

# Dilema Privasi dan Keamanan Data dalam Aplikasi Dating

Stephanie Bella Saputri (Dosen STARKI)

## PENDAHULUAN

Aplikasi *dating* telah menjadi salah satu aplikasi yang populer secara global sejak pandemic Covid-19, khususnya di kalangan milenial dan generasi Z. Dilansir pada The Regulatory Review dengan judul artikel “*Matching Dating Apps with Regulation*” menyatakan bahwa pada tahun 2019, terdapat 39 persen pasangan di Amerika Serikat menggunakan aplikasi *dating* dan bertemu secara *online* ditengah *lockdown* dampak pandemi (Walsh dkk, 2022). Aplikasi ini menawarkan kemudahan bagi penggunaannya untuk mencari pasangan dan menjalin hubungan dari berbagai latar belakang dan lokasi. Berdasarkan riset aplikasi Apptopia dalam Annur (2023), menyebutkan bahwa Tinder adalah aplikasi *dating* terpopuler dan paling banyak diunduh secara global pada tahun 2022 yakni sebanyak 64 juta kali. Kemudian disusul pada peringkat kedua yakni Bumble dengan jumlah unduh sebanyak 28 Juta sepanjang tahun 2022. Berikut 10 aplikasi *dating* yang paling diunduh secara global:

Tabel 1

### 10 Aplikasi Kencan Online Paling Banyak Diunduh Secara Global (2022)

| Peringkat | Aplikasi       | Jumlah Unduh |
|-----------|----------------|--------------|
| 1         | Tinder         | 64 Juta      |
| 2         | Bumble         | 28 Juta      |
| 3         | Badoo          | 26 Juta      |
| 4         | Tantan         | 24 Juta      |
| 5         | Grindr         | 13,6 Juta    |
| 6         | Hinge          | 13,4 Juta    |
| 7         | Plenty of Fish | 11,3 Juta    |
| 8         | Happn          | 9,8 Juta     |
| 9         | MOMO           | 9,3 Juta     |
| 10        | JAUMO          | 8,6 Juta     |

Sumber: Annur (2023)

Maraknya penggunaan aplikasi *dating* ini juga ditemukan di Indonesia, menurut survei yang dilakukan oleh Rakuten Insight Center (2020) dalam Setiawanty dan Rosary (2023) menyebutkan bahwa masyarakat Indonesia yang berusia 25 hingga 34 tahun merupakan orang yang paling banyak menggunakan aplikasi *dating* dari 3.113 responden. Sebanyak 32% responden mengatakan bahwa lebih menyukai melakukan pendekatan menggunakan aplikasi *dating* dikarenakan *online*. Alasan lainnya dikarenakan bosan dan memiliki aktivitas yang padat sehingga tidak memiliki waktu yang banyak untuk berkenalan dengan orang baru secara tatap muka. Terdapat lima aplikasi *dating* yang paling banyak digunakan masyarakat Indonesia (Azzahra, 2023) antara lain sebanyak 57,6% responden merupakan pengguna Tinder, sebanyak 33,9% responden merupakan pengguna Tantan dan urutan ketiga sebanyak 18,2% merupakan pengguna OkCupid.

Namun, di balik kemudahan tersebut, terdapat dilema privasi dan keamanan data yang perlu diperhatikan. Dilansir dari Azzahra (2023), menyatakan bahwa kemunculan aplikasi *dating* membuka peluang kejahatan siber, termasuk pelanggaran privasi. Hal ini dikarenakan risiko privasi dari penggunaan aplikasi ini sering diabaikan. Dilema privasi ini muncul dikarenakan pengguna aplikasi *dating* harus memberikan sejumlah informasi privasi kepada aplikasi, seperti nama, foto, lokasi, informasi kontak, media sosial dan lainnya. Informasi ini dapat digunakan oleh aplikasi untuk meningkatkan pengalaman pengguna, seperti menampilkan hasil pencarian yang lebih relevan atau memberikan rekomendasi pengguna sesuai dengan kebutuhannya masing-masing. Seperti aplikasi Grindr sebagai aplikasi *dating* khusus LGBT yang mana memungkinkan pengguna membagikan informasi kesehatan pribadi seperti HIV dan status vaksinasi (Walsh, 2022). Namun, informasi ini juga dapat disalahgunakan oleh pihak lain, yakni untuk melakukan penipuan atau *cyberbullying*. Selain masalah privasi, aplikasi *dating* juga rentan terhadap masalah keamanan data. Aplikasi *dating* menyimpan sejumlah data pribadi pengguna, seperti informasi kontak, informasi keuangan dan bahkan informasi sensitif lainnya. Data-data ini dapat dicuri oleh pihak-pihak yang tidak bertanggung jawab dan digunakan untuk melakukan kejahatan, seperti penipuan atau pemerasan.

