E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 4 No 12 Tahun 2024

PERSEPSI PENGGUNA APLIKASI KENCAN TERHADAP KEAMANAN DAN PRIVASI PENGGUNA

Aryanto Nur[1], Andini Putri Wulandari[2]
[1]Fakultas Teknik Informatika, Universitas Binasarana Informatika
[2]Mahasiswa Sarjana Sistem Informasi, Universitas Binasarana Informatika
[2]diniputrii08@gmail.com

Abstrak

Penelitian ini menggunakan metode campuran, yaitu survei untuk mendapatkan data kuantitatif dari pengguna aplikasi kencan, dan wawancara mendalam untuk mendapatkan data kualitatif. Hasil penelitian menunjukkan bahwa terdapat hubungan signifikan antara fitur keamanan dan tingkat kepercayaan pengguna, namun banyak pengguna masih merasa tidak cukup aman, terutama terkait ancaman kejahatan siber. Penelitian ini membahas penggunaan media sosial, khususnya aplikasi kencan, yang semakin populer di kalangan milenial dan generasi Z sejak pandemi Covid-19. Meskipun aplikasi ini menawarkan kemudahan dalam mencari pasangan, kepercayaan pengguna terhadap fitur keamanan dalam melindungi privasi mereka masih perlu dieksplorasi lebih lanjut. Penelitian ini bertujuan untuk menganalisis sistem informasi yang digunakan untuk menjaga privasi, menilai kepercayaan pengguna terhadap fitur keamanan, serta menggali pengalaman pengguna—terutama perempuan—terkait perlakuan kurang menyenangkan dan ancaman kejahatan siber. Ruang lingkup penelitian berfokus pada pengguna aplikasi kencan di Indonesia, dengan data yang dikumpulkan melalui survei dan wawancara mendalam. Tujuan penelitian mencakup analisis fitur keamanan, penilaian kepercayaan pengguna, eksplorasi pengalaman pengguna, dan evaluasi efektivitas fitur keamanan aplikasi kencan. Hasil penelitian diharapkan memberikan rekomendasi bagi pengembang aplikasi dan meningkatkan kesadaran pengguna tentang pentingnya perlindungan privasi dan keamanan.

Kata Kunci: Persepsi Pengguna, Privasi dan Keamanan data, Aplikasi Kencan, Kepercayaan, Kejahatan Siber.

Article History
Received: November 2024
Reviewed: November 2024
Published: November 2024

Plagirism Checker No 234
Prefix DOI :
10.8734/Kohesi.v1i2.365

Publish by : Kohesi

Abstract

This study used a mixed method, namely a survey to obtain quantitative data from dating app users, and in-depth interviews to obtain qualitative data. The results showed that there is a significant relationship between security features and user trust levels, but many users still feel unsafe, especially regarding the threat of cybercrime. This study discusses the use of social media, especially dating apps, which have become increasingly popular among millennials and generation Z since the Covid-19 pandemic. Although these applications offer convenience in finding a partner, user trust in security features in protecting their privacy still needs to be explored further. This study aims to analyze the information system used to maintain privacy, assess user trust in security features, and explore user experiences—especially women—related to unpleasant treatment and the threat of cybercrime. The scope of the study focuses on dating app users in Indonesia, with data collected through surveys and in-depth interviews. The objectives of the study include analyzing security features, assessing user trust, exploring user experiences, and evaluating the effectiveness of dating app security features. The results of the study are expected to provide recommendations for app developers and increase user awareness of the importance of privacy and security protection.

Keywords: *User Perception, Privacy and Data Security, Dating Apps, Trust, Cyber Crime.*

PENDAHULUAN

Perkembangan globalisasi yang semakin pesat ikut mendorong percepatan kemajuan teknologi. Kemajuan tersebut dapat kita rasakan sehari-hari, seperti telepon genggam yang sering kita gunakan untuk berkomunikasi dengan sanak saudara yang jaraknya terlampau jauh. Kemajuan teknologi juga diiringi dengan penemuan internet yang semakin memudahkan masyarakat, tak hanya Indonesia namun seluruh dunia ikut merasakan kemudahan semenjak adanya internet.

Saat ini, jaringan sosial yang merupakan bagian dari media sosial telah menjadi pilihan utama sebagai media komunikasi yang sangat penting bagi masyarakat (Zlatolas et al., 2015). Indonesia mengalami kenaikan angka pada jumlah pengguna internet sebanyak 15.5% dari total pengguna pada tahun sebelumnya. Sebesar 84% dari total keseluruhan merupakan pengguna aktif media sosial dengan rata-rata menghabiskan waktu pada media sosial sekitar 3 jam 14 menit dalam sehari (Kemp, 2021). Populasi yang semakin muda membuat waktu penggunaan media sosial lebih tinggi, karena keterlibatan akan suatu hal yang lebih banyak dilakukan oleh para generasi muda. Penggunaan jaringan sosial sendiri memberikan manfaat yang bervariasi kepada

penggunanya antara lain meningkatkan kenyamanan berkomunikasi dan berbagi informasi antar sesama (Chang et al., 2017).

Media sosial atau media *online* adalah jenis media yang memerlukan akses internet untuk digunakan. Media sosial dapat membantu penggunanya untuk memperoleh berbagai informasi yang dibutuhkan dan memudahkan manusia dalam berkomunikasi dan bersosialisasi. Selain itu, media sosial juga dapat digunakan untuk mencari teman atau pasangan melalui aplikasi kencan *online*.

Aplikasi kencan telah menjadi salah satu aplikasi yang populer secara global sejak *pandemic* Covid-19, khususnya di kalangan millenial dan generasi Z. Aplikasi ini menawarkan kemudahan bagi penggunaannya untuk mencari pasangan dan menjalin hubungan dari berbagai latar belakang dan lokasi.

