Jurnal Industri Pariwisata **e-ISSN : 2620-9322**
Vol 7, No. 2, 2025

ANALISIS FAKTOR-FAKTOR YANG MENENTUKAN PERSEPSI PENGUNJUNG TERKAIT KEAMANAN DAN PRIVASI DATA PADA REGISTRASI PEMBELIAN TIKET ONLINE PENYELENGGARAAN EVENT

Renno Reymond Okto Zulfikar[1], Onggo Pramudito[2], Kurniawan Gilang Widagdyo[3]

[1,2]Universitas Mercu Buana
Jl. Meruya Selatan, Kembangan, Jakarta Barat
[3]Politeknik Multimedia Nusantara
Jl. Jenderal Gatot Subroto, Gading Serpong, Kab Tangerang
Email Correspondence: kurniawan.gilang@mnp.ac.id

ABSTRAK

Urgensi penelitian ini terletak pada kebutuhan untuk memahami bagaimana pengunjung event menilai dan merespons kebijakan keamanan dan privasi yang diterapkan dalam sistem registrasi online. Tujuan utama penelitian ini adalah mengidentifikasi dan menganalisis faktor-faktor kunci yang memengaruhi persepsi pengunjung terhadap keamanan dan privasi data saat pembelian tiket online. Dengan menggunakan metode kuantitatif melalui analisis faktor, penelitian ini memberikan pandangan yang komprehensif tentang perspektif pengunjung terkait keamanan data dalam registrasi online. Hasil penelitian menemukan empat faktor baru yang memengaruhi persepsi pengunjung: pertama, jaminan sistem keamanan, dengan nilai Eigen sebesar 7.066 yang menjelaskan 22.70% varians; kedua, kepercayaan terhadap proses registrasi, dengan nilai Eigen 3.453 dan varians 21.75%; ketiga, protokol keamanan, dengan nilai Eigen 1.195 dan varians 5.55%; serta keempat, persetujuan pemanfaatan data pribadi, dengan nilai Eigen 1.073 dan varians 4.98%. Penelitian ini menyimpulkan bahwa keempat faktor tersebut memiliki implikasi penting terhadap tingkat kepercayaan pengunjung dan keputusan mereka dalam menggunakan layanan tiket online.

Kata Kunci: MICE; Manajemen Event; Analisa Faktor; Keamanan dan Privasi; Registrasi Online

ABSTRACT

The urgency of this research lies in the need to understand how event attendees evaluate and respond to the security and privacy policies implemented in online registration systems. The primary objective is to identify and analyze the key factors influencing visitors' perceptions of data security and privacy in online ticket purchases. This study employs a quantitative factor analysis method to provide a comprehensive understanding of visitors' perspectives on data security and privacy during online registration. The findings reveal four new factors influencing visitors' perceptions. The first, labeled as the system security assurance factor, has an Eigenvalue of 7.066, explaining 22.70% of the variance and consists of 10 indicators. The second factor, trust in the registration process, has an Eigenvalue of 3.453, explaining 21.75% of the variance, and consists of 7 indicators. The third factor, security protocols, has an Eigenvalue of 1.195 and explains 5.55% of the variance with 2 indicators. The fourth factor, consent for data use, has an Eigenvalue of 1.073, accounting for 4.98% of the variance, with a single indicator.

Keyword: *MICE; Management Event; Factor Analysis; Privacy and Security; Registration Online*

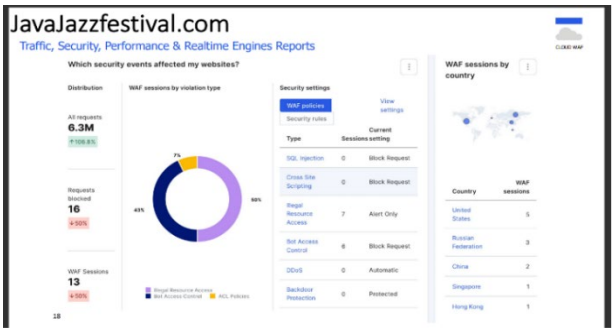
PENDAHULUAN

Industri event, khususnya dalam konteks MICE dan Special Event, beroperasi di lingkungan dimana penggunaan teknologi informasi dan registrasi online sudah menjadi hal yang lumrah. Dalam hal ini, penting bagi penyelenggara acara untuk memahami secara mendalam faktor-faktor yang membentuk persepsi pengunjung terhadap keamanan informasi. Keterlibatan pengunjung dalam acara sering kali bergantung pada kepercayaan mereka terhadap keamanan informasi pribadi yang dibagikan melalui sistem pendaftaran online.

Isu terkait pentingnya keamanan data pribadi dalam registrasi online semakin menonjol dengan adanya pelanggaran keamanan data yang menghebohkan dunia. Kepercayaan pengunjung terhadap keutuhan dan keamanan data pribadinya menjadi landasan yang sangat penting bagi keberhasilan penyelenggaraan suatu acara. Oleh karena itu, pendaftaran online memerlukan pemahaman menyeluruh tentang faktor-faktor yang mempengaruhi persepsi pengunjung terhadap keamanan dan privasi. Beberapa kasus kebocoran data terkait penyelenggaraan event pernah terjadi dan menjadi perhatian serius terkait jaminan privasi dan keamanan data, beberapa kasus diataranya sebagai berikut:

