JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI:https://doi.org/10.38035/jihhp.v6i1.6108
https://creativecommons.org/licenses/by/4.0/
Received: 20 Juli 2025 | **Revised:** 22 Oktober 2025 | **Accepted:** 30 Oktober 2025

Analisis Perlindungan Data Pribadi Pada Aplikasi *Tinder*

Divia Natasha[1], Siti Farhani[2]
[1] Universitas Al Azhar Indonesia, Jakarta, Indonesia, *nadiviaaa@gmail.com*
[2]Universitas Al Azhar Indonesia, Jakarta, Indonesia, *sitifarhani@uai.ac.id*

Corresponding Author: *nadiviaaa@gmail.com*[1]

Abstract: *Misuse of personal data by irresponsible parties often occurs. To address this issue, Law No. 27 of 2022 on Personal Data Protection was created as a measure to provide legal protection against such misuse. Personal data protection aims to ensure awareness and respect for the importance of personal data protection. This type of research uses a normative legal approach. Legal research that focuses on legal principles and the level of legal compliance. This approach aims to identify patterns, relationships, and trends in existing legal data. Dating app developers have an obligation to protect users' personal data, including implementing adequate security measures, obtaining user consent before collecting and using data, and providing transparency about their privacy practices. They must also comply with applicable data privacy laws and regulations. Tinder is committed to enhancing security and reducing risk in its digital environment by developing secure access protocols and network architectures that enable systematic control over internal access, applying the principle of least privilege. Tinder must provide a transparent and easily accessible privacy policy that details the types of data collected, the reasons for collection, and how the data is used.*

Keyword: *personal data protection, data theft, cybercrime, privacy policy*

Abstrak: Penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab sering terjadi. Untuk mengatasi masalah ini, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi diciptakan sebagai langkah untuk memberikan perlindungan hukum terhadap penyalahgunaan tersebut. Perlindungan data pribadi bertujuan untuk menjamin kesadaran dan penghormatan terhadap pentingnya perlindungan data pribadi. Jenis penelitian ini menggunakan pendekatan hukum normatif. Penelitian hukum yang berfokus pada prinsip-prinsip hukum dan tingkat keselarasan hukum. Pendekatan ini bertujuan untuk mengidentifikasi pola, hubungan, dan tren dalam data hukum yang ada. Developer aplikasi kencan memiliki kewajiban untuk melindungi data pribadi pengguna, termasuk menerapkan langkah-langkah keamanan yang memadai, mendapatkan persetujuan pengguna sebelum mengumpulkan dan menggunakan data, dan memberikan transparansi tentang praktik privasi mereka. Mereka juga harus mematuhi undang-undang dan regulasi privasi data yang berlaku. *Tinder* berkomitmen untuk meningkatkan keamanan dan mengurangi risiko di lingkungan digitalnya dengan mengembangkan protokol akses aman dan arsitektur jaringan yang memungkinkan kontrol sistematis terhadap akses internal, menerapkan prinsip hak akses

paling rendah. *Tinder* harus menyediakan kebijakan privasi yang transparan dan mudah diakses, yang merinci jenis data yang dikumpulkan, alasan pengumpulannya, serta cara penggunaan data tersebut.

Kata Kunci: perlindungan data pribadi, pencurian data, kejahatan siber, kebijakan privasi

PENDAHULUAN

Sebelum UU Nomor 27 Tahun 2022, Indonesia belum memiliki dasar regulasi komprehensif untuk perlindungan data pribadi, dan peraturan yang ada dianggap tidak cukup untuk menangani risiko terkait penggunaan data pribadi yang semakin luas. Ketiadaan regulasi yang kuat ini menimbulkan kekhawatiran akan penyalahgunaan data dan kurangnya jaminan privasi bagi warga negara di era digital yang berkembang pesat. Terjawab saat 17 Oktober Tahun 2022, Indonesia mengesahkan UUPDP untuk tujuan melindungi data pribadi warganya dan memenuhi standar internasional seperti GDPR. UU ini diharapkan dapat meningkatkan respons terhadap ancaman privasi, menciptakan ekonomi digital yang aman, dan meningkatkan kepercayaan publik terhadap pemerintahan dan transaksi digital(JDIH Kota Semarang, 2024).

UUD 1945 Pasal 5 ayat (1) menjelaskan "Pasal ini menunjukkan bahwa pembentukan undang-undang, termasuk undang-undang tersebut, berada di tangan Presiden bersama DPR. Ini berarti bahwa negara memiliki kewenangan untuk membuat regulasi yang spesifik mengenai perlindungan data pribadi, yang kemudian akan menjadi dasar hukum bagi aplikasi seperti *Tinder*". *Tinder* sebagai penyedia layanan harus mematuhi aturan tersebut.

Pasal 20 "Pasal ini menjelaskan bahwa undang-undang harus mendapatkan persetujuan dari DPR. Ini berarti bahwa proses pembentukan undang-undang perlindungan data pribadi harus melibatkan partisipasi dan persetujuan dari perwakilan rakyat, memastikan bahwa regulasi tersebut mencerminkan kepentingan masyarakat". Implikasi pada *Tinder*: Pasal 5 ayat (1) dan Pasal 20 menunjukkan bahwa negara memiliki kewenangan bertujuan untuk melindungi hak-hak dasar. Ini adalah langkah krusial untuk memastikan bahwa aplikasi seperti *Tinder* beroperasi dalam kerangka hukum yang jelas(Undang-Undang Dasar Negara Republik Indonesia 1945, 1945).

