.25168>
- Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, 110. <https://doi.org/10.1016/j.chb.2020.106382>
- Dwitha Yuniar, A., & Fibrianto, A. S. (2019). *The Affect of Technical Familiarity and Consumer Protection Behavior in Using E-Commerce as Platform Online Shopping*.
- Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, 65. <https://doi.org/10.1016/j.tele.2021.101717>
- Goldshtein, M., Chiou, E. K., & Roscoe, R. D. (2024). 'I Just Don't Trust Them': Reasons for Distrust and Non-Disclosure in Demographic Questionnaires for Individuals in STEM. *Societies*, 14(7). <https://doi.org/10.3390/soc14070105>
- Gouthier, M. H. J., Nennstiel, C., Kern, N., & Wendel, L. (2022). The more the better? Data disclosure between the conflicting priorities of privacy concerns, information sensitivity and personalization in e-commerce. *Journal of Business Research*, 148, 174–189. <https://doi.org/10.1016/j.jbusres.2022.04.034>
- Groepel-Klein, A., & Freichel, M. (n.d.). The Impact of Shopping Environment and Type of Data on Consumers' Willingness to Disclose Sensitive Data. In *Advances in Consumer Research* (Vol. 47). Retrieved <https://economictimes.indiatimes>.
- Han, H., Zhang, C. (Jason), Ketema, A. F., Kim, S. (Sam), Chua, B. L., & Al-Ansi, A. (2026). Emerging data security and information privacy issues in the lodging industry: The impact of brand confidence. *International Journal of Hospitality Management*, 133. <https://doi.org/10.1016/j.ijhm.2025.104513>
- Herbert, C., Marschin, V., Erb, B., Meißner, D., Aufheimer, M., & Bösch, C. (2021). Are You Willing to Self-Disclose for Science? Effects of Privacy Awareness and Trust in Privacy on Self-Disclosure of Personal and Health Data in Online Scientific Studies—An Experimental Study. *Frontiers in Big Data*, 4. <https://doi.org/10.3389/fdata.2021.763196>
- Herriger, C., Merlo, O., Eisingerich, A. B., & Arigayota, A. R. (2025). Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, Augmented Reality, Big Data, and the Internet of Things: Systematic Review. In *Journal of Medical Internet Research* (Vol. 27, Number 1). JMIR Publications Inc. <https://doi.org/10.2196/71951>

- Li, J., Zhang, Y., & Mou, J. (2023). Understanding information disclosures and privacy sensitivity on short-form video platforms: An empirical investigation. *Journal of Retailing and Consumer Services*, 72. <https://doi.org/10.1016/j.jretconser.2023.103292>
- Lund, B. D. (2022). *Libraries in a World of Data* (pp. 182–196). <https://doi.org/10.4018/978-1-7998-8942-7.ch011>
- Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, 8(2), 258–269. <https://doi.org/10.17645/mac.v8i2.2855>
- Nong, P., Williamson, A., Anthony, D., Platt, J., & Kardia, S. (2022). Discrimination, trust, and withholding information from providers: Implications for missing data and inequity. *SSM - Population Health*, 18. <https://doi.org/10.1016/j.ssmph.2022.101092>
- Okditazeini, V., & Irwansyah, I. (2018). Ancaman Privasi dan Data Mining di Era Digital: Analisis Meta-Sintesis pada Social Networking Sites (SNS). *Jurnal Studi Komunikasi Dan Media*, 22(2), 109. <https://doi.org/10.31445/jskm.2018.220202>
- Paspatis, I., Tsohou, A., & Kokolakis, S. (2023). How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors. In *Multimodal Technologies and Interaction* (Vol. 7, Number 8). Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/mti7080076>
- Prince, C., Omrani, N., & Schiavone, F. (2023). Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. *Information Technology and People*, 37(8), 1–24. <https://doi.org/10.1108/ITP-05-2023-0467>
- Rahayu, I. L., Syarifa, R., Akmalia, L. R., Samosir, M. S., Puja Hanggrita, E., Muflikhati, I., & Simanjuntak, M. (2023). Willingness to Share Data Pribadi dan Kaitannya dengan Penyalahgunaan Data Konsumen E-Commerce di Indonesia: Pendekatan Mixed Methods. *Jurnal Ilmu Keluarga Dan Konsumen*, 16(3), 274–287. <https://doi.org/10.24156/jikk.2023.16.3.274>
- Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online Privacy Literacy and Online Privacy Behavior—The Role of Crystallized Intelligence and Personality. *International Journal of Human-Computer Interaction*, 37(15), 1455–1466. <https://doi.org/10.1080/10447318.2021.1894799>
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F., Trepte, S., Teutsch, • D, Masur, • P K, Eicher, • C, Fischer, • M, Hennhöfer, • A, & Lind, • F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the “Online Privacy Literacy Scale (OPLIS).” *Governance and Technology Series*, 20. https://doi.org/10.1007/978-94-017-9385-8_14
- Williams, M., & Nurse, J. R. C. (2016). *Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective* (T. Tryfonas, Ed.; Vol. 9750). Springer International Publishing. <https://doi.org/10.1007/978-3-319-39381-0>
- Zhang, C., Cui, C., & Yao, Q. (2021). “I” Am Willing to Disclose, but “We” are Unwilling: The Impact of Self-Construal on Individuals' Willingness to Disclose. *Psychology Research and Behavior Management*, 14, 1929–1945. <https://doi.org/10.2147/PRBM.S336223>