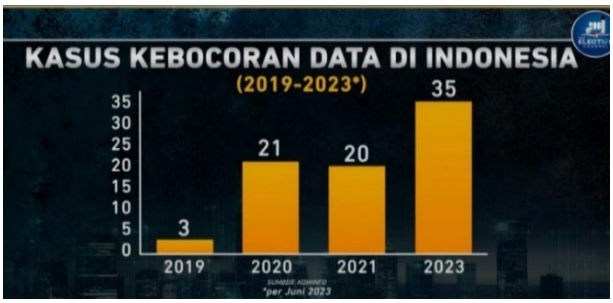
Pada bulan September 2011, dua iPad berisi data yang dikumpulkan dari salah satu acara pelanggan mereka dicuri oleh karyawan Eventbrite. Eventbrite menggambarkan dirinya sebagai "platform teknologi acara terbesar di dunia". untuk menciptakan "teknologi yang memungkinkan setiap orang untuk berkreasi, berbagi, menemukan, dan fokus pada hal-hal baru yang mendorong minat dan memperkaya kehidupan mereka." Kevin Hartz, pendiri dan CEO Eventbrite pada saat itu, menulis dalam postingan blog di situs web perusahaan bahwa "informasi yang berpotensi berisiko termasuk informasi kartu kredit lengkap dari 28 orang yang membeli tiket acara tersebut; nama dan alamat email dari Eventbrite setiap pelanggan yang membeli tiket acara tersebut secara online, serta beberapa nama, alamat email, dan empat digit terakhir kartu kredit penggemar yang membeli tiket tersebut salah dicatat karena bug di aplikasi iPad" Meskipun perusahaan memberi tahu peserta yang alamat emailnya mungkin telah disusupi dan segera memberi tahu pihak berwenang serta mulai mengunci kata sandi dan menghapus data di kedua perangkat dari jarak jauh, Hartz tetap memahami bahwa membobol informasi pribadi merupakan pelanggaran kepercayaan dan meminta maaf kepada mereka yang menjadi korban (Peña & Mortada, 2016)

Selama berlangsungnya Event Java Jazz Festival 2022, peningkatan jumlah pengunjung yang signifikan menyebabkan website ticketing acara tersebut menjadi target serangan DDoS atau bot attack. Dalam laporan yang diterbitkan pada 27–29 Mei 2022, tercatat bahwa serangan DDoS semakin kompleks. Salah satu metode yang teridentifikasi adalah pengiriman lalu lintas berlebih ke jaringan melalui kombinasi beberapa vektor serangan, seperti UDP flood, SYN flood, large SYN, dan DNS amplification. Serangan ini mencakup penggunaan DNS amplification dengan volume besar ke berbagai target, serta serangan SYN flood pada port 80 secara bersamaan. Pada serangan pertama, lalu lintas mencapai 192 Gbps dan 33 juta Mbps, sementara beberapa menit kemudian memuncak hingga 1,02 Tbps dan 155 Mbps melalui kombinasi teknik serangan yang berbeda. Panitia berhasil melakukan mitigasi secara cepat dan otomatis, sehingga mampu mengatasi serangan DDoS dalam waktu kurang dari satu detik dan menangani serangan dengan berbagai ukuran dan durasi pada situs JJF 2022 (Adianto, 2022)



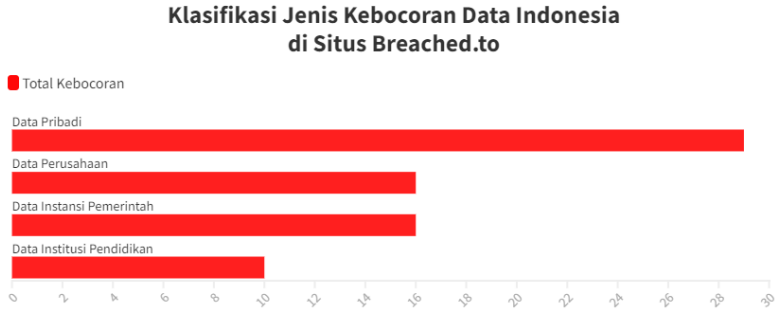
Tabel 1. Serangan cyber pada website registrasi Java Jazz Festival 2022
Sumber: bluepowertechnology.com

Selain serangan terhadap sistem registrasi online, beberapa aplikasi yang menyimpan data pelanggan juga menjadi target serangan siber, yang mengakibatkan keresahan di masyarakat. Salah satu insiden melibatkan pembobolan akun Paylater milik pengguna Traveloka, di mana seorang pengguna bernama Trias mengalami kerugian akibat akun Paylater-nya dibobol dan tetap dibebani tagihan (Esaunggul, 2023). Menurut tulisannya di mediakonsumen.com, peretasan tersebut terjadi pada 4 April 2019, ketika akun Gmail-nya diakses oleh pihak tidak bertanggung jawab dan mengakibatkan empat transaksi pembelian tiket senilai Rp 2.848.310 yang dilakukan melalui layanan Paylater. Selain itu, terjadi juga kebocoran data pengguna BPJS Ketenagakerjaan, di mana 18,5 juta data pengguna dijual di forum gelap dengan harga Rp 153 juta. Dalam unggahan di BreachForums, penjahat siber dengan nama Bjorka membocorkan 19,5 juta data dengan judul 'BPJS Ketenagakerjaan Indonesia 19 million'. Kebocoran data juga dialami oleh Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) Kementerian Dalam Negeri, dengan total 337 juta data bocor yang mencakup informasi penting seperti nama, Nomor Induk Kependudukan (NIK), nomor Kartu Keluarga (KK), tanggal lahir, alamat, nama orang tua, serta nomor akta lahir dan nikah (Javier, 2022)



Tabel 2. Jumlah Kasus Kebocoran Data Di Indonesia
Sumber:Metrotv news

Tabel diatas menjelaskan bahwasannya serangan ciber terhadap keamanan dan privasi data cenderung meningkat setiap tahunnya dan sebagian besar pencurian berasal dari luar negeri, menurut data dari Kementerian Komunikasi dan Informasi, sejak 2019 sudah ada 79 kasus terjadi pencurian data di dalam negeri (Febriari, 2023)