Penyalahgunaan data pribadi kini menjadi dasar yang penting, seiring dengan bertambahnya penggunaan teknologi, perlindungan terhadap data pribadi menjadi sangat penting untuk mencegah pelanggaran privasi dan kejahatan siber(Mamonto, 2022). Penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab sering terjadi. Untuk mengatasi hal ini, Undang-Undang Perlindungan Data Pribadi (UUPDP) dibuat untuk memberikan perlindungan hukum dan meningkatkan kesadaran akan pentingnya perlindungan data pribadi(Saly et al., 2023).

Perlindungan data pribadi pada aplikasi *Tinder* berdasarkan (UUPDP) merupakan aturan penting keamanan data pribadi dapat ditingkatkan melalui enkripsi, akses terbatas, audit, pelatihan, dan kebijakan keamanan yang baik di Indonesia. *Tinder*, sebagai aplikasi kencan online, mengumpulkan dan memproses berbagai jenis data pribadi pengguna. Analisis ini mengkaji bagaimana *Tinder* mematuhi ketentuan UUPDP, Asas perlindungan data pribadi mencakup prinsip-prinsip yang memastikan pemrosesan data dilakukan dengan aman dan bertanggung jawab (Saly et al., 2023).

Internet merupakan sarana untuk mempermudah jangkauan kita dengan sangat mudah dapat memesan kebutuhan apapun menjadi mudah(Syahri, 2024). Perkembangan disaat ini termasuk perkembangan teknologi informasi serta komunikasi semakin pesat telah mengubah cara manusia berinteraksi, termasuk dalam hal mencari pasangan. Aplikasi kencan seperti *Tinder* telah menjadi trend populer di kalangan masyarakat untuk menemukan hubungan romantis. Namun, di balik kemudahan yang ditawarkan, terdapat berbagai kendala serta

dampak yang signifikan terkait hal tersebut, salah satunya adalah *Love Scamming*. *Love Scamming* adalah praktik penipuan di mana pelaku berpura-pura menjalin hubungan emosional dengan korban untuk mengeksploitasi perasaan tersebut demi keuntungan finansial(Zahra et al., 2022).

Tidak dapat disangkal bahwa banyak wanita merasa rentan ketika menghadapi masalah cinta, terutama jika mereka tidak diberikan kesempatan oleh orang-orang di sekitarnya untuk mengenal pria di luar lingkaran mereka(Widyarto & Hapsari, 2022). Menurut laporan dari berbagai lembaga, termasuk *Federal Trade Commission (FTC)* di Amerika Serikat, kasus *Love Scamming* terus meningkat, dengan kerugian yang mencapai miliaran dolar setiap tahunnya. Pada tahun 2022, *Federal Trade Commission (FTC)* atau Komisi Perdagangan Amerika Serikat melaporkan bahwa 70.000 orang menjadi korban penipuan cinta, dengan total kerugian mencapai 1,3 miliar dolar AS(Hidup et al., 2024). Penipuan cinta ini tidak hanya terjadi di Amerika Serikat, tetapi juga berpotensi menimpa banyak orang di Indonesia.

Sri Wiyanti Edyyono, dosen di FH UGM dan Ketua Pusat Kajian *Law, Gender, and Society* UGM, menyatakan bahwa penipuan yang mengatasnamakan cinta, atau yang dikenal sebagai love scam, semakin sering terjadi belakangan ini(Titin et al., 2024).

Dalam konteks ini, Data pribadi pada penggunaan aplikasi kencan, seperti nama, alamat, foto, dan informasi lainnya, dapat sangat disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, regulasi mengenai perlindungan data pribadi menjadi krusial untuk melindungi pengguna dari potensi penyalahgunaan. Di Indonesia, UUPDP menjadi dasar acuan dalam hukum yang mengatur pengumpulan, penyimpanan, dan pengolahan data pribadi. UU ini mengharuskan penyelenggara aplikasi untuk menjaga keamanan data pengguna dan memberikan hak kepada individu untuk mengakses dan mengontrol data pribadi mereka. Banyak pengguna aplikasi kencan yang tidak menyadari pentingnya menjaga data pribadi mereka, sehingga mereka rentan terhadap penipuan. Oleh karena itu, edukasi mengenai perlindungan data pribadi harus ditingkatkan agar pengguna lebih waspada terhadap risiko yang ada.

Penelitian yang dilakukan oleh Adinda Arifiah (2025) dengan judul "Keterbukaan Diri Remaja Pengguna Aplikasi Kencan *Tinder*", Adinda Arifiah meneliti keterbukaan diri remaja di Tinder, mengeksplorasi motivasi, strategi manajemen privasi, dan dampaknya terhadap hubungan interpersonal, serta memberikan wawasan baru tentang bagaimana teknologi mengubah cara generasi muda membangun hubungan, disertai rekomendasi praktis untuk menjaga keseimbangan antara keterbukaan dan privasi. Di sisi lain, dalam penelitian saya ini, menganalisis kepatuhan Tinder terhadap regulasi UUPDP, menyoroti aspek perlindungan data, hak subjek data, dan implikasi hukum dari pelanggaran, serta mengidentifikasi kekuatan dan kelemahan regulasi dalam melindungi korban kejahatan siber seperti *Love Scamming*. Dengan demikian, *research gap* terletak pada perbedaan perspektif antara perilaku pengguna yang diteliti dari sudut pandang komunikasi dan psikologi sosial, serta tanggung jawab platform yang dikaji dari sudut pandang hukum dan regulasi data pribadi(Arifiah, 2025).