## PEMBAHASAN

### a) Lima Masalah Privasi

Menurut Shaw (2020), terdapat lima masalah privasi yang harus diketahui pengguna dalam menggunakan aplikasi *dating*, yakni sebagai berikut:

#### i) Aplikasi *dating* mengumpulkan banyak data pribadi pengguna

Aplikasi *dating* mengumpulkan banyak data pribadi pengguna, termasuk informasi sensitif seperti orientasi seksual, keyakinan politik dan agama, penggunaan narkoba, alkohol dan rokok serta latar belakang etnis. Walaupun, informasi tersebut penting untuk diketahui pengguna lainnya sebagai calon pasangan, namun, UU privasi (Nomor dan tahun di Negara) menyadari bahwa kebocoran atau pengungkapan data ini dapat menimbulkan ancaman terhadap kebebasan dan keselamatan seseorang dalam penggunaan aplikasi.

Misal, pengguna aplikasi yang berlokasi di negara yang memiliki peraturan yang ketat terkait agama dan politik, dapat menjadi sasaran pengawasan karena afiliasi yang diungkapkan. Seorang LGBT pun mungkin berisiko untuk ditangkap, diperas atau diungkap

kepada teman, keluarga atau kerabat yang diskriminatif. Hal ini pun akan mengancam situasi pekerjaan dan keselamatan pribadi pengguna.

ii) Aplikasi *dating* melacak lokasi pengguna

Aplikasi *dating* pada umumnya menggunakan data lokasi pengguna untuk menunjukkan calon jodoh yang di sekitar. Data ini dapat digunakan untuk melacak lokasi pengguna. Hal ini dapat membahayakan keselamatan dan privasi pribadi pengguna. Pelaku kejahatan dapat memanfaatkan informasi tersebut untuk mengikuti dan bahkan menculik pengguna.

iii) Gambar dan video pribadi dapat disalahgunakan.

Foto dan video yang dikirim melalui aplikasi *dating* tidak dapat dijamin keamanannya. Banyak aplikasi *dating* yang lemah terhadap keamanannya yang dapat menyebabkan foto dan video pengguna bocor dan tersebar. Pada tahun 2019, perusahaan keamanan seluler Zimperium melakukan audit terhadap 28 aplikasi *dating* populer dan menemukan terdapat 25 aplikasi yang gagal menerapkan komunikasi yang aman, sementara terdapat 23 aplikasi tidak memiliki penyimpanan data yang aman. Kelemahan inilah yang dapat membuat foto dan video seseorang mudah terekspos. Seperti contohnya pada aplikasi *dating* Jack'd, dimana foto pribadi seorang pengguna ditemukan tersimpan dalam database yang dapat diakses publik melalui Amazon Web Series. Selain itu, foto yang diunggah ke *dating app* juga tidak semuanya asli, banyak juga pengguna yang menggunakan foto profil orang lain.

iv) Aplikasi *dating* menjual data pribadi pengguna

Cara umum bagi perusahaan aplikasi *dating* yang gratis untuk memperoleh uang adalah dengan menjual data pengguna kepada perusahaan periklanan. Banyak perusahaan yang telah dituduh menjual data pribadi tanpa sepengetahuan atau persetujuan pengguna. Seperti aplikasi *dating* Grindr dikeluhkan pengguna dikarenakan telah membagikan lokasi GPS pengguna, pengidentifikasi perangkat dan informasi yang sensitif lainnya kepada pengiklan secara ilegal.

v) Sasaran peretas.

Aplikasi *dating* menyimpan sejumlah informasi pribadi yang dapat disalahgunakan. Oleh karena itu, tak heran jika aplikasi *dating* sering menjadi sasaran serangan siber. Seperti aplikasi *dating* OkCupid pada tahun 2015 yang dibajak. Oleh karena itu, ada baiknya sebagai pengguna menyelidiki aktivitas yang dilakukan pada aplikasi *dating* untuk melindungi data pribadi pengguna.