Tabel 3. Klasifikasi Jenis Kebocoran Data di Indonesia
Sumber: Tempo.com

Berdasarkan informasi yang dihimpun oleh Tempo, sejumlah pengguna anonim diketahui membagikan data pribadi yang diperoleh dari berbagai sumber, termasuk jasa fotokopi, perusahaan, dan lembaga pendidikan. Selain itu, Tempo juga menemukan bahwa beberapa pengguna forum tersebut membagikan informasi yang berasal dari lembaga pemerintah, seperti kementerian, kepolisian, Badan Intelijen Negara (BIN), dan Bea Cukai. Data yang bocor ke lembaga pemerintah ini umumnya mencakup informasi sensitif, seperti foto, nama lengkap, Nomor Induk Kependudukan (NIK), pekerjaan, serta akta kelahiran dan ijazah. Selain data dari instansi pemerintah, ditemukan pula kebocoran data pribadi dari sektor swasta, termasuk perusahaan marketplace, telekomunikasi, pertambangan, dan komoditas. Data pribadi yang tersebar di internet tersebut juga meliputi informasi yang berasal dari sejumlah institusi perguruan tinggi (Javier, 2022)

Kemajuan teknologi juga turut mempermudah penyelenggara event (Event Organizer) dalam menjual tiket eventnya, trend penjualan secara offline dengan mengantri di tiket box perlahan tergantikan dengan penjualan tiket secara online menggunakan aplikasi atau website. Kompetisi antar event yang semakin ketat membuat pemilihan platform tempat jual tiket event online menjadi krusial. Bukan hanya pembeli yang diuntungkan dengan sistemnya yang mudah, EO pun perlu menimbang mana platform yang paling bermanfaat, praktis, dan terpercaya. Setidaknya terdapat 3 platform registrasi serta penjualan tiket online yang banyak digunakan oleh berbagai macam event di Indonesia seperti (Nabila, 2020)

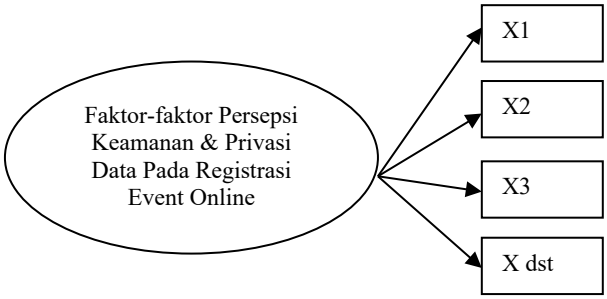
1. Platform Loket.com. Platform penjualan tiket event Online ini sangat populer di kalangan penyelenggara acara. Sebelum menjadi tren acara online, Loket.com adalah rumah bagi ribuan acara offline, dari kecil hingga besar. Di masa pandemi, Loket.com berinovasi dalam pengembangan acara online untuk menyediakan fitur acara online khusus bagi pembuat acara.
2. Platform Eventbrite. Eventbrite tersedia di banyak negara, jadi tidak ada batasan berapa banyak orang yang dapat membeli tiket acara, pembelian dapat dilakukan jika pembeli memiliki kartu kredit/debit atau PayPal untuk pembayaran.
3. Platform Goers. Platform satu ini memberikan pilihan kategori event yang beragam. Mulai dari konser, workshop, seminar, dan lain-lain. Bukan hanya fokus untuk penjualan tiket event online, di Goers juga terdapat penjualan tiket bioskop.

Berdasarkan hal tersebut maka rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Apa saja faktor-faktor yang menjadi pertimbangan utama bagi pengunjung dalam menilai tingkat keamanan dan privasi data saat menggunakan melakukan registrasi pembelian tiket secara online?
2. Bagaimana faktor-faktor tersebut memengaruhi persepsi pengunjung terkait dengan keamanan dan privasi data?
3. Bagaimana implikasi dari faktor-faktor tersebut terhadap kepercayaan pengunjung dan keputusan mereka untuk menggunakan layanan penjualan tiket online dalam partisipasi acara?

METODE PENELITIAN

Metode yang digunakan pada penelitian ini dibagi menjadi dua bagian besar berdasarkan jenis datanya yaitu kualitatif dan kuantitatif. Pengolahan data dengan menggunakan teknik statistik analisa faktor eksploratori sebagai teknik analisis kuantitatif digunakan untuk mengetahui apa saja faktor-faktor yang menjadi persepsi pengunjung event terkait keamanan dan privasi data pada registrasi event secara online, yang kemudian di sesuaikan dengan hasil wawancara mendalam menggunakan analisis deskritif sebagai metode analisis kualitatif. Pengolahan dan analisis data statistik menggunakan metode analisa faktor yang di olah menggunakan SPSS ver 16. Adapun penjabaran uraian diatas tertuang pada kerangka penelitian dibawah:



Gambar 1. Model Kerangka Konseptual Penelitian

Metode Analisis Data

Analisis Faktor adalah metode statistik multivariat yang bertujuan untuk mengurangi dan menyederhanakan variabel-variabel yang saling berhubungan dengan prinsip dasar mengidentifikasi sejumlah faktor bersama dari sekumpulan variabel X1, X2, …, Xp. Teknik ini memungkinkan reduksi jumlah variabel asli menjadi sejumlah variabel baru yang lebih sedikit, yang dikenal sebagai faktor, variabel laten, atau konstruk. Dengan menggunakan pendekatan ini, interpretasi hasil analisis menjadi lebih mudah, dan informasi penting yang terkandung dalam variabel asli dapat dikonsolidasi ke dalam faktor-faktor tersebut, sehingga mengurangi jumlah faktor yang diperlukan dibandingkan dengan jumlah variabel awal, sambil tetap menyimpan sebagian besar informasi variabel asli (Baroroh, 2013).