Penelitian oleh Alvian Dwiangga Wijaya dan Teddy Prima (2022) mengkaji perlindungan data pribadi secara umum dalam penggunaan aplikasi *smartphone*, menekankan pentingnya kepastian hukum yang diatur dalam konstitusi dan memberikan rekomendasi bagi pemerintah dan penegak hukum. Sebaliknya, dalam penelitian ini pada aplikasi kencan *Tinder*, atas dasar ini dapat memberikan gambaran dalam sudut pandang UUPDP, serta implikasinya terhadap kasus *Love Scamming*. Perbedaan utama terletak pada cakupan dan fokus penelitian: Wijaya dan Prima membahas isu secara makro dan fundamental, sedangkan penelitian ini mengaplikasikan kerangka hukum tersebut dalam konteks mikro dan spesifik, memberikan analisis mendalam tentang risiko dan tantangan yang dihadapi pengguna *Tinder*. Dengan demikian, penelitian ini saling melengkapi, di mana satu memberikan perspektif luas dan yang

lainnya menyelami detail spesifik dalam perlindungan data pribadi di era digital(Wijaya & Anggriawan, 2022).

Penerapan prinsip keadilan menjamin bahwa korban memperoleh perlindungan hukum yang cukup, sedangkan prinsip kepastian hukum memberikan kejelasan mengenai tindakan yang melanggar hukum beserta sanksi yang akan diterapkan. Di sisi lain, prinsip kemanfaatan fokus pada keuntungan jangka panjang dari penegakan hukum(Chandra, 2024).

Dengan demikian, hal ini ada dalam kejahatan baru yang terjadi di masyarakat melalui media daring melalui jaringan elektronik global. Jenis tindakan kejahatan ini meliputi berbagai bentuk, mulai dari penipuan online hingga pencurian data diri, yang semuanya memanfaatkan teknologi untuk mencapai tujuan ilegal(Wijayanti & Hafidz, 2020).

Semua aktivitas atau kejahatan yang terjadi di ruang siber atau dunia maya tetap dianggap sebagai tindakan hukum yang nyata, meskipun berlangsung di lingkungan virtual dan bukti-buktinya bersifat elektronik hal ini disebabkan oleh fakta bahwa kejahatan siber memiliki dampak yang nyata terhadap korban(Khoirunnisa et al., 2025). Penyedia layanan internet dan platform e-commerce memainkan peran krusial dalam mengidentifikasi dan mencegah aktivitas penipuan di platform mereka. Mereka juga bertanggung jawab untuk memberikan edukasi kepada pengguna mengenai cara melindungi diri dari penipuan(Simanungkalit et al., 2024).

Dalam penelitian ini akan membahas beberapa pertanyaan tentang :

1) Bagaimana kebocoran data dan penyalahgunaan informasi pribadi terjadi dalam konteks *Love Scamming* di aplikasi kencan *Tinder*, dan apa implikasinya terhadap perlindungan data pribadi?
2) Bagaimana Undang-Undang Perlindungan Data Pribadi Memgatur Perlindungan Data Pribadi Pada *Tinder*?

Dengan demikian, artikel ini bertujuan untuk mengeksplorasi hubungan antara perlindungan data pribadi dan tindak pidana *Love Scamming* pada aplikasi kencan seperti *Tinder*. Melalui analisis regulasi yang ada dan fakta-fakta terkait, diharapkan dapat memberikan pemahaman yang lebih baik mengenai tantangan dan solusi dalam melindungi pengguna dari risiko yang ada di dunia digital.

METODE

Jenis penelitian ini mengadopsi pendekatan hukum normatif. Metode yuridis normatif merupakan penelitian hukum yang menekankan pada prinsip-prinsip hukum serta tingkat keselarasan dalam hukum. Pendekatan ini bertujuan untuk mengidentifikasi pola, hubungan, dan tren yang terdapat dalam data hukum yang tersedia.

Penelitian kuantitatif dalam bidang hukum biasanya bergantung pada data yang diperoleh dari putusan hukum dan peraturan perundang-undangan. Pendekatan ini memungkinkan peneliti untuk melakukan analisis statistik yang dapat mengungkap pola dan tren dalam data hukum yang tersedia. Dengan menggunakan data numerik, peneliti dapat menguji hipotesis dan mengeksplorasi hubungan antara variabel yang berbeda, memberikan wawasan yang lebih mendalam tentang dinamika hukum. Dengan demikian, penelitian kuantitatif memberikan kontribusi yang signifikan dalam memahami dan menganalisis fenomena hukum secara lebih luas dan objektif.

HASIL DAN PEMBAHASAN

Kebocoran data dan penyalahgunaan informasi pribadi dalam konteks *Love Scamming* di aplikasi kencan *Tinder*, serta implikasinya terhadap perlindungan data pribadi.

Kebocoran informasi data dan penyalahgunaan informasi data pribadi merupakan masalah serius yang memperburuk risiko *Love Scamming*. Data pribadi yang bocor dapat digunakan oleh penipu untuk membuat profil palsu yang lebih meyakinkan dan menargetkan

korban dengan lebih efektif(Anggraini, 2023). Risiko kebocoran data dapat mengakibatkan akses tidak sah terhadap informasi pribadi konsumen(Priliasari, 2023).

Selain itu, data aktivitas pengguna, seperti preferensi pencocokan, riwayat obrolan, dan informasi profil yang dikunjungi, juga dapat dieksploitasi. Kebocoran data dapat disebabkan oleh berbagai faktor, termasuk kerentanan keamanan pada sistem aplikasi, serangan siber, dan kelalaian manusia. Pengembang aplikasi perlu mengambil tindakan preventif untuk melindungi data pengguna dari ancaman tersebut. Saat ini, dapat dikatakan bahwa ada situasi darurat dalam perlindungan data pribadi seiring dengan pesatnya kemajuan teknologi(Setiawan & Najicha, 2022).