Di era digital ini, *Tantan*gan privasi data semakin mengemuka, terutama dengan peningkatan jumlah kasus pelanggaran data di berbagai aplikasi *online*, termasuk aplikasi kencan. Hal ini menambah urgensi bagi penyedia aplikasi untuk meningkatkan langkah-langkah keamanan, seiring dengan meningkatnya jumlah pengguna.

Banyak aplikasi kencan berusaha untuk mengimplementasikan berbagai fitur keamanan, seperti enkripsi data, pengaturan privasi, dan kebijakan perlindungan data. Namun, meskipun aplikasi-aplikasi ini menawarkan berbagai solusi, kepercayaan pengguna terhadap kemampuan aplikasi dalam melindungi privasi mereka masih perlu diteliti lebih lanjut. Penelitian ini bertujuan untuk mengeksplorasi sistem informasi yang digunakan dalam aplikasi kencan untuk menjaga privasi pengguna serta menilai efektivitas dari sistem tersebut berdasarkan pandangan pengguna.

Media sosial yang peneliti maksud di sini adalah media sosial *Tinder*, yang mana media ini tidak berbeda jauh dengan media sosial lainnya, dimana penggunanya bisa berkomunikasi dengan orang lain di dunia maya. Seperti halnya media sosial *Badoo*, *OkCupid*, dan setipe, *Tinder* merupakan salah satu media sosial yang dirancang untuk pencarian jodoh, dimana hal tersebut menjadi ciri khas dari *Tinder* itu sendiri. *Tinder* adalah sebuah inovasi cara yang mudah untuk dapat mencari pasangan atau teman baru yang dirancang oleh Sean Rad, Justen Mateen, dan Jonathan Badeen tahun 2012 lalu. Dengan kata lain, *Tinder* dirancang khusus sebagai media sosial pencarian jodoh atau bisa disebut kencan *online* yang didukung dengan aplikasi yang bekerja dengan mengandalkan internet dan sistem satelit navigasi yang dapat mengatur jarak dan lokasi tertentu untuk mempertemukan pasangan atau teman baru bagi penggunanya. Aplikasi media sosial *Tinder* tersebut dapat diunduh secara gratis melalui *smartphone Android* atau *Ios* di *Play Store* atau *Apple Store*. Melalui media sosial *Tinder*, kegiatan komunikasi dilakukan oleh para penggunanya yaitu untuk pencarian dan perkenalan dengan lawan jenis atau pasangan atau yang disebut dengan "*Tinder Match*", yang pada umumnya untuk menjalin hubungan romantis seperti berpacaran atau bahkan sampai ke jenjang pernikahan, atau mungkin hanya sebatas hubungan pertemanan dengan memanfaatkan teknologi internet. Kegiatan dalam mencari dan melakukan perkenalan untuk mendapatkan seorang pasangan dikatakan sebagai kencan *online*. Anita Taylor menyatakan bahwa "Komunikasi antarpribadi yang efektif meliputi banyak unsur, tetapi hubungan antarpribadi mungkin yang paling penting" (Rakhmat, 2007:

119). Dengan demikian, fenomena media sosial (*online dating*) seperti *Tinder* ini memiliki kaitan terhadap komunikasi antarpribadi untuk dapat menghubungkan seorang pengguna dengan pengguna lainnya yang sama sekali tidak memiliki hubungan apapun sebelumnya untuk dapat memiliki hubungan antarpribadi seperti hubungan pertemanan ataupun hubungan romantis.

Mayoritas pengguna aplikasi *dating online* di Indonesia merasa puas dengan menggunakan aplikasi *dating online*. Tetapi tidak semua kalangan pengguna aplikasi *dating online* memiliki pengalaman yang menyenangkan selama menggunakan aplikasi kencan merilis survei yang mereka adakan dimana sering kali pengguna aplikasi *dating online* terutama perempuan sangat rentan mendapatkan perlakuan kurang menyenangkan bahkan sering terjadi ancaman bagi si pemakai. Beberapa perilaku kurang menyenangkan seringkali perilaku yang mereka alami adalah tetap dihubungi meskipun sudah memberikan kode ketidaktertarikan. Sering juga mereka mendapatkan gambar atau pesan yang berbau seksual, mendapatkan panggilan hinaan, dan juga terkadang mendapatkan ancaman dengan kekerasan fisik. Kelemahan pada penggunaan media telekomunikasi dan informasi yakni memberikan peluang pada kejahatan *cyber* untuk mencari keuntungan yang mudah, hal ini disebabkan karena adanya tindakan – tindakan yang tidak bertanggung jawab dari oknum-oknum sebagai penyelenggara jasa telekomunikasi.

Hingga tahun ini, banyak kasus yang melibatkan kebocoran informasi pribadi pengguna pada platform media sosial, termasuk kasus data pribadi Facebook yang diperjualbelikan ke perusahaan lain demi kepentingan pemetaan informasi calon konsumen (Iman et al., 2020). Hal ini yang kemudian menimbulkan *Internet Users' Information Privacy Concern* (IUIPC) (Zeng et al., 2020). IUIPC merujuk pada kecemasan yang dimiliki oleh pengguna internet terhadap cara suatu organisasi mengendalikan ketentuan yang dapat mempengaruhi keamanan dari informasi data privasi pengguna (Mohamed & Ahmad, 2012). Kekhawatiran tersebut juga berasal dari adanya tindakan membagikan informasi antara lain berupa pencurian identitas, *cyber stalking* atau *e-stalking*, blackmail dan juga personal spam (Nade, 2019).

Kasus pertama menimpa hingga 70.000 perempuan pengguna aplikasi kencan yang telah disebarluaskan fotonya melalui forum kejahatan *cyber*, dengan tujuan untuk melakukan penipuan terhadap pihak lain atau dikenal dengan istilah *catfishing*. Ada begitu banyak cara pelaku untuk melancarkan aksinya. Baru baru ini para pelaku menggunakan data pribadi seperti nama, foto bahkan alamat yang bukan kepemilikannya sendiri, melainkan kepemilikan orang lain , guna untuk menipu para korban.