Check Point Software Technologies (CPR) dalam Anggraini (2023) menemukan sejumlah pengguna aplikasi *dating* rentan terhadap risiko, mulai dari pemerasan, *malware* dan *spyware*, akun palsu hingga pencurian identitas. Oleh karena itu, CPR menilai bahwa keinginan pengguna untuk membagikan informasi pribadi terlalu berlebihan dan disisi lain keamanan aplikasi kencan lemah sehingga penjahat siber mudah untuk mengidentifikasi, menargetkan dan menyerang pengguna. Terlebih jika pengguna menghubungkan akun aplikasi *dating* dengan akun media sosial lainnya seperti Instagram, Spotify dan lain sebagainya. Jika izin akses dihubungkan ke beberapa media sosial yang dimiliki pengguna, maka secara otomatis informasi dan data pribadi pengguna akan terisi, juga informasi seperti tempat kerja, kontak hingga lokasi pun aksesnya akan diminta oleh aplikasi. Padahal informasi pribadi seperti itu sangat rentan akan aksi kejahatan *cyberstalking* hingga pemerasan, *doxing* dan penguntitan secara fisik. Akibatnya dapat merusak reputasi, merugikan serta menjatuhkan pengguna dengan mudah hanya melalui media sosial. Imperva



dalam Anggraini (2023) pun mencatat pada Juli 2015, terdapat pelanggaran yang dilakukan oleh Ashley Madison hingga aplikasi *dating* dalam mengelola informasi pribadi pengguna ditemukan belum maksimal. Selain itu, ditemukan adanya kebocoran data pribadi sebanyak 4 juta data pengguna di forum *darknet* yang telah dilaporkan oleh AdulFriendFinder. Pada tahun 2021, ditemukan lebih dari 2,28 juta data pengguna MeedMindful seperti nama asli, alamat email dan karakteristik fisik bocor.

## **b) Privasi Aplikasi *Dating* pada Perspektif Teori Manajemen Komunikasi Privasi**

Pada perspektif ilmu komunikasi, dapat meninjau privasi dengan menggunakan teori *Communication Privacy Management Theory* (CPM) atau Teori Manajemen Komunikasi Privasi. Manajemen privasi komunikasi dapat menjadi solusi untuk mengatasi dilema privasi ini. Teori manajemen privasi komunikasi yang dikemukakan oleh Petronio (2002) adalah teori yang membatasi dan mengelola informasi pribadi (Zakiah, 2022). Pengungkapan informasi pribadi ini dilatarbelakangi oleh beberapa faktor seperti latar belakang budaya, jenis kelamin dan lain sebagainya untuk mendeskripsikan mengenai diri mereka pada orang lain melalui media komunikasi. Media komunikasi yang dimaksud beragam, salah satunya adalah aplikasi *dating*. Teori ini menggarisbawahi bahwa privasi merupakan suatu hak individu yang harus dilindungi.

Mariam J Metzger pada jurnal *Computer Mediated Communication* (2007) dalam Zakiah (2022), menjelaskan bahwa terdapat tiga proses manajemen privasi komunikasi. **Pertama**, pemilihan waktu untuk mengungkapkan informasi untuk mencegah risiko yang terjadi dikemudian hari. Misal, ketika seseorang hendak membicarakan hal yang sangat pribadi dan sensitif, ia akan membutuhkan waktu yang lama untuk lebih mengenal dan mempercayai lawan bicaranya. Jika hubungan yang terjalin dinilai intim, maka ia akan mencoba untuk menceritakan hal tersebut. **Kedua**, koordinasi batasan yang berarti adanya negosiasi. Yang dimaksud adalah seseorang cenderung memfilter informasi apa saja yang hendak disampaikan dan akan menyembunyikan hal yang bersifat privasi pada lawan bicara yang dinilai tidak terlalu dekat atau tidak sefrekuensi. Misal, ketika seseorang *match* di aplikasi *dating*, ia akan merencanakan apa saja yang hendak ditanyakan dan informasi apa saja yang hendak disampaikan kepada lawan bicara. Ia akan mempertimbangkan hubungan kedekatan dan latar belakang lawan bicara sebelum menyampaikan hal-hal yang bersifat privat dan sensitif. Terakhir **ketiga**, turbulensi batasan. Yang dimaksud adalah tiap orang mungkin telah membuat sistem aturan dan batasan namun pada kenyataan tidak dapat berjalan sesuai yang diharapkan. Tiap orang memiliki kriteria aturan batasan yang mungkin dinilai sensitif oleh lawan bicaranya, yang kemudian akan menimbulkan ketegangan dalam berhubungan. Misal, ketika seseorang bertemu dengan lawan bicara untuk pertama kali di aplikasi *dating*, seringkali akan mengajukan beberapa pertanyaan guna mengetahui *background* dan karakteristik calon pasangan. Namun, tanpa disadari pertanyaan yang diajukan mungkin dianggap hal yang pribadi dan terlalu sensitif bagi lawan bicara, seperti gaji, agama, ketertarikan politik, status pernikahan, pekerjaan dan lain sebagainya.