Undang-undang dan regulasi privasi data yang relevan meliputi *General Data Protection Regulation* (GDPR) di Eropa, *California Consumer Privacy Act* (CCPA) di Amerika Serikat, dan undang-undang perlindungan data pribadi di negara-negara lain. Undang-undang ini melindungi hak individu terkait data pribadi dengan memberikan akses, kemampuan untuk memperbaiki, dan menghapus informasi, serta membatasi pengumpulan dan penggunaan data oleh organisasi(Davis & Iapp, 2025).

Pengembang aplikasi kencan harus melindungi data pribadi pengguna dengan menerapkan keamanan, mendapatkan persetujuan, memberikan transparansi, dan mematuhi regulasi privasi data yang berlaku. Pengguna dapat mengajukan keluhan kepada otoritas perlindungan data terkait pelanggaran hak privasi, yang berwenang menyelidiki, memberikan sanksi, dan memerintahkan perbaikan praktik privasi oleh organisasi.

Pada tanggal 24 Juni 2025, perlindungan data pribadi di Indonesia, khususnya dalam konteks aplikasi kencan seperti Tinder, masih menjadi perhatian utama. Kasus kebocoran data yang merugikan jutaan penduduk Indonesia pada September 2024. Menunjukkan kerentanan yang ada. Meskipun UU PDP telah disahkan, efektivitas implementasinya masih perlu ditingkatkan melalui pengawasan yang ketat dan penegakan hukum yang efektif. Berdasarkan informasi yang dilansir dari "*Behind the Screen: Navigating Cybersecurity Risks and Personal Data*" peningkatan signifikan pengguna internet di Indonesia dan risiko yang menyertainya, seperti kebocoran data pribadi dan kejahatan siber. Artikel ini menyoroti berbagai bentuk ancaman digital termasuk *phishing*, *malware*, *doxxing*, dan penyalahgunaan AI untuk *deepfake* dan Kekerasan Berbasis Gender Online (KBGO). Dokumen ini juga menjelaskan dampak serius dari kejahatan digital terhadap korban, baik secara material maupun psikologis, serta menyoroti stigma sosial yang sering dihadapi korban KBGO. Terakhir, artikel ini menekankan pentingnya perlindungan data pribadi melalui langkah-langkah individu dan kebutuhan akan regulasi yang kuat dari pemerintah untuk memastikan keamanan dan keadilan di ruang digital(Indonesia, 2025).

Aplikasi kencan online seperti *Tinder* mengumpulkan berbagai data pribadi pemakai, termasuk nama, usia, lokasi, minat, dan preferensi. Data ini digunakan untuk mencocokkan pengguna dengan potensi pasangan. Namun, pengumpulan dan pemrosesan data pribadi ini juga menimbulkan risiko penyalahgunaan atau kebocoran data. Beberapa aspek perlindungan data pribadi pada *Tinder* yang perlu diperhatikan berdasarkan UUPDP:

a) Persetujuan Pengguna: *Tinder* harus memastikan bahwa pengguna memberikan persetujuan yang jelas dan eksplisit sebelum data pribadi mereka dikumpulkan dan diproses. Persetujuan ini harus diberikan secara sukarela, spesifik, dan berdasarkan informasi yang cukup.
b) Transparansi: *Tinder* Pengembang wajib memberikan penjelasan secara detail dan transparan kepada pengguna tentang cara penggunaan data pribadi mereka, dengan siapa data tersebut dibagikan, dan bagaimana data tersebut dilindungi.
c) Keamanan Data: *Tinder* harus menjalankan standarisasi penggunaan keamanan yang sangat memadai untuk melindungi data pribadi pengguna dari akses yang tidak sah,

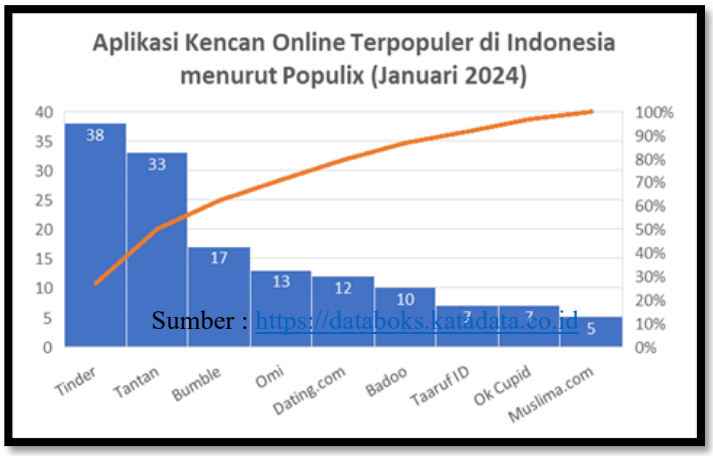
kebocoran, atau penyalahgunaan. Ini termasuk penggunaan enkripsi, firewall, dan sistem deteksi intrusi.

d) Hak Pengguna: *Tinder* harus menjalankan hak privat pengguna terkait data pribadi pemakai, termasuk dalam hak untuk mengakses, memperbaiki, menghapus, dan membatasi pemrosesan data pribadi mereka.
e) Notifikasi Kebocoran Data: Jika terjadi kebocoran data, *Tinder* harus memberitahukan kepada pengguna yang terkena dampak dan kepada otoritas yang berwenang dalam waktu yang wajar.