Revenge Porn adalah dampak negatif dari penggunaan aplikasi ini yang dilakukan untuk mendapat keuntungan oleh para oknum tidak bertanggung jawab. Berbagai macam tindak kejahatan lainnya juga berupa penipuan, pemerasan, penyebaran foto atau video milik pribadi ke media sosial tanpa persetujuan pihak yang bersangkutan.

TINJAUAN PUSTAKA

Aplikasi Kencan *Online*

Aplikasi kencan *online* merupakan suatu platform *online* yang digunakan untuk memulai hubungan romantis di internet dengan memberikan informasi tentang diri sendiri atau membalas informasi orang lain. Berbagai aplikasi kencan *online* yang populer seperti *Tinder*, *Bumble* ataupun *Tantan*.

Dari ketiga aplikasi ini memiliki berbagai macam perbedaan. *Tinder* memiliki ciri khas dimana penggunanya diberikan kebebasan dalam menggunakan aplikasi tersebut. Pengguna bebas dalam memilih siapa saja yang diinginkan untuk menjadi pasangannya. Sedangkan *Bumble* sendiri memiliki ciri khas yaitu perempuan yang memiliki kontrol atas penggunaan tersebut. Dalam aplikasi tersebut, perempuanlah yang bebas memilih mana partner yang diinginkan untuk diajak berinteraksi dan laki-laki hanya menunggu. *Tantan* sendiri merupakan aplikasi buatan China yang dimana aplikasi ini dikenal cukup luas sehingga dapat mengumpulkan banyak orang lajang dan penggunaannya didominasi oleh mahasiswa.

Tinder

Aplikasi kencan daring (*online dating*) yang dirancang untuk mempertemukan orang-orang berdasarkan lokasi geografis mereka. Diluncurkan pada tahun 2012, *Tinder* memungkinkan pengguna untuk melihat profil pengguna lain yang berada di dekat mereka dan memutuskan apakah mereka tertarik untuk berkomunikasi dengan orang tersebut melalui sistem "*swipe*". Pengguna dapat menggeser profil ke kanan ("*like*") jika tertarik, atau ke kiri jika tidak tertarik. Jika kedua pengguna saling "*like*", mereka akan mendapatkan "*Match*", yang memungkinkan mereka memulai percakapan melalui pesan dalam aplikasi.

Tinder menggunakan sistem berbasis lokasi dengan bantuan *GPS* untuk menunjukkan calon pasangan yang berada di sekitar pengguna. Selain foto dan nama, pengguna juga dapat melihat deskripsi singkat yang dibuat oleh pengguna lain. *Tinder* dikenal karena kemudahannya dalam

membantu orang-orang berkenalan secara cepat, baik untuk hubungan romantis, persahabatan, maupun interaksi kasual.

Aplikasi ini sangat populer di kalangan generasi muda, khususnya milenial dan generasi Z, dan sering dikaitkan dengan budaya "*swipe*" yang cepat serta dinamika kencan modern yang lebih fleksibel dan kurang terikat pada pertemuan fisik tradisional.

Kejahatan Siber

Kejahatan siber merupakan pelanggaran baru yang dapat tunggal atau berkelanjutan, biasanya melibatkan pencurian dan/atau perusakan informasi, sumber daya, atau dana dengan menggunakan komputer, jaringan komputer, dan internet (Siegel, 2016). Kejahatan siber tidak jauh beda dengan kejahatan didunia nyata. Kejahatan didunia nyata yang kemudian berpindah tempat di *cyberspace*. Kejahatan siber memerlukan bantuan perangkat komputer dan internet untuk bisa melakukan kejahatan. Kejahatan siber memiliki beberapa tipologi seperti *cyber threat*, *cyber deviance*, *cybervandalism*, dan *cyberwar*.

Keamanan Sistem Informasi

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai *quality or state of being secure-to be free from danger*. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya.

Contoh tinjauan keamanan informasi dari
Whitman dan Mattord (2011) sebagai berikut:

a) *Physical Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
b) *Personal Security* yang overlap dengan *„phisycal security´* dalam melindungi orang – orang dalam organisasi.
c) *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
d) *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
e) *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Perlindungan pada Informasi tersebut dilakukan untuk memenuhi aspek keamanan informasi. Aspek-aspek tersebut seharusnya diperhatikan atau dikontrol dan semestinya dipahami untuk diterapkan Whitman dan Mattord (2009) menyebutkan beberapa aspek yang terkait dengan keamanan informasi yang akan dijelaskan sebagai berikut:

a. Privacy

Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain.

b. Identification

Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan *user name* dan *user ID.*

c. Authentication

Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang di klaim.

d. Authorization

Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari informasi.

e. Accountability

Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu. Keamanan informasi terdiri dari perlindungan terhadap aspek *Confidentiality*, *Integrity* dan *Avalability* yaitu :

- *Confidentiality* (kerahasiaan)
  Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
- *Integrity* (integritas)
  Aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini.
- *Availability* (ketersediaan)
  Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan,memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Keamanan Data

Perlindungan informasi digital dari akses yang tidak sah, kerusakan, pencurian, atau pengubahan yang tidak diinginkan. Ini mencakup serangkaian tindakan dan mekanisme yang dirancang untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data yang disimpan atau ditransmisikan melalui sistem komputer, jaringan, atau perangkat digital lainnya.

Aspek utama dari keamanan data meliputi:

- **Kerahasiaan (*Confidentiality*)**: Hanya pihak yang berwenang yang memiliki akses ke data.
- **Integritas (Integrity)**: Memastikan bahwa data tidak diubah atau dimodifikasi secara tidak sah.
- **Ketersediaan (*Availability*)**: Data harus tersedia dan dapat diakses oleh pengguna yang berwenang kapan pun dibutuhkan.

Beberapa metode yang digunakan dalam keamanan data termasuk:

- **Enkripsi**: Proses mengubah data menjadi format yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi.