Penelitian ini menggunakan teknik analisa faktor sebagai desain dasar penelitian yang bersifat deskriptif kuantitatif. Tujuan dari analisis ini adalah untuk mengidentifikasi faktor-faktor yang membentuk persepsi pengunjung mengenai keamanan dan privasi data dalam konteks penjualan tiket online untuk penyelenggaraan acara. Berikut ini gambar mengenai Diagram Alir Penelitian

Gambar 3. Diagram Alir Penelitian

Tahapan penelitian yang akan dilaksanakan dapat dijelaskan sebagai berikut:

1. **Perumusan Masalah**: Langkah awal melibatkan identifikasi tujuan analisis faktor. Variabel yang digunakan dalam analisis faktor perlu ditentukan berdasarkan penelitian sebelumnya, teori, dan pertimbangan peneliti. Variabel-variabel tersebut harus diukur menggunakan skala interval atau rasio. Selain itu, ukuran sampel (n) harus memadai untuk analisis.
2. **Evaluasi Kelayakan Data**: Peneliti harus menentukan apakah data yang ada memenuhi persyaratan untuk analisis faktor. Tahap ini dimulai dengan mengidentifikasi matriks korelasi antara indikator-indikator yang diobservasi, yang dievaluasi menggunakan nilai Kaiser-Meyer-Olkin (KMO).
3. **Ekstraksi Faktor**: Ekstraksi faktor adalah metode untuk menyederhanakan data dengan mereduksi sejumlah indikator menjadi faktor yang lebih sedikit, sambil tetap mempertahankan kemampuan untuk menjelaskan hubungan antara indikator-indikator yang diobservasi. Dalam penelitian ini, teknik Principal Components Analysis (PCA) digunakan untuk proses ekstraksi faktor.
4. **Rotasi Faktor**: Rotasi faktor bertujuan untuk memperoleh struktur faktor yang lebih sederhana dan lebih mudah diinterpretasikan. Dalam hal ini, metode Varimax digunakan untuk proses rotasi.
5. **Interpretasi Faktor**: Faktor-faktor yang terbentuk diinterpretasikan dengan mengidentifikasi variabel-variabel yang mendasarinya. Proses interpretasi ini dilakukan dengan judgment peneliti.
6. **Penggunaan Skor Faktor**: Skor faktor yang dihasilkan berguna untuk analisis lanjutan, seperti regresi, diskriminan, atau analisis lainnya. Variabel surrogate digunakan sebagai representasi utama dari suatu faktor, sementara *summated scale* adalah kombinasi dari beberapa variabel dalam satu faktor, yang dapat berupa nilai rata-rata atau penjumlahan dari semua variabel yang membentuk faktor tersebut.

Adapun rumus dari Analisa faktor adalah sebagai berikut

$Xi = Bi1F1 + Bi2F2 + Bi3F3 + ... + BijFj + ... + BimFm + Vi\mu i$ (1)

keterangan:

Xi = Variabel ke i yang dibakukan

Bij = Koefisien regresi yang dibakukan untuk variabel i pada komponen faktor j

Fj = Komponen fator ke j

Vi = Koefisien regresi yang dibakukan untuk variabel i pada komponen faktor i

μi = Faktor unik variabel ke i

m = Banyaknya komponen faktor

Indeks Kaiser-Meyer-Olkin (KMO) digunakan untuk menilai kecukupan sampel dalam analisis faktor. Nilai KMO yang tinggi, yakni antara 0,5 hingga 1,0, menunjukkan bahwa data memiliki kecukupan untuk dilakukan analisis faktor. Sebaliknya, nilai KMO di bawah 0,5 mengindikasikan bahwa analisis faktor tidak sesuai untuk diterapkan pada data tersebut (Baroroh, 2013).

$$KMO = \frac{\sum_i \sum_{i \neq k} r_{ik}^2}{\sum_i \sum_{i \neq k} r_{ik}^2 + \sum_i \sum_{i \neq k} a_{ik}^2}$$

Measure of Sampling Adequacy (MSA) adalah indeks yang digunakan untuk menilai kecukupan sampel dalam analisis faktor dengan membandingkan koefisien korelasi parsial untuk setiap variabel. MSA memberikan gambaran mengenai sejauh mana data yang tersedia memadai untuk analisis faktor, dan memastikan bahwa variabel-variabel yang diteliti memiliki korelasi yang cukup kuat untuk melakukan ekstraksi faktor secara efektif (Baroroh, 2013).

$$MSA_i = \frac{\sum_{i \neq k} r_{ik}^2}{\sum_{i \neq k} r_{ik}^2 + \sum_{i \neq k} a_{ik}^2}$$

keterangan:
i = 1,2,...,p
k = 1,2,...,p
rik = Koefisien korelasi sederhana antara variabel ke-i dan ke-k
aik = Koefisien korelasi Parsial antara variabel ke-i dan ke-k

Definisi dan Variabel Operasional

Persepsi Keamanan Data

Persepsi adalah penilaian awal yang muncul dalam pikiran seseorang terhadap objek tertentu (Eid, 2011). Dalam konteks e-commerce, persepsi keamanan mengacu pada pandangan konsumen mengenai tingkat keamanan saat melakukan transaksi online. Menurut Eid (2011), persepsi keamanan mencerminkan keyakinan subjektif konsumen bahwa informasi pribadi mereka, baik dari aspek perdata maupun finansial, akan terlindungi dari akses, penyimpanan, dan manipulasi oleh pihak ketiga selama proses transaksi dan penyimpanan data, sehingga membangun ekspektasi kepercayaan diri konsumen secara konsisten. Sebagaimana dijelaskan oleh Armesh et al. (2010), persepsi keamanan sering kali dikaitkan dengan potensi ancaman yang dapat menyebabkan kerugian ekonomi melalui gangguan pada sumber data atau jaringan, modifikasi data, penolakan layanan, atau tindakan penipuan serta penyalahgunaan wewenang (Kinasih & Albari, 2012)

Menurut Roca et al. (2009) dan Armesh et al. (2010), persepsi keamanan dipahami sebagai potensi ancaman yang dapat menciptakan kondisi atau kejadian yang berisiko menimbulkan kesulitan ekonomi. Ancaman ini mencakup kerusakan data, pengumpulan dan modifikasi data, penolakan layanan, serta tindakan penipuan dan penyalahgunaan wewenang terhadap sumber data atau jaringan (Kinasih & Albari, 2012). Secara teknis, persepsi keamanan melibatkan jaminan terhadap integritas, kerahasiaan, otentikasi, dan tanpa pencatatan transaksi (Flavia'n dan Guinah'u, 2006). Dalam hal ini, integritas sistem informasi merujuk pada ketidakmampuan pihak ketiga untuk memodifikasi data yang ditransmisikan atau disimpan tanpa izin. Di sisi lain, kerahasiaan mencakup perlindungan

data agar hanya dapat diakses oleh individu yang memiliki otoritas yang sesuai (Kinasih & Albari, 2012).