Program keamanan *Tinder* dirancang untuk melindungi organisasi dan data pengguna dengan memanfaatkan infrastruktur keamanan canggih, praktik pengelolaan data yang bertanggung jawab, serta standar keamanan dan privasi terbaik. Upaya ini bertujuan untuk menghadapi berbagai ancaman yang mengintai layanan internet.

Tinder berkomitmen untuk meningkatkan keamanan dan mengurangi risiko di lingkungan digitalnya dengan mengembangkan protokol akses aman dan arsitektur jaringan yang memungkinkan kontrol sistematis terhadap akses internal, menerapkan prinsip hak akses paling rendah. Selain itu, autentikasi dua faktor (2FA) diterapkan secara internal(*Tinder*, 2024).

Keamanan diintegrasikan di setiap tahap siklus pengembangan untuk menciptakan produk yang lebih baik dan aman, serta memastikan penerapan prinsip desain yang aman. Semua aplikasi dan sistem, termasuk fitur baru, kode, dan perubahan konfigurasi, menjalani tinjauan dan penilaian desain keamanan yang menyeluruh.



Grafik 1. Aplikasi Kencan Online Terpopuler di Indonesia menurut Populix (Januari 2024)

Berdasarkan grafik survei diatas yang dilakukan oleh Populix, sekitar 63% dari seribu orang Indonesia yang disurvei pada awal 2024 mengaku pernah menggunakan layanan tersebut(Muhamad, 2024). Survei oleh Populix menunjukkan bahwa Tinder adalah aplikasi kencan paling populer di Indonesia, digunakan oleh 38% responden, diikuti Tantan (33%) dan Bumble (17%). Aplikasi lain seperti Omi, Dating.com, Badoo, dan OK Cupid memiliki pengguna di bawah 15%, sementara Taaruf ID dan Muslima.com masing-masing digunakan oleh 7% dan 5%. Alasan utama penggunaan aplikasi adalah untuk mencari teman (56%), rasa ingin tahu (48%), dan bersenang-senang (46%), dengan hanya 27% yang mencari pasangan. Survei dilakukan pada 15-22 Januari 2024 dengan 1.165 responden, mayoritas berusia 17-35 tahun dan berasal dari Pulau Jawa.

Pengaturan Undang-Undang Perlindungan Data Pribadi Pada *Tinder*

Pertanyaan pemantik yang mendasar adalah bagaimana aplikasi seperti *Tinder* dapat secara efektif memastikan perlindungan data pribadi penggunanya dan mencegah praktik penipuan asmara yang merugikan, mengingat dampak yang dapat berujung pada kerugian materi dan psikologis korban. "*Dalam perspektif hukum, keberadaan aplikasi kencan digital*

seperti Tinder menempatkan perlindungan data pribadi sebagai tanggung jawab utama penyelenggara platform dan penggunanya". *Love Scamming*, yang dalam banyak kasus memanfaatkan celah informasi dan data pengguna, menuntut adanya kerangka hukum yang ketat dan implementasi teknologi verifikasi yang mutakhir untuk menghindari penyalahgunaan data demi keuntungan tidak sah.

Berikut adalah poin-poin penting dan pasal-pasal terkait dari UUPDP yang relevan dengan operasional *Tinder*:

1) Definisi dan Jenis Data Pribadi

a) Pasal 1 Angka 1 UUPDP: "*Data Pribadi merujuk pada informasi yang dapat digunakan untuk mengidentifikasi seseorang, baik secara langsung maupun tidak langsung, melalui berbagai jenis sistem, baik yang berbasis elektronik maupun non-elektronik*".
Relevansi dengan *Tinder*: *Tinder* mengumpulkan berbagai data yang secara langsung mengidentifikasi pengguna (nama, foto, tanggal lahir) dan data yang dapat mengidentifikasi pengguna jika dikombinasikan (lokasi, preferensi, riwayat chat).

b) Pasal 4 Ayat (1) UUPDP: "*Menyatakan bahwa Data Pribadi meliputi data sensitif yang, dalam pemrosesannya, dapat berakibat serius bagi Subjek Data, seperti potensi diskriminasi dan kerugian yang lebih besar*".

c) Pasal 4 Ayat (2) UUPDP: "*Meliputi kategori data pribadi mencakup data kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lain sesuai peraturan perundang-undangan*".
Relevansi dengan *Tinder*: *Tinder* dapat mengumpulkan data spesifik seperti preferensi seksual (jika diungkapkan), informasi kesehatan (jika disebutkan di profil), atau data biometrik (jika menggunakan fitur verifikasi wajah). Data lokasi juga bisa menjadi sensitif.

d) Pasal 4 Ayat (3) UUPDP: *"Data Pribadi umum meliputi nama, jenis kelamin, agama, status perkawinan, dan kombinasi data seperti nomor telepon seluler dan alamat IP untuk identifikasi individu".*
Relevansi dengan *Tinder*: Nama, jenis kelamin, usia, dan foto profil adalah contoh data umum yang dikumpulkan *Tinder*.