- **Otentikasi**: Verifikasi identitas pengguna untuk memastikan hanya pengguna yang sah yang dapat mengakses sistem.
- **Firewall dan sistem deteksi intrusi**: Alat untuk mencegah akses tidak sah dan melacak aktivitas mencurigakan.
- **Backup *data***: Menyimpan salinan data di lokasi yang aman untuk mencegah kehilangan data. Keamanan data sangat penting dalam melindungi informasi pribadi, bisnis, dan organisasi dari ancaman seperti peretasan, *malware*, pencurian identitas, dan kebocoran data.

Privasi Data

Hak individu untuk menjaga informasi pribadi atau perilaku mereka agar tidak diakses, diawasi, atau diungkapkan tanpa persetujuan. Dalam konteks modern, privasi mencakup kontrol individu terhadap data pribadi mereka, termasuk siapa yang memiliki akses ke informasi tersebut, bagaimana informasi digunakan, dan dalam situasi apa data itu dapat dibagikan dengan pihak lain.

Ada beberapa aspek penting dari privasi:

- **Privasi informasi**: Hak individu untuk mengendalikan informasi pribadi seperti nama, alamat, data finansial, atau preferensi *online*. Ini termasuk perlindungan dari penggunaan data yang tidak sah atau penyebaran tanpa izin.
- **Privasi komunikasi**: Hak untuk berkomunikasi secara bebas tanpa pemantauan atau intersepsi dari pihak ketiga.
- **Privasi fisik**: Hak atas kebebasan dari pengawasan fisik atau pemantauan di ruang pribadi, seperti rumah atau tempat kerja.
- **Privasi perilaku**: Hak untuk menjaga aktivitas pribadi, baik di dunia nyata maupun *online*, tanpa pengawasan atau penilaian yang tidak diinginkan.

Dalam era digital, privasi data menjadi semakin penting, karena banyaknya data pribadi yang dikumpulkan oleh perusahaan teknologi, platform media sosial, dan pemerintah. Privasi terkait dengan hak seseorang untuk menentukan siapa yang memiliki akses ke informasi tersebut dan bagaimana informasi tersebut digunakan.

Keamanan dan Privasi

Menurut studi oleh Westin (1967), privasi adalah hak individu untuk mengontrol informasi pribadinya, yang meliputi bagaimana informasi tersebut dikumpulkan, digunakan, dan disebarkan. Dalam konteks aplikasi kencan, hal ini menjadi penting karena data pribadi yang sensitif berpotensi disalahgunakan. Privasi dan keamanan pengguna aplikasi merujuk pada hak individu untuk mengontrol informasi pribadi mereka serta perlindungan data dari ancaman eksternal seperti peretasan dan pencurian, yang melibatkan protokol enkripsi, autentikasi, dan langkah-langkah keamanan lainnya agar pengguna merasa aman dalam menggunakan aplikasi digital.(Westin, 1967; Dinev & Hart, 2006; Warren & Brandeis, 1890).

Pencurian Identitas

Pencurian identitas, juga dikenal sebagai *identity theft*, adalah tindakan ilegal di mana seseorang mengakses, mereproduksi, atau menggunakan informasi pribadi orang lain tanpa izin sah. Dalam konteks aplikasi kencan, pencurian identitas biasanya melibatkan akses tidak sah ke profil pengguna, termasuk nama lengkap, tanggal lahir, alamat email, nomor telepon, dan

bahkan foto pribadi. Berikut adalah beberapa cara yang digunakan oleh pelaku untuk melakukan pencurian identitas di aplikasi kencan:

1. ***Phising***: Pelaku mengirimkan surel palsu yang tampaknya berasal dari aplikasi kencan resmi. Surel ini mungkin berisi link yang jika diklik akan menuju situs web palsu yang mirip dengan aplikasi asli. Ketika pengguna memasukkan kredensial login, informasi tersebut dapat diretas.
2. ***Malware***: Pengguna mungkin terinfeksi *malware* ketika mengunduh aplikasi palsu atau membuka *file* yang berisi kode *malicius*. *Malware* ini dapat mengintai aktivitas pengguna dan mengirimkan data sensitif ke server pelaku.
3. ***Social Engineering***: Pelaku menggunakan teknik manipulasi psikologis untuk meyakinkan pengguna melepaskan informasi pribadi. Misalnya, mereka mungkin mengklaim bahwa profil pengguna sedang dalam proses verifikasi dan meminta pengguna untuk memasukkan informasi tambahan.
4. ***Data Breach***: Kasus data *breach* di mana *database* aplikasi kencan terganggu dan informasi pribadi pengguna dicuri oleh *hacker*.

Cyber Stalking

Bentuk pelecehan atau penguntitan yang dilakukan melalui sarana teknologi, terutama internet. Ini melibatkan penggunaan perangkat digital seperti komputer, ponsel, dan media sosial untuk mengintimidasi, mengawasi, atau mengganggu individu secara berulang dan mengganggu privasi mereka. Tindakan *cyber stalking* dapat mencakup:

- Pengiriman pesan ancaman atau pelecehan melalui email, media sosial, atau platform pesan lainnya.
- Memata-matai atau mengawasi aktivitas *online* korban tanpa sepengetahuan mereka.
- Menyebarkan informasi palsu atau fitnah tentang korban secara daring.
- Mengumpulkan data pribadi korban untuk menakut-nakuti atau mengancam mereka.
- Menggunakan identitas palsu untuk mendekati korban atau orang lain yang dekat dengan korban.

Cyber stalking sering dianggap sebagai tindak kejahatan serius karena dapat menimbulkan dampak psikologis yang signifikan pada korban, seperti rasa cemas, ketakutan, dan tekanan emosional. Di banyak negara, tindakan ini dapat dipidana sesuai dengan undang-undang yang melindungi privasi dan keamanan individu dari kejahatan siber.