Roca et al. (2009) juga menyebutkan bahwa keamanan mencakup penerapan kemajuan teknis yang dapat meningkatkan keinginan untuk melakukan pembelian secara online. Ini termasuk penggunaan teknologi kriptografi, tanda tangan digital, dan sertifikat digital yang dirancang untuk melindungi pengguna dari risiko penipuan, peretasan, atau "phishing" (Kinasih & Albari, 2012). Keamanan mencakup langkah-langkah perlindungan yang diambil untuk menjaga aset informasi dari setiap transaksi yang dilakukan antara konsumen dan perusahaan. Laudon (2016) menguraikan bahwa dalam konteks ini, informasi yang diberikan oleh perusahaan harus konsisten dengan produk dan layanan yang diterima oleh konsumen (Fermayani, 2022).

Persepsi Privasi Data

Konsep privasi sangat erat dengan konsep ruang personal dan teritorialitas. Ruang personal adalah ruang sekeliling individu, yang selalu dibawa kemana saja orang pergi, dan orang akan merasa terganggu jika ruang tersebut diinterfensi. Artinya, ruang personal terjadi ketika orang lain hadir, dan bukan semata-mata ruang personal, tetapi lebih merupakan ruang interpersonal. Pengambilan jarak yang tepat ketika berinteraksi dengan orang lain merupakan suatu cara untuk memenuhi kebutuhan akan privasi (Yuwinanto, 2017)

Privasi merupakan aspek yang amat rentan terhadap potensi penyalahgunaan oleh pihak-pihak yang tidak memiliki kepentingan yang sah. Privasi merupakan sebuah konsep yang erat hubungannya dengan informasi pribadi seperti biodata, foto, lokasi, video, dan data-data penting lainnya yang dimiliki oleh individu secara pribadi. Privasi merujuk pada data pribadi yang harus dijaga kerahasiannya oleh perusahaan dan tidak boleh disampaikan kepada pihak manapun dalam upaya melindungi informasi konsumen (Yuwinanto, 2017). Dalam konteks transaksi elektronik seperti registrasi online pada suatu event, privasi menjadi sangat rentan terhadap upaya peretasan oleh pihak yang tidak bertanggung jawab, yang dapat mengakibatkan kerugian bagi pengunjung event.

Semakin baik perusahaan EO menjaga privasi pengunjung, semakin besar kepercayaan dan niat pengunjung untuk melakukan transaksi secara online. Menurut ketentuan yang terdapat dalam Undang-Undang ITE Nomor 19 Tahun 2016 mengenai Perubahan terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, privasi merujuk pada data yang mengandung informasi elektronik atau dokumen lain yang merupakan bukti yang perlu dijaga integritas dan keutuhannya secara rahasia sesuai dengan ketentuan peraturan dan undang-undang. Pasal 43 ayat 2 dari undang-undang tersebut menegaskan bahwa perusahaan e-commerce wajib memperhatikan privasi konsumennya, dan apabila terjadi pelanggaran, perusahaan tersebut akan dikenai sanksi pidana (Fermayani, 2022).

Privasi merupakan faktor kunci yang dapat mempengaruhi minat pengguna dalam mengadopsi transaksi yang menggunakan sistem elektronik. Sehingga kemampuan organisasi dalam memperoleh, mengontrol, dan memanfaatkan serta menjaga informasi pribadi tersebut menjadi sangat penting dalam proses transaksi elektronik (Yuwinanto, 2017). Menurut Roca et al. (2009), persepsi privasi seseorang mengacu pada kemungkinan bahwa perusahaan online mengumpulkan dan menggunakan data tentang individu secara tidak pantas (Kinasih & Albari, 2012). Karena alasan tersebut, konsumen cenderung enggan untuk memberikan informasi pribadi mereka saat diminta oleh situs,

karena mereka merasa khawatir akan kemungkinan pengumpulan dan penyalahgunaan informasi yang dikirim melalui internet serta penggunaan yang tidak tepat terhadap data mereka.

Armesh et al. (2010) menyampaikan bahwa privasi dalam e-commerce merujuk pada sejauh mana individu bersedia untuk membagikan informasi melalui internet demi melakukan pembelian. Oleh karena itu, aspek-aspek yang perlu dievaluasi dalam hal privasi mencakup (Kinasih & Albari, 2012):

(1) keberadaan pernyataan privasi,

(2) kebijakan perusahaan terkait penjualan informasi pelanggan kepada pihak ketiga,

(3) penggunaan alat pelacak untuk mengumpulkan data pribadi.