2) Hak Subjek Data Pribadi

UUPDP memberikan hak-hak fundamental kepada Subjek Data Pribadi yang harus dipenuhi oleh Pengendali Data Pribadi (dalam hal ini, *Tinder*).

a) Pasal 5 UUPDP: *"Subjek Data Pribadi dapat memberikan informasi mengenai identitas, dasar hukum, tujuan penggunaan, serta tanggung jawab pihak yang meminta Data Pribadi tersebut".*
Relevansi dengan *Tinder*: *Tinder* wajib menyediakan kebijakan privasi yang jelas dan mudah diakses, menjelaskan data apa yang dikumpulkan, mengapa dikumpulkan, dan bagaimana data tersebut digunakan.

b) Pasal 6 UUPDP: *"Subjek Data Pribadi memiliki hak untuk menambah, memperbarui, dan memperbaiki kesalahan atau ketidakakuratan Data Pribadi sesuai dengan tujuan pemrosesannya".*
Relevansi dengan *Tinder*: Pengguna *Tinder* harus memiliki kemampuan untuk mengedit profil mereka, memperbarui informasi, atau mengoreksi kesalahan.

c) Pasal 7 UUPDP: *"Subjek Data Pribadi dapat melakukan akses dan mendapatkan salinan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan".*
Relevansi dengan *Tinder*: Pengguna harus dapat meminta dan menerima salinan data pribadi mereka yang disimpan oleh *Tinder*.

d) Pasal 8 UUPDP: *"Subjek Data Pribadi berhak untuk menghentikan pemrosesan, menghapus, dan memusnahkan sesuai dengan peraturan perundang-undangan".*

Relevansi dengan *Tinder*: Pengguna harus memiliki opsi untuk menghapus akun mereka dan meminta penghapusan data pribadi mereka dari sistem *Tinder*.

e) Pasal 9 UUPDP: "Subjek Data Pribadi memiliki hak untuk mencabut persetujuan pemrosesan yang telah diberikan kepada Pengendali".
Relevansi dengan *Tinder*: Pengguna harus dapat menarik persetujuan mereka untuk pemrosesan data tertentu, meskipun ini mungkin membatasi fungsionalitas aplikasi.

f) Pasal 10 Ayat (1) UUPDP: "*Subjek Data Pribadi berhak untuk mengajukan keberatan terhadap keputusan yang dihasilkan melalui pemrosesan otomatis dan pemrofilan yang memiliki dampak signifikan"*.
Relevansi dengan *Tinder*: *Tinder* menggunakan algoritma untuk mencocokkan pengguna (pemrofilan). Pengguna harus memiliki hak untuk memahami bagaimana pemrofilan ini bekerja dan mengajukan keberatan jika merasa ada keputusan otomatis yang tidak adil atau merugikan.

g) Pasal 12 Ayat (1) UUPDP: "Subjek Data Pribadi memiliki hak untuk menuntut dan menerima kompensasi atas pelanggaran yang terjadi dalam pemrosesan Data Pribadi sesuai dengan peraturan perundang-undangan yang berlaku".
Relevansi dengan *Tinder*: Jika *Tinder* melanggar ketentuan UUPDP terkait pemrosesan data, pengguna berhak menuntut ganti rugi.

3) Kewajiban Pengendali Data Pribadi (Tinder)

Sebagai Pengendali Data Pribadi, *Tinder* memiliki sejumlah kewajiban yang ketat.

a) Pasal 20 Ayat (1) dan (2) UUPDP: "*Pengendali Data Pribadi harus memiliki landasan yang sah untuk melakukan pemrosesan, yang mencakup berbagai alasan seperti persetujuan dan kewajiban hukum*".
Relevansi dengan *Tinder*: *Tinder* harus mendapatkan persetujuan eksplisit dari pengguna untuk sebagian besar pemrosesan data, terutama data spesifik. Kebijakan privasi dan syarat penggunaan harus secara jelas menyatakan dasar hukum pemrosesan.

b) Pasal 21 Ayat (1) UUPDP: "*Pengendali Data Pribadi harus memberikan informasi lengkap terkait pemrosesan berdasarkan persetujuan, termasuk tujuan, jenis data, dan hak Subjek Data Pribadi*".
Relevansi dengan *Tinder*: *Tinder* harus transparan tentang semua aspek pemrosesan data mereka.

c) Pasal 22 Ayat (1) dan (4) UUPDP: "*Persetujuan pemrosesan Data Pribadi harus jelas, mudah dipahami, dan menggunakan bahasa yang sederhana, terutama jika mencakup tujuan tambahan*".
Relevansi dengan *Tinder*: Proses persetujuan di *Tinder* (misalnya, saat pendaftaran) harus memenuhi standar ini, tidak boleh ada klausul tersembunyi atau bahasa yang membingungkan.

d) Pasal 27 UUPDP: "*Pengendali Data Pribadi harus memastikan bahwa pemrosesan dilakukan dengan batasan yang jelas, sesuai dengan hukum, dan transparan kepada Subjek Data Pribadi*".
Relevansi dengan *Tinder*: *Tinder* hanya boleh mengumpulkan data yang relevan dan diperlukan untuk tujuan yang dinyatakan (misalnya, mencocokkan pengguna).

e) Pasal 29 Ayat (1) UUPDP: "Pengendali Data Pribadi memiliki tanggung jawab untuk memastikan bahwa Data Pribadi yang diproses tetap akurat, lengkap, dan konsisten".
Relevansi dengan *Tinder*: *Tinder* harus memiliki mekanisme untuk memastikan data profil pengguna akurat dan terkini.

f) Pasal 34 Ayat (1) dan (2) UUPDP: "*Pengendali Data Pribadi harus melakukan DPIA untuk pemrosesan yang berisiko tinggi, termasuk pengambilan keputusan otomatis dan pemrosesan data besar*".