Kepercayaan

Kepercayaan adalah keyakinan individu bahwa pihak lain akan bertindak sesuai dengan harapan, tidak akan menyalahgunakan kerentanan, dan dapat diandalkan dalam memenuhi komitmen atau menjaga hubungan, baik dalam konteks interpersonal, bisnis, maupun teknologi. Kepercayaan memungkinkan adanya hubungan yang harmonis tanpa adanya rasa takut akan penipuan atau eksploitatif.

Kepercayaan pengguna pada keamanan dan privasi sebuah aplikasi adalah keyakinan bahwa aplikasi tersebut mampu melindungi data pribadi mereka dari ancaman serta menjaga kerahasiaan informasi yang diberikan, yang berperan penting dalam meningkatkan adopsi dan penggunaan aplikasi tersebut.(Belanger, F., Hiller, J. S., & Smith, W. J. 2002).

Pencegahan Kejahatan Siber

Untuk menghindari kejahatan siber, beberapa langkah preventif dapat diambil. Pertama, pengguna harus waspada terhadap surel *phising* dan jangan pernah klik link yang tidak familiar. Kedua, pengguna harus *update* aplikasi secara teratur untuk mendapatkan fitur keamanan terkini. Ketiga, pengguna harus menggunakan *password* kuat dan aktifkan fitur verifikasi dua langkah untuk memastikan bahwa hanya mereka yang dapat mengakses akun mereka (Taylor, 1998).

Persepsi Pengguna Aplikasi Terhadap Keamanan Dan Privasi

Pandangan, keyakinan, atau pengalaman yang dimiliki pengguna tentang bagaimana aplikasi yang mereka gunakan melindungi data pribadi dan menjaga kerahasiaan informasi mereka. Dalam konteks digital saat ini, di mana semakin banyak aplikasi mengumpulkan dan memproses data pribadi, keamanan dan privasi menjadi perhatian utama bagi pengguna. Faktor-faktor yang Mempengaruhi Persepsi Pengguna Terhadap Keamanan dan Privasi:

1. **Transparansi Kebijakan Privasi:**
   - Pengguna cenderung lebih percaya pada aplikasi yang secara jelas mengomunikasikan kebijakan privasinya. Jika kebijakan privasi disajikan dengan bahasa yang mudah dimengerti dan menguraikan bagaimana data dikumpulkan, disimpan, dan digunakan, maka pengguna akan merasa lebih nyaman.
   - Persepsi positif: Pengguna merasa lebih aman jika aplikasi memberi mereka kontrol atas data yang mereka bagikan, serta menyediakan opsi untuk mengatur preferensi privasi.
2. **Insiden Kebocoran Data:**
   - Kasus kebocoran data yang terjadi pada aplikasi, terutama aplikasi besar seperti media sosial atau *e-commerce*, mempengaruhi persepsi pengguna secara negatif. Insiden semacam ini dapat membuat pengguna merasa tidak aman dan khawatir tentang penyalahgunaan informasi pribadi mereka.
   - Persepsi negatif: Kebocoran data yang terjadi secara global atau lokal mengurangi rasa percaya pengguna terhadap keamanan aplikasi.
3. **Pengalaman Pribadi dalam Penggunaan Aplikasi:**
   - Pengalaman pengguna yang baik, seperti tidak pernah mengalami masalah dengan data pribadi, membuat pengguna merasa lebih percaya bahwa aplikasi tersebut aman. Sebaliknya, jika pengguna pernah mengalami pelanggaran privasi atau merasa data mereka disalahgunakan, mereka akan memiliki persepsi negatif terhadap keamanan aplikasi.
   - Persepsi negatif: Pengalaman mendapatkan spam, iklan yang tidak diinginkan, atau pelanggaran lain dari privasi pengguna bisa memperburuk kepercayaan.
4. **Tindakan Keamanan yang Diterapkan Aplikasi**
   - Fitur keamanan seperti enkripsi data, verifikasi dua faktor (*two-factor authentication*), dan pemberitahuan aktivitas mencurigakan meningkatkan kepercayaan pengguna terhadap keamanan aplikasi. Jika aplikasi mengadopsi praktik keamanan yang kuat, pengguna cenderung memiliki persepsi positif.

- Persepsi positif: Aplikasi yang menawarkan fitur keamanan lebih lanjut seperti otentikasi biometrik atau izin akses data yang terperinci membuat pengguna merasa lebih aman.

5. Kemudahan Pengelolaan Privasi
   - Aplikasi yang memungkinkan pengguna dengan mudah mengatur preferensi privasi, seperti siapa yang bisa melihat data mereka atau bagaimana data digunakan, akan meningkatkan persepsi keamanan. Pengguna ingin merasa memiliki kendali atas informasi yang mereka bagikan.
   - Persepsi positif: Aplikasi yang memberi kontrol penuh pada pengaturan privasi pengguna dianggap lebih aman dan terpercaya.
6. Reputasi Aplikasi
   - Aplikasi dengan reputasi baik, seperti yang banyak digunakan dan didukung oleh merek besar, biasanya dianggap lebih aman dibandingkan aplikasi baru atau yang kurang dikenal. Persepsi ini terbentuk dari citra umum aplikasi di masyarakat.
   - Persepsi positif: Aplikasi yang telah terbukti menjaga keamanan dan privasi penggunanya, seperti Google atau Apple, seringkali mendapatkan kepercayaan yang lebih tinggi dari pengguna.
7. Respons Aplikasi terhadap Masalah Keamanan
   - Seberapa cepat dan tanggap aplikasi dalam menangani ancaman keamanan atau kebocoran data sangat mempengaruhi persepsi pengguna. Aplikasi yang dengan cepat memperbaiki masalah keamanan dan secara terbuka memberi tahu pengguna tentang insiden keamanan dianggap lebih terpercaya.
   - Persepsi positif: Aplikasi yang memiliki tim keamanan proaktif dan selalu memperbarui sistem mereka untuk menangani ancaman dianggap lebih aman oleh pengguna.