Atas dasar kajian Pustaka diatas maka variable operasional pada penelitian ini tertuang pada table dibawah ini

Tabel 4 Variabel Operasioanl

Variable	**Dimensi**	**Indikator**	**Skala Pengukuran**
Perspesi Keamanan Data	Jaminan teknis keamanan jaringan transmisi	Data terenkripsi sebelum di transmisikan	Interval
		Jaringan menggunakan firewall level tertinggi sehingga sulit di bobol hacker	
		Jaringan telah menggunakan protocol keamanan tingkat tinggi seperti SSL/TLS	
	Jaminan teknis keamanan website	Menggunakan layanan atau perangkat lunak mitigasi serangan DDoS (Distributed Denial of Service)	
		Mengimplementasikan firewall aplikasi web untuk memantau dan mengontrol lalu lintas HTTP	
		Menggunakan protokol enkripsi seperti HTTPS	
	Jaminan keamanan saat melakukan transaksi finansial	Menerapkan otentikasi multi-faktor biasanya melalui kombinasi kata sandi, kode OTP (One-Time Password)	
		Menggunakan protokol keamanan seperti SSL/TLS untuk memastikan bahwa data yang ditransmisikan antara browser pengguna	

Variable	Dimensi	Indikator	Skala Pengukuran
		dan server web dienkripsi dengan aman.	
		Menggunakan firewall, sistem deteksi intrusi, dan solusi keamanan lainnya untuk melindungi sistem pembayaran online	
Perspesi Privasi Data	Jaminan hukum perlindungan data pribadi	Informasi yang jelas dan mudah dimengerti kepada pengguna tentang kebijakan privasi mereka, termasuk bagaimana data pribadi akan digunakan, disimpan, dan dilindungi.	
	Persetujuan dengan pelanggan dalam memberikan informasi data pribadi	Melakukan registrasi online harus memperoleh persetujuan yang jelas dan spesifik dari pengguna sebelum mengumpulkan atau menggunakan data pribadi	
	Kenyamanan layout saat memberikan data pribadi	Tampilan bersih dan susunan formulir berurutan	
		Layout website adaptif dapat menyesuaikan diri dengan berbagai perangkat dan ukuran layar	
	Ketenangan dalam memberikan data pribadi	Kepercayaan terhadap organisasi penyelenggara acara	
		Kejelasan dan transparansi penggunaan data pribadi	
		Adanya jaminan data pribadi tidak ada disalahgunakan	

Berdasarkan tabel operasional diatas maka variabel yang akan diteliti terdiri dari 20 variabel meliputi X1 = data terenkripsi, X2 = terlindungi firewall, X3 = protokol keamanan SSL/TLS, X4 = mitigasi serangan DDoS, X5 = firewal berbasis web, X6 = protokol HTTPS, X7 = otentifikasi multifactor, X8 = enkripsi browser dan server, X9 = pembayaran online terlindungi firewall, X10 = kebijakan privasi jelas dan mudah di mengerti, X11 = kemudahan navigasi antar menu, X12 = kecepatan merespons perintah, X13 = kelancaran proses registrasi, X14 = persetujuan pemanfaaan data pribadi, X15 = persetujuan jelas dan spesifik, X16 = interface bersih dan berurutan, X17 = layout website adaptif, X18 = tingkat kepercayaan terhadap penyelenggara acara, X19 = kejelasan

transparansi penggunaan data pribadi, X20 = jaminan data pribadi tdk akan disalahgunakan.

HASIL DAN PEMBAHASAN

Penelitian ini melibatkan 156 orang mahasiswa dengan rentang usia 19 – 30 tahun dari beberapa perguruan tinggi swasta ternama di wilayah Jakarta yang dipilih melalui metode *purposive random sampling*. Pemilihan mahasiswa sebagai responden didasarkan pada temuan survei pra-penelitian yang menunjukkan bahwa mahasiswa merupakan salah satu kelompok masyarakat yang memiliki minat tinggi dalam mengikuti berbagai acara, termasuk konser musik dan exhibition, di mana sebagian besar acara tersebut telah menerapkan sistem registrasi online. Sebanyak 156 responden yang berpartisipasi seluruhnya merupakan mahasiswa populasi muda yang terdiri atas Gen Y dan Gen Z dengan rentang usia 19 hingga 30 tahun. Dari jumlah tersebut, lebih dari 50% responden berusia antara 19 dan 20 tahun dan sisanya berada di rentang usia 21 – 30 tahun, dengan distribusi jenis kelamin sebanyak 64% wanita dan 36% pria. Jenis acara dengan menggunakan sistem registrasi online yang dihadiri oleh responden terdiri dari 41% seminar, 26% pameran atau exhibition, 25% konser musik, serta sisanya mencakup meeting, konferensi, rapat, dan kegiatan lainnya.

Metode pengumpulan data pada penelitian ini menggunakan teknik penyebaran angket dan wawancara yang melibatkan penggunaan google form untuk mengumpulkan informasi dari responden secara langsung serta proses wawancara mendalam kepada beberapa responden guna mendapatkan pemahaman mendetail melalui serangkaian pertanyaan terbuka yang dirancang sesuai tujuan penelitian namun juga memberikan fleksibilitas kepada responden untuk menjelaskan secara mendalam. Penelitian ini menggunakan 7 (tujuh) faktor utama yaitu; Jaminan teknis keamanan jaringan transmisi, Jaminan teknis keamanan website, Jaminan keamanan saat melakukan transaksi finansial, Jaminan hukum perlindungan data pribadi, Persetujuan dengan pelanggan dalam memberikan informasi data pribadi, Kenyamanan layout saat memberikan data pribadi, serta Ketenangan dalam memberikan data pribadi. Ketujuh faktor tersebut kemudian terbagi menjadi 20 (dua puluh) indikator. Keseluruh indikator tersebut direduksi menggunakan Analisa faktor sehingga membentuk faktor baru yang lebih tepat.

Untuk memperoleh faktor baru, langkah-langkah dalam analisis faktor meliputi: 1) penyusunan matriks data berupa matriks korelasi antara variabel-variabel asli, 2) ekstraksi faktor atau dekomposisi matriks data menjadi faktor-faktor, 3) rotasi faktor, dan 4) interpretasi faktor hasil rotasi. Syarat atau asumsi dalam analisis faktor adalah: 1) data yang dianalisis harus berdistribusi normal, 2) nilai Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO MSA) harus lebih besar dari 0,5, serta nilai Bartlett's Test of Sphericity (Sig) harus kurang dari 0,05, dan 3) terdapat hubungan atau korelasi yang kuat antar variabel, yang ditandai dengan nilai Anti-Image Correlation lebih besar dari 0,5..