Relevansi dengan *Tinder*: Mengingat penggunaan algoritma pencocokan dan pengumpulan data spesifik dalam skala besar, *Tinder* sangat mungkin diwajibkan untuk melakukan DPIA secara berkala.

g) Pasal 35 UUPDP: "*Pengendali Data Pribadi wajib melindungi Data Pribadi dengan menerapkan langkah-langkah keamanan yang memadai serta melaksanakan prosedur operasional yang tepat*".
Relevansi dengan *Tinder*: *Tinder* harus menerapkan langkah-langkah keamanan siber yang kuat untuk melindungi data pengguna dari pelanggaran, peretasan, atau akses tidak sah.

h) Pasal 36 UUPDP: "*Pengendali Data Pribadi bertanggung jawab untuk memastikan bahwa Data Pribadi tetap rahasia dan tidak diungkapkan kepada pihak yang tidak berwenang*".
Relevansi dengan *Tinder*: Data pengguna harus dijaga kerahasiaannya dan tidak diungkapkan kepada pihak yang tidak berwenang.

i) Pasal 46 Ayat (1) UUPDP: "Pengendali Data Pribadi diwajibkan untuk segera memberitahukan Subjek Data Pribadi dan otoritas perlindungan data dalam waktu 3x24 jam apabila terjadi pelanggaran terhadap Perlindungan Data Pribadi.
Relevansi dengan *Tinder*: Jika terjadi kebocoran data atau insiden keamanan, *Tinder* wajib segera memberitahukan kepada pengguna yang terdampak dan otoritas terkait.

4) Sanksi Administratif dan Pidana

UUPDP juga mengatur sanksi bagi pelanggaran.

a) Pasal 57 Ayat (1) dan (2) UUPDP: *"Pengendali Data Pribadi yang melanggar kewajiban dapat dikenakan berbagai sanksi administratif, termasuk peringatan, penghentian pemrosesan, penghapusan data, dan denda".*

b) Pasal 57 Ayat (3) UUPDP: *"Denda administratif maksimum untuk pelanggaran oleh Pengendali Data Pribadi adalah 2% dari pendapatan atau penerimaan tahunan".*
Relevansi dengan *Tinder*: Ketidakpatuhan *Tinder* terhadap kewajiban-kewajiban di atas dapat berujung pada sanksi finansial yang signifikan dan pembatasan operasional.

c) Pasal 65 UUPDP: "*Setiap individu dilarang secara hukum untuk* mendapatkan, mengungkapkan, atau memanfaatkan Data Pribadi milik orang lain untuk kepentingan pribadi atau pihak lain yang dapat menimbulkan kerugian".

d) Pasal 67 UUPDP: "Pelanggaran terhadap Pasal 65 dapat mengakibatkan sanksi pidana yang berupa hukuman penjara dan/atau denda".
Relevansi dengan *Tinder*: Meskipun ini lebih ditujukan pada individu yang menyalahgunakan data, *Tinder* sebagai platform juga harus memastikan bahwa fitur-fiturnya tidak memfasilitasi pelanggaran semacam ini.

5) Kelembagaan

Pasal 58 Ayat (2) UUPDP: "Perlindungan Data Pribadi diatur dan dilaksanakan oleh lembaga yang ditunjuk oleh Presiden".
Relevansi dengan *Tinder*: Lembaga ini akan menjadi otoritas pengawas yang akan menerima laporan, melakukan investigasi, dan menjatuhkan sanksi terhadap *Tinder* jika terjadi pelanggaran.

Pada kenyataan pemerintah melalui UUPDP setidaknya memberikan payung hukum terhadap korban tindak pidana love scammer, banyak beberapa faktor kekuatan dan kelemahan dalam melindungi hak korban. Berikut adalah analisis mengenai faktor kekuatan dan kelemahan dalam regulasi perlindungan data pribadi di Indonesia, beserta pasal dan ayat yang relevan dari Undang-Undang yang mengatur perlindungan data pribadi.

A) Kekuatan

1) Kerangka Hukum yang Jelas:

a) UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan kerangka hukum yang jelas untuk perlindungan data pribadi.
b) Pasal 1 Ayat 1 mendefinisikan data pribadi sebagai "setiap data yang dipergunakan untuk mengidentifikasi individu."

2) Hak Pemilik Data:
a) UU ini memberikan hak-hak tertentu kepada pemilik data, seperti hak untuk mengakses, memperbaiki, dan menghapus data pribadi mereka.
b) Pasal 26 menyatakan bahwa pemilik data memiliki hak untuk meminta informasi tentang penggunaan data pribadi mereka.

3) Sanksi Hukum yang Tegas:
a) UU ini menetapkan sanksi yang tegas bagi pelanggar, termasuk denda dan hukuman penjara.
b) Pasal 48 mengatur tentang sanksi administratif dan pidana bagi pelanggaran ketentuan perlindungan data pribadi.

B) Kelemahan

1) Definisi yang Tidak Jelas:
a) Beberapa istilah dalam UUPDP masih ambigu, seperti "data pribadi sensitif" dan "pengolahan data." Ketidakjelasan ini dapat menyulitkan penegakan hukum.
b) Pasal 1 Ayat 2 mendefinisikan data pribadi sensitif, tetapi tidak memberikan contoh yang jelas.

2) Kurangnya Penegakan Hukum:
a) Meskipun ada regulasi, penegakan hukum sering kali lemah. Banyak kasus love scam tidak ditindaklanjuti secara serius oleh pihak berwenang.
b) Pasal 49 menyebutkan bahwa penegakan hukum harus dilakukan oleh lembaga yang berwenang, tetapi implementasinya sering kali tidak optimal.