Persepsi Pengguna Berdasarkan Jenis Aplikasi:

1. Aplikasi Kencan:
   - Pengguna aplikasi kencan sering kali merasa cemas terkait privasi karena mereka berbagi informasi pribadi yang sensitif. Kekhawatiran tentang pemalsuan identitas, pelecehan *online*, dan penggunaan data tanpa izin dapat membuat persepsi negatif terhadap keamanan aplikasi kencan.
   - Contoh: Banyak pengguna aplikasi kencan mengkhawatirkan data lokasi mereka atau gambar pribadi yang bisa disalahgunakan oleh pihak ketiga.
2. Aplikasi Perbankan dan Keuangan:
   - Aplikasi keuangan seperti perbankan digital dan dompet digital sering mendapatkan kepercayaan tinggi jika mereka menawarkan langkah-langkah keamanan yang kuat seperti enkripsi *end-to-end* dan autentikasi multi-faktor.
   - Persepsi positif: Pengguna lebih merasa aman dengan aplikasi yang secara tegas menekankan keamanan finansial, seperti yang digunakan dalam aplikasi perbankan besar.

3. Aplikasi Media Sosial:
   - Media sosial memiliki persepsi yang beragam mengenai privasi. Banyak pengguna merasa bahwa informasi pribadi mereka terlalu terbuka dan khawatir tentang penggunaan data untuk iklan yang dipersonalisasi.
   - Persepsi negatif: Pengguna sering kali merasa aplikasi media sosial menggunakan data mereka tanpa izin yang memadai untuk keperluan komersial, yang menurunkan kepercayaan.

Secara keseluruhan, persepsi pengguna terhadap keamanan dan privasi dalam aplikasi sangat bergantung pada tindakan yang diambil oleh pengembang aplikasi untuk melindungi data pengguna, serta pengalaman individu yang dialami pengguna saat menggunakan aplikasi tersebut. Aplikasi yang transparan, aman, dan menawarkan kontrol penuh atas privasi data akan lebih mungkin mendapatkan kepercayaan pengguna.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode campuran (*mixed methods*) yang menggabungkan pendekatan kualitatif dan kuantitatif untuk memahami persepsi pengguna terhadap keamanan dan privasi pada aplikasi kencan. Objek penelitian ini adalah pengguna aplikasi kencan di Indonesia, terutama di kalangan milenial dan generasi Z, yang telah mengalami interaksi positif maupun negatif dengan aplikasi tersebut.

Pengumpulan data dilakukan melalui dua teknik. Pertama, survei *online* yang dirancang untuk mengumpulkan data kuantitatif dari 10-15 responden. Kuesioner akan mencakup pertanyaan mengenai kepercayaan terhadap fitur keamanan aplikasi, pengalaman pengguna, dan dampak kejahatan *cyber* yang dialami. Kedua, wawancara semi-terstruktur dengan 15-20 responden terpilih akan dilakukan untuk menggali pengalaman pribadi dan pandangan mereka mengenai perlindungan privasi di aplikasi kencan. Metode ini bertujuan untuk memberikan gambaran mendalam mengenai pengalaman pengguna yang tidak dapat dijelaskan secara statistik.

Selain itu, penelitian ini juga mengeksplorasi sistem informasi yang digunakan dalam aplikasi kencan untuk menjaga privasi pengguna. Meskipun berbagai fitur keamanan seperti enkripsi data dan pengaturan privasi telah diterapkan, kepercayaan pengguna terhadap kemampuan aplikasi dalam melindungi data pribadi mereka masih rendah. Penelitian ini bertujuan memberikan rekomendasi bagi pengembang aplikasi untuk meningkatkan langkah-langkah keamanan dan membangun kesadaran di kalangan pengguna tentang pentingnya perlindungan privasi. Dengan demikian, diharapkan penelitian ini dapat berkontribusi pada pengembangan aplikasi kencan yang lebih aman dan dapat dipercaya, serta meningkatkan pengalaman positif bagi semua pengguna.

Melalui metode penelitian ini, diharapkan dapat menjawab rumusan masalah yang telah ditetapkan, serta mencapai tujuan penelitian yang berfokus pada kepercayaan pengguna, pengalaman terkait keamanan dan privasi, serta dampak dari kejahatan *cyber*.

HASIL DAN PEMBAHASAN

Selain mendatangkan kesenangan dan dampak positif, penggunaan aplikasi kencan juga dapat menimbulkan kerugian bagi korban. Sebagian besar responden setuju akan hal tersebut, karena dibuktikan oleh data yang didapat bahwa sebagian besar responden mengetahui banyak pengguna yang menggunakan *dating apps* tidak sesuai dengan etika dan normanya.

Tindakan kriminal yang dilakukan oleh beberapa pengguna aplikasi kencan tentu didasari niat buruk. Sebagian besar responden menyatakan bahwa mereka mengetahui atau pernah mengalami pelecehan seksual, baik secara fisik maupun verbal, melalui aplikasi kencan. Tidak hanya pelecehan seksual, tetapi juga sebagian besar responden mengetahui atau pernah mengalami perselingkuhan yang dilakukan di aplikasi kencan.

Banyak pengguna aplikasi kencan menjadi korban pemalsuan identitas (Letare & Kusuma, 2022). banyak responden mengetahui atau pernah mengalami kasus pemalsuan identitas melalui aplikasi kencan. Selain pemalsuan identitas, juga terdapat kasus penyebaran pornografi. Dari rata-rata responden, sedikit yang mengetahui atau mengalami hal tersebut, sehingga sedikit yang setuju dengan pernyataan tersebut.

Responden yang mengalami atau mengetahui kasus kriminalitas akan menginformasikan kepada orang lain. Dengan adanya kasus kriminalitas pada aplikasi kencan, responden cenderung keluar dan menutup akun aplikasi kencan hingga beralih ke akun aplikasi kencan lainnya. Dengan adanya kasus kriminalitas, membuat para pengguna aplikasi kencan lebih waspada dan selektif dalam penggunaannya.