Hasil output dari analisis menunjukkan nilai Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO MSA) sebesar 0,890 dan nilai Bartlett’s Test of Sphericity sebesar 0,00. Karena nilai KMO MSA melebihi ambang batas 0,5 dan nilai Bartlett’s Test of Sphericity kurang dari 0,05, maka ke-20 indikator yang digunakan memenuhi syarat dan layak untuk diproses lebih lanjut dengan analisis faktor. Selain itu, hasil uji Anti-Image Correlation menunjukkan bahwa semua 20 indikator memiliki nilai MSA lebih besar dari 0,50, sehingga seluruh indikator dapat dilanjutkan dalam analisis. Analisis faktor mengidentifikasi setidaknya empat faktor baru, masing-masing dengan nilai Eigen Value di atas 1,00.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.890
Bartlett's Test of Sphericity	Approx. Chi-Square	1.581E3
	df	190
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	7.066	35.332	35.332	6.629	33.147	33.147	4.534	22.669	22.669
2	3.453	17.266	52.598	3.027	15.136	48.283	4.350	21.748	44.417
3	1.195	5.974	58.572	.761	3.803	52.086	1.110	5.548	49.965
4	1.073	5.365	63.937	.575	2.877	54.963	1.000	4.998	54.963
5	.832	4.161	68.098						

Extraction Method: Principal Axis Factoring.

Interpretasi data Analisa Faktor

Hasil perhitungan analisa faktor mendapatkan empat faktor baru yang memiliki kesamaan karakteristik indikator, guna mendapatkan nama dari masing-masing faktor maka dilakukan wawancara mendalam dengan beberapa responden untuk memastikan apakah benar terdapat kesesuaian antar indikator dari ke empat faktor baru tersebut.

Faktor pertama diberi nama faktor jaminan sistem keamanan memiliki nilai Eigen Value sebesar 7.066 dengan nilai varians sebesar 22.70% terdiri dari 10 indikator meliputi data yang terenkripsi, jaringan terlindungi firewall, mitigasi serangan DDoS, implementasi firewall berbasis web, protocol HTTPS, otentifikasi multifactor, server terenkripsi, pembayaran online terfirewall, kebijakan privasi mudah dan jelas, serta kemudahan navigasi antar menu dengan nilai faktor loading terbesar 0.723 untuk indikator protocol HTTPS dan 0.702 untuk indikator otentifikasi multifactor.

Faktor kedua diberi nama tingkat kepercayaan proses registrasi memiliki nilai Eigen Value sebesar 3.453 dengan nilai varians sebesar 21.75% yang terdiri dari 7 indikator meliputi kelancaran proses registrasi, persetujuan yang jelas dan spesifik, interface website berurutan, layout website adaptif, kepercayaan terhadap EO, transparansi penggunaan data pribadi, serta jaminan data pribadi tidak akan disalahgunakan. Adapun faktor loading terbesar 0.829 merujuk indikator tingkat kepercayaan EO serta faktor loading sebesar 0.762 untuk indikator kelancaran proses registrasi pembelian tiket online.

Faktor ke tiga diberi nama Protokol Keamanan yang terbentuk memiliki nilai Eigen Value sebesar 1.195 dengan nilai varians sebesar 5.55% yang terdiri dari 2 indikator yaitu jaringan terlindungi firewall dan protocol keamanan SSL/TLS dengan nilai faktor loading tertinggi yaitu 0.585.

Faktor ke empat diberi nama persetujuan pemanfaatan data pribadi memiliki nilai Eigen Value sebesar 1.073 dengan varians sebesar 4.98% serta hanya memiliki 1 indikator yaitu persetujuan pemanfaatan data pribadi dengan nilai faktor loading 0.569.

Rotated Factor Matrix[a]

	Factor			
	1	2	3	4
data terenkripsi sebelum dikirim	.669			
jaringan terlindungi firewal			.444	
jaringan menggunakan tingkat tinggi protokol keamanan SSL/TLS			.585	
mitigasi serangan DDoS	.646			
mengimplementsikan firewal berbasis web	.555			
menggunakan protokol HTTPS	.723			
mengimplementasikan otentifikasi multifactor	.702			
data antara browser dengan server terenkripsi	.601			
pembayaran online terlindungi firewal	.584			
kebijakan privasi jelas dan mudah di mengerti	.674			
kemudahan navigasi antar menu	.682			
kecepatan merespons perintah	.573			
kelancaran proses registrasi		.762		
adanya persetujuan pemanfaaan data pribadi				.569
adanya persetujuan yang jelas dan spesifik		.731		
interface bersih dan berurutan		.675		
layout website adaptif		.758		
tingkat kepercayaan terhadap penyelenggara acara		.829		
kejelasan dan transparansi penggunaan data pribadi		.706		
adanya jaminan data pribadi tdk akan disalah gunakan		.695		

Extraction Method: Principal Axis Factoring.
Rotation Method: Varimax with Kaiser Normalization.

Nilai transformation matrix mengacu pada bobot atau koefisien yang menunjukkan seberapa besar pengaruh setiap faktor terhadap variabel yang dianalisis setelah rotasi dilakukan, dikatakan kuat jika memiliki nilai > 0,7 sementara dikatakan lemah jika nilai < 0,7. Dari keempat faktor yang terbentuk, faktor pertama menunjukkan nilai matriks transformasi sebesar 0,708. Faktor kedua memiliki nilai matriks transformasi sebesar -0,769, sedangkan faktor ketiga menunjukkan nilai sebesar 0,623, dan faktor keempat memiliki nilai sebesar 0,593. Hal ini menunjukkan faktor 1 memiliki pengaruh positif yang signifikan sementara faktor 2 memiliki pengaruh signifikan namun berlawanan. Sementara itu tetapi faktor 3 dan 4 walaupun memiliki pengaruh namun tidak terlalu kuat dan signifikan dikarenakan nilai matriks transformasinya < 0,70.