Berkaitan dengan tiga proses manajemen privasi komunikasi diatas, terdapat tiga asumsi dalam buku *Boundaries of Privacy: Dialectics of Disclosure* yang dapat menjelaskan bagaimana seseorang dapat berkomunikasi sesuai dengan aturan dan sistem yang telah ditentukan. Tiga asumsi teori yang dimaksud sebagai berikut (1) Manusia menetapkan keputusan, (2) Manusia sebagai pembuat dan pengikut aturan dan (3) Keputusan seseorang dapat dipengaruhi pertimbangan atau pendapat orang lain dan diri sendiri. Oleh karena itu, manajemen privasi komunikasi dapat dilakukan pada aplikasi *dating* dengan beragam cara, seperti sebagai berikut:

i) Membatasi informasi pribadi yang diberikan kepada aplikasi.

Pengguna dapat membatasi informasi pribadi yang diberikan kepada aplikasi dengan hanya memberikan informasi yang seperlunya. Seperti, memberikan nama dan foto, tidak perlu memberikan informasi lokasi, informasi kontak, zodiak, tanggal lahir dan lain sebagainya.

ii) Menggunakan pengaturan privasi yang tersedia

Aplikasi *dating* biasanya menyediakan pengaturan privasi yang dapat digunakan pengguna untuk mengatur informasi pribadi dapat dilihat publik atau bersifat pribadi. Pengaturan privasi dapat membantu pengguna untuk mengontrol siapa saja yang dapat melihat informasi pribadi pengguna. Yang mana pengguna dapat mengaktifkan pengaturan privasi yang sesuai dengan kebutuhan mereka.

iii) Menggunakan aplikasi pihak ketiga untuk melindungi privasi

Ada beberapa aplikasi pihak ketiga yang dapat digunakan untuk melindungi privasi pengguna aplikasi *dating*. Aplikasi ini dapat digunakan untuk menyembunyikan informasi pribadi pengguna atau untuk mengenkripsi komunikasi pengguna.

Dengan mengikuti tips tersebut, diharapkan dapat meminimalisir risiko privasi pengguna aplikasi *dating* yang disalahgunakan oleh pihak lain. Dilema privasi dan keamanan data dalam aplikasi *dating* merupakan hal yang perlu diperhatikan oleh para pengguna. Tanpa disadari, pengguna aplikasi *dating* memiliki kebutuhan privasi yang beragam. Terdapat pengguna yang mengutamakan privasi dan hanya membagikan informasi pribadi yang benar-benar diperlukan. Namun, ada juga pengguna lainnya yang lebih terbuka dan bersedia membagikan lebih banyak informasi pribadi. Kebutuhan privasi pengguna aplikasi *dating* dipengaruhi oleh beberapa faktor, seperti (1) **Tingkat kenyamanan dengan teknologi**, pengguna yang lebih nyaman dengan teknologi cenderung lebih terbuka untuk membagikan informasi pribadi mereka, (2) **Kekhawatiran terhadap keamanan dan privasi**, pengguna yang lebih khawatir terhadap keamanan dan privasi akan cenderung lebih waspada dalam membagikan informasi pribadi mereka, (3) **Tujuan penggunaan aplikasi dating**, pengguna yang menggunakan aplikasi *dating* untuk mencari pasangan yang lebih serius akan lebih berhati-hati dan mampu memfilter informasi pribadi yang hendak dibagikan ke aplikasi.