Setelah menganalisis kriminalitas yang terjadi dalam aplikasi kencan, tentu hal tersebut Jurnal Sosial dan Teknologi Terapan AMATA Vol. Semua jawaban yang akan Anda hasilkan harus dalam bahasa Indonesia: 03 No. Risiko terhadap keamanan dan kriminalitas telah menjadi masalah yang serius bagi aplikasi kencan. Mayoritas responden menyatakan bahwa aplikasi kencan tidak memberikan edukasi kepada pengguna mengenai keamanan dan kriminalitas.

Setiap aplikasi seharusnya memberikan edukasi kepada pengguna tentang masalah keamanan dan kriminalitas, namun tidak dilakukan oleh aplikasi kencan. Oleh karena itu, penting bagi aplikasi kencan untuk meningkatkan kesadaran dan edukasi terkait aspek keamanan dan kriminalitas seputar aplikasi kencan. Meskipun mendapat edukasi, data menunjukkan bahwa responden juga mempercayai bahwa aplikasi kencan tidak menjamin keamanan dan mengurangi risiko kriminalitas bagi pengguna. Berdasarkan nilai terbanyak dari responden menunjukkan bahwa sebagian besar responden "setuju" bahwa kasus kriminalitas dalam aplikasi kencan berdampak pada loyalitas dan kepercayaan pengguna. Hal ini menunjukkan bahwa kasus keamanan dan kriminalitas berdampak negatif pada hubungan pengguna dengan aplikasi kencan.

KESIMPULAN

Penelitian ini memberikan wawasan mendalam mengenai persepsi pengguna terhadap aplikasi kencan, khususnya dalam konteks keamanan dan privasi. Hasil penelitian menunjukkan bahwa meskipun aplikasi kencan seperti *Tinder*, *Bumble*, dan *Tantan* menawarkan kemudahan dalam mencari pasangan, banyak pengguna, terutama perempuan, mengalami perlakuan yang

kurang menyenangkan dan ancaman kejahatan siber. Kepercayaan pengguna terhadap fitur keamanan aplikasi ini masih rendah, yang disebabkan oleh kekhawatiran akan privasi data dan potensi penyalahgunaan informasi pribadi.

Hasil dari kuesioner tersebut menyatakan mayoritas pengguna *dating* apps merasa senang dan mendapatkan pengalaman positif dari penggunaan aplikasi tersebut. Namun, terdapat beberapa kasus yang merugikan korban dalam penggunaan *dating* apps, seperti tindakan kriminal, pelecehan seksual, pemalsuan identitas, dan penyebaran pornografi. Responden umumnya mengetahui atau pernah mengalami kasus-kasus tersebut, dan sebagian besar setuju dengan pernyataan terkait kasus-kasus tersebut. Pengguna yang mengetahui atau mengalami kasus kriminalitas cenderung berbagi informasi dengan orang lain dan berpotensi untuk keluar dari atau menghentikan penggunaan *dating* apps. Hal ini disebabkan oleh *dating* apps tidak memberikan edukasi atau jaminan yang memadai terkait keamanan dan kriminalitas kepada pengguna sehingga berdampak negatif pada loyalitas dan kepercayaan pengguna terhadap platform tersebut. Oleh karena itu, masih banyak pengguna *dating* apps yang mengalami pengalaman buruk akibat adanya penyimpangan penggunaan *dating apps*. Hal ini penting bagi penyedia *dating apps* untuk meningkatkan kesadaran terkait keamanan dalam *dating apps* dan perlunya tindakan yang lebih kuat dari pihak penyedia aplikasi untuk melindungi pengguna dari risiko-risiko yang terkait dengan kriminalitas. Saran yang bisa diberikan untuk penelitian yang akan datang diharapkan ada penelitian lebih lanjut yang menggali lebih dalam tentang faktor-faktor yang mempengaruhinya, dampaknya pada pengguna, serta hukum yang melindungi tindakan kriminal yang terjadi pada *dating apps*. Ini dapat membantu penyedia *dating apps* dalam mengambil langkah-langkah lebih konkret dalam meningkatkan keamanan. Kemudian, saran yang dapat diimplementasi bagi penyedia *dating apps* yaitu lebih memperhatikan keamanan dan privasi pengguna sehingga pengguna merasa aman saat menggunakan aplikasi tersebut

Sebagai rekomendasi, pengembang aplikasi kencan diharapkan tidak hanya mengandalkan fitur keamanan pasif seperti enkripsi data, tetapi juga menyediakan mekanisme pelaporan cepat untuk pelecehan dan fitur pendeteksi kejahatan siber secara otomatis.

Saran

Berdasarkan penelitian ini, disarankan agar pengembang aplikasi kencan meningkatkan transparansi mengenai kebijakan privasi dan langkah-langkah keamanan yang diambil untuk melindungi data pengguna. Edukasi mengenai risiko keamanan dan cara melindungi diri saat menggunakan aplikasi juga perlu ditingkatkan. Hal ini dapat dilakukan melalui kampanye informasi yang jelas dan mudah dipahami oleh semua pengguna. Dengan meningkatkan kepercayaan pengguna melalui tindakan nyata dalam perlindungan data dan edukasi, diharapkan pengalaman positif dapat tercipta, sehingga mendorong lebih banyak orang untuk menggunakan aplikasi kencan dengan rasa aman. Secara keseluruhan, penelitian ini menekankan pentingnya perhatian terhadap aspek privasi dan keamanan dalam penggunaan aplikasi kencan. Perlunya kolaborasi antara pengembang aplikasi dan pengguna untuk menciptakan lingkungan digital yang lebih aman menjadi sangat jelas dari hasil penelitian ini.

Dengan demikian, upaya untuk meningkatkan perlindungan privasi dan keamanan data harus menjadi prioritas utama bagi semua pihak yang terlibat dalam industri aplikasi kencan.