Factor Transformation Matrix

Factor	1	2	3	4
1	.708	.619	.251	.227
2	.613	-.769	.180	-.012
3	-.066	.106	.623	-.772
4	-.345	-.115	.719	.593

Extraction Method: Principal Axis Factoring.
Rotation Method: Varimax with Kaiser Normalization.

KESIMPULAN

Berdasarkan hasil analisis, terdapat empat faktor utama yang menjadi pertimbangan utama bagi pengunjung dalam menilai tingkat keamanan dan privasi data saat melakukan registrasi pembelian tiket secara online. Faktor-faktor tersebut meliputi: jaminan sistem keamanan, tingkat kepercayaan terhadap proses registrasi, protokol keamanan, serta persetujuan pemanfaatan data pribadi. Keempat faktor ini memiliki implikasi penting terhadap tingkat kepercayaan pengunjung dan keputusan mereka untuk menggunakan layanan penjualan tiket online dalam berpartisipasi pada suatu acara. Akan tetapi ketidak cermatan pengunjung event dalam membaca serta mempelajari *term and condition* serta pemberian izin pemanfaatan data pribadi pada saat melakukan registrasi online berpotensi menyebabkan terekspos nya data pribadi kepada aplikasi pihak ketiga atau vendor di luar acara yang diikuti.

Hasil analisis menunjukkan bahwa faktor-faktor seperti jaminan sistem keamanan, tingkat kepercayaan terhadap penyelenggara acara (Event Organizer/EO), serta kelancaran proses registrasi memiliki dampak signifikan terhadap persepsi pengunjung mengenai keamanan dan privasi data mereka. Sebaliknya, faktor protokol keamanan dan persetujuan pemanfaatan data pribadi menunjukkan pengaruh yang relatif kurang signifikan. Temuan ini mengindikasikan bahwa pengunjung tampaknya kurang memprioritaskan protokol keamanan yang diterapkan serta kurang memperhatikan perihal persetujuan syarat dan ketentuan terhadap penggunaan data pribadi mereka.

DAFTAR PUSTAKA

Adianto, A. (2022). *Bagaimana Imperva Bantu Amankan Website Java Jazz Festival 2022 Dari Bot Attack?*. Bluepower.com, Jakarta. Retrieved from https://www.bluepowertechnology.com/news-detail/bagaimana-imperva-bantu-amankan-website-java-jazz-festival-2022-dari-bot-attack

Baroroh, A. (2013). *Analisis Multivariat dan Time Series*. Jakarta: Elex Media Komputindo.

Busthomi, I., et al. (2020). *Optimasi Keamanan Informasi Pendaftaran Event Menggunakan Teknologi Blockchain*. Jurnal Ilmiah FIFO, 12(1). Retrieved from https://media.neliti.com/media/publications/458118-none-1dddfdc9.pdf

CNN Indonesia. (2023, July 20). *4 Kasus Kebocoran Data di Semester I 2023, Mayoritas Dibantah*. Retrieved from https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah

Esaunggul.ac.id. (2023, June 5). *Ancaman Cyber Crime Semakin Liar: Tiga Kasus Kebocoran Data Terbesar Yang Terjadi Di Indonesia*. Retrieved from https://fasilkom.esaunggul.ac.id/ancaman-cyber-crime-semakin-liar-tiga-kasus-kebocoran-data-terbesar-yang-terjadi-di-indonesia/

Febriari, S. (2023, July 19). *Deretan Kasus Kebocoran Data Pribadi di Indonesia Sepanjang 2022-2023*. Retrieved from https://www.metrotvnews.com/play/NA0CXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023

Fermayani, R., et al. (2022). *Analisis Pengaruh Privasi, Keamanan, Dan Kepercayaan Terhadap Niat Untuk Bertransaksi Secara Online Di Lazada*. Jurnal Menara Ekonomi, 8(1). Retrieved from https://jurnal.unej.ac.id/index.php/tourismjournal/article/download/37949/12743/

Javier, F. (2022, September 7). *Kebocoran Data, Bukti Keamanan Siber Indonesia yang Lemah*. Retrieved from https://data.tempo.co/data/1501/kebocoran-data-bukti-keamanan-siber-indonesia-yang-lemah

Kinasih, B. S., & Albari. (2012). *Pengaruh Persepsi Keamanan Dan Privasi Terhadap Kepuasan Dan Kepercayaan Konsumen Online*. Jurnal Siasat Bisnis, 16(1). Retrieved from https://journal.uii.ac.id/JSB/article/download/3912/3498/5670

Nabila. (2020, November 2). *Rekomendasi Platform Tempat Jual Tiket Event Online Tahun Ini*. Retrieved from https://www.loket.com/index.php/blog/platform-jual-tiket-event-online

Peña, P., & Mortada, L.-Z. (2016). *Will You Be Attending? How Event Apps Collect Your Data*. Berlin. Retrieved from https://ourdataourselves.tacticaltech.org/posts/24_events_conferences_1/

Romizal, A. (2023). *Persepsi Pengalaman Pengunjung Pameran terhadap Teknologi Self Service Registration*. Journal of Tourism and Creativity, 7(1). Retrieved from https://jurnal.unej.ac.id/index.php/tourismjournal/article/download/37949/12743/

Wibisono, Y. P., et al. (2019). *e-Vent: Support System for Event Registration*. Presented at ICAITI 2019, Bali. Retrieved from https://www.researchgate.net/publication/339093329_e-Vent_Support_System_for_Event_Registration

Yuwinanto, H. P. (2017). *Privasi Online dan Keamanan Data*. Jurnal Unair. Retrieved from https://journal.unair.ac.id/download-fullpapers-palim0d249692cafull.pdf