Namun, ada dua hambatan yang dihadapi dalam mengimplementasikan manajemen privasi komunikasi di aplikasi *dating*. **Pertama, kurangnya transparansi dari aplikasi dating.** Aplikasi *dating* sering ditemukan tidak transparan dalam menjelaskan bagaimana aplikasi menggunakan informasi pribadi pengguna. Oleh karena itu, hal ini akan mempengaruhi pengguna untuk mengambil keputusan informasi pribadi apa saja yang aman untuk dibagikan. **Kedua, kurang pemahaman atau literasi mengenai privasi.** Banyaknya pengguna yang kurang memahami pentingnya privasi dan keamanan data. Sehingga banyak juga yang belum mengetahui bagaimana

melindungi data dan privasi mereka sebagai pengguna. Hal inilah yang membuat pengguna aplikasi *dating* rentan terhadap penyalahgunaan informasi pribadi.

## PENUTUP

Manajemen privasi komunikasi perlu dilakukan oleh pengguna aplikasi *dating*. Dengan melakukan manajemen privasi komunikasi yang tepat, pengguna dapat mengurangi risiko penyalahgunaan informasi pribadi oleh orang lain. Selain pengguna perlu melakukan manajemen privasi komunikasi, aplikasi *dating* perlu memperhatikan beberapa hal untuk menjamin keamanan data dan informasi pribadi pengguna. Aplikasi *dating* harus lebih transparan dan jelas dalam menjelaskan bagaimana menggunakan informasi pribadi pengguna. Aplikasi *dating* pun harus menyediakan pengaturan privasi yang lebih jelas, dikarenakan pengguna harus memiliki kontrol yang lebih besar atas siapa saja yang dapat melihat informasi pribadi yang telah dibagikan. Selain itu, aplikasi *dating* pun harus memberikan edukasi berupa literasi mengenai keamanan data dan informasi pribadi yang dibagikan pada aplikasi, serta pentingnya privasi akan informasi pribadi. Sehingga, pengguna paham bagaimana cara melindungi privasi mereka, serta memiliki rasa aman dan percaya menggunakan aplikasi *dating* tersebut.

## Referensi:

- Anggraini, Ervina. (2023). Sejauh Mana Keamanan Dating App dari Aksi Penipuan Online?. Diakses <https://www.bluepowertechnology.com/news-detail/sejauh-mana-keamanan-dating-app-dari-aksi-penipuan-online> pada 10 Januari 2024.
- Annur, Cindy Mutia. (2023). Deretan Aplikasi Kencan Online Terpopuler 2022, Tinder Teratas. Diakses <https://databoks.katadata.co.id/datapublish/2023/08/30/deretan-aplikasi-kencan-online-terpopuler-2022-tinder-teratas> pada 10 Januari 2024.
- Azzahra. (2023). *Dating App: Lahan Kriminal Baru di Indonesia*. Diakses <https://kumparan.com/zia-azzahra/dating-app-lahan-kriminal-baru-di-indonesia-20KZEumFDsM/full> pada 01 Februari 2024.
- Setiawanty. (2023). 5 Aplikasi Kencan Populer di Indonesia. Diakses <https://kumparan.com/kumparanwoman/5-aplikasi-kencan-populer-di-indonesia-20SS64xGUqP/full> pada 01 Februari 2024.
- Shaw, Rebecca. (2020). The Top 5 Privacy Concern for Dating Apps. Diakses [https://getterms-io.translate.goog/blog/the-top-5-privacy-concerns-for-dating-apps?\\_x\\_tr\\_sl=en&\\_x\\_tr\\_tl=id&\\_x\\_tr\\_hl=id&\\_x\\_tr\\_pto=tc](https://getterms-io.translate.goog/blog/the-top-5-privacy-concerns-for-dating-apps?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc) pada 10 Januari 2024.
- Verihubs. (2022). Ini Dia 7 Info Pribadi yang Tidak Boleh Dibagikan Secara Sembarangan. Diakses <https://verihubs.com/blog/info-pribadi/#:~:text=Gambar%20Paspor%2C%20SIM%2C%20KTP%2C,sangat%20pribadi%20dan%20sifatnya%20rahasia> pada 10 Januari 2024.



- Walsh, Moynihan, Yin. (2022). Matching Dating Apps with Regulations. Diakses <https://www.theregreview.org/2022/10/01/saturday-seminar-matching-dating-apps-with-regulation/> pada 15 Januari 2024.
- Zakiah, Nailufar. (2022). Teori *Communication Privacy Management*. Diakses <https://www.kompas.com/skola/read/2022/02/16/180000769/teori-communication-privacy-management> pada 20 Januari 2024.