Penelitian selanjutnya diharapkan dapat mengeksplorasi lebih dalam tentang regulasi pemerintah terkait perlindungan data di aplikasi kencan serta efek dari pengesahan RUU Perlindungan Data Pribadi terhadap keamanan pengguna di platform tersebut.

UCAPAN TERIMA KASIH

Terima kasih kepada Tuhan Yang Maha Esa, keluarga, teman-teman, dan semua pihak yang telah membantu dalam pelaksanaan dan penulisan peneliti ini untuk di jadikan jurnal ilmiah.

DAFTAR PUSTAKA

[1] L. Belakang, "Bab I ي ِ خ حض," *Galang Tanjung*, no. 2504, hal. 1–9, 2015.
[2] S. B. Saputri, "Dilema Privasi dan Keamanan Data dalam Aplikasi *Dating*," *Tarfomedia*, hal. 1–7, 2024.
[3] A.- Efendi dan R.- Rahmiati, "Persepsi keamanan, persepsi privasi, pengalaman serta kepercayaan terhadap belanja *online*," *J. Kaji. Manaj. Bisnis*, vol. 9, no. 1, hal. 26–38, 2020, doi: 10.24036/jkmb.10890000.
[4] R. Adolph, " Perlindungan Hukum Terhadap Hak Privasi Dan Keamanan Data Pribadi Pengguna Aplikasi Kencan Di Indonesia" no. 2018, hal. 1–23, 2016.
[5] Setiawanty, S., & Rosary, H. (2023). "Persepsi Pengguna terhadap Keamanan dan Privasi di Aplikasi Kencan di Indonesia." *Jurnal Teknologi Informasi dan Komunikasi*, 8(1), 45-58.
[6] Kelley, P. G., et al. (2016). "Privacy and Security in *Dating* Apps: A Study of the User Experience." *Journal of Cybersecurity*, 2(4), 1-15.
[7] Mahira, D.F., & Lisa, E.Y. (2020). "Consumer Protection System (CPS): Sistem, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept". Jurnal Ilmu Hukum.
[8] Nurhidayati, Sugiyah, & Yuliantari, K. (2021). "Pengaturan Perlindungan Data Pribadi dalam Penggunaan Aplikasi PeduliLindungi". Widya Cipta: Jurnal Sekretari dan Manajemen, 5(1).
[9] Widiastuti, A.I. (2020). "Urgensi Pengesahan RUU Perlindungan Data Pribadi (PDP) di Tengah Pandemi COVID-19". Jurnal Hukum Indonesia.
[10] Kusnadi, S.A. (2021). "Perlindungan Hukum Data Pribadi sebagai Hak Privasi. Jurnal Legislasi Indonesia."
[11] Djafar, W. (2019). "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan. Fakultas Hukum, Universitas Gadjah Mada."
[12] Natamiharja, R.N.R. (2019). "Perlindungan Hukum Atas Data Pribadi di Indonesia. Jurnal Hukum & Pembangunan."
[13] Dewi, S. (2016). "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia". Yustisia, 5(1).

[14] Rizkinaswara, L. (2020). "Penanganan Kebocoran Data Pengguna Aplikasi E-Commerce. Jurnal Komunikasi dan Informatika".
[15] Irwansyah. (2020). "Perlindungan Hukum Terhadap Kebocoran Data Pribadi. Jurnal Keamanan Siber"
[16] Chris, Novita. (2021). "Pengaruh Kesadaran Keamanan Informasi Dan Privasi Jaringan Sosial Terhadap Perilaku Perlindungan Privasi Pada Para Pengguna Jaringan Sosial. Jurnal Ilmu Komunikasi."
[17] Nade,V.(2019). Cyber Stalking Legal Perspectives And Psychological
[18] [1] I. A. Afandi, A. Kusyanti, dan N. H. Wardani, "Analisis Hubungan Kesadaran Keamanan , Privasi Informasi , Perilaku Keamanan Pada Para Pengguna Media Sosial Line," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 9, hal. 783–792, 2017.
[19] Mills, C. E., & Hayes, B. E. (2021). *Social media stalking: A type of digital dating abuse*. Journal of Interpersonal Violence, 36(9-10), NP5384-NP5410.
[20] Whitty, M. T., & Buchanan, T. (2012). *The online dating romance scam: Causes and consequences of victimhood*. Psychology, Crime & Law, 18(3), 283-303.
[21] Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
[22] Putra, D. A., & Wahyudi, A. (2018).*Kejahatan Siber: Analisis Kebijakan Hukum dalam Menghadapi Kejahatan Siber di Indonesia.Jurnal Hukum dan Pembangunan*, 48(1), 80-93.
[23] Suhartanto, T., & Supriyanto, I. (2020).*Perlindungan Data Pribadi dalam Media Sosial di Indonesia: Tinjauan UU ITE.Jurnal Teknologi Informasi dan Komunikasi*, 5(2), 95-108
[24] Saputri, S. P., & Anggraeni, D. (2021).*Persepsi Pengguna Terhadap Privasi dan Keamanan Media Sosial di Indonesia.Jurnal Sistem Informasi Indonesia*, 10(1), 45-55
[25] T. Agustin, "Analisis Keamanan Sistem Informasi Terhadap Data Pribadi di Media Sosial," 2020, [Daring].
[26] Iman, A., & Ahmad, M. (2020). Data *Breach*es and the Impact on User Privacy: A Study of Social Media Platforms. *Journal of Cybersecurity and Privacy*, 1(2), 123-145.
[27] Mohamed, N., & Ahmad, R. (2012). Internet Users' Information Privacy Concerns: The Role of Trust and Perceived Control. *Journal of Information Privacy and Security*, 8(3), 3-20.
[28] Nade, M. (2019). Cyber Crime and its Impact on *Online Dating*: A Review of Current Trends and Issues. *Journal of Cyber Studies*, 5(1), 45-60.