3) Keterbatasan Sumber Daya dan Kurangnya Edukasi dan Kesadaran
a) Penegakan hukum terhadap kejahatan siber memerlukan sumber daya yang memadai, baik dari segi teknologi maupun pelatihan. Banyak lembaga penegak hukum di Indonesia yang masih kekurangan dalam hal ini.
b) Meskipun kesadaran masyarakat meningkat, masih banyak individu yang tidak memahami risiko yang terkait dengan berbagi data pribadi di platform online. Ini membuat mereka rentan terhadap penipuan.

4) Regulasi yang Terfragmentasi:
Selain UUPDP, terdapat berbagai regulasi lain yang mengatur aspek-aspek tertentu dari perlindungan data dan kejahatan siber, yang dapat menyebabkan kebingungan dan inkonsistensi dalam penegakan hukum.

Dengan adanya UUPDP, diharapkan dapat memberikan kerangka hukum yang jelas untuk melindungi hak-hak pengguna. Namun, tantangan tetap ada, terutama dalam hal penegakan hukum dan kesadaran masyarakat mengenai risiko yang terkait dengan berbagi data pribadi. Kekuatan Undang-undang tersebut, seperti hak pemilik data dan sanksi tegas bagi pelanggar, harus diimbangi dengan upaya nyata dalam implementasi dan edukasi kepada masyarakat agar mereka dapat melindungi diri dari praktik penipuan asmara yang merugikan.

Di sisi lain, kelemahan dalam regulasi ini, seperti definisi yang tidak jelas dan kurangnya penegakan hukum, menunjukkan bahwa masih banyak yang perlu diperbaiki. Keterbatasan sumber daya dan kurangnya kesadaran masyarakat juga menjadi faktor yang memperburuk situasi ini.

KESIMPULAN

Berdasarkan UU Nomor 27 Tahun 2022, aplikasi *Tinder* memiliki dasar tanggung jawab besar dalam melindungi data pribadi penggunanya dengan memastikan transparansi dan persetujuan melalui kebijakan privasi yang jelas dan proses persetujuan yang eksplisit untuk setiap jenis data yang dikumpulkan serta tujuan pemrosesannya. Selain itu, *Tinder* harus memfasilitasi hak subjek data, seperti akses, perbaikan, penghapusan, dan penarikan persetujuan data oleh pengguna, serta menerapkan langkah-langkah keamanan siber yang kuat untuk mencegah pelanggaran data.

Lebih lanjut, *Tinder* wajib menjalankan akuntabilitas dengan melakukan penilaian dampak privasi dan memiliki mekanisme pelaporan insiden keamanan data secara cepat. Aplikasi ini juga harus memastikan kepatuhan terhadap penggunaan algoritma pemrofilan yang tidak diskriminatif dan memberikan hak keberatan kepada pengguna. Kegagalan memenuhi kewajiban tersebut dapat berakibat pada sanksi administratif berat, termasuk denda finansial yang signifikan, serta merusak reputasi dan kepercayaan pengguna.

REFERENSI

Anggraini, E. (2023). Sejauh Mana Keamanan Dating App dari Aksi Penipuan Online? *Bluepowertechnology.Com*. https://www.bluepowertechnology.com/news-detail/sejauh-mana-keamanan-dating-app-dari-aksi-penipuan-online

Arifiah, A. (2025). *Keterbukaan Diri Remaja Pengguna Aplikasi Kencan Tinder*. *19*(9).

Chandra, E. (2024). Efektivitas Pelaksanaan Penyidikan Tindak Pidana Penipuan Modus Love Scamming Di Kepolisian Resort Barelang Kota Batam. In *Universitas Islam Sultan Agung* (Vol. 8, Issue 5). Universitas Islam Sultan Agung.

Client Alert. (2025). *U . S . Cybersecurity and Data Privacy Review and Outlook – 2025*. U.S. Cybersecurity and Data Privacy Review and Outlook – 2025 - Gibson Dunn. https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-review-and-outlook-2025/

Davis, M., & Iapp, C. (2025). *Privacy Laws 2025 : Prepare for the 8 Laws Going into Effect*. 1–28.

Hidup, G., Lain, B., & Daerah, P. (2024). *Love Scam : Penipuan Berkedok Percintaa yang Perlu Diwaspadai*. 1–7.

Indonesia, G. U. U. (2025). *Behind the Screen: Navigating Cybersecurity Risks and Personal Data*. 1–19.

JDIH Kota Semarang. (2024). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP): Menjaga Keamanan dan Privasi Data Warga Negara*. 1–5. https://jdih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara

Khoirunnisa, K., Raharjo, E., & Tamza, F. B. (2025). *Perspektif Hukum Pidana dalam Penanggulangan Kejahatan Romance Scam : Analisis Peran Subdit V Siber Ditreskrimsus Polda Lampung*. *2*.

Mamonto, D. F. (2022). *Analisis Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022*. *33*(1), 1–12.

Muhamad, N. (2024). *Ini Aplikasi Kencan Online Terpopuler di Indonesia Awal 2024*. Databoks, Dalam Databoks.Katadata.Co.Id.

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection of Consumer Personal Data in E-Commerce According To Laws dan Regulations in Indonesia). *Jurnal Rechts Vinding*, *12*(2), 261–279.

Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023).

Analisis Perlindungan Data Pribadi Terkait Uu No.27 Tahun 2022. *Jurnal Serina Sosial Humaniora*, *1*(3), 145–153.

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, *6*(1), 976–982.

Simanungkalit, J. A. R., Hertadi, R., & Hosnah, A. ul. (2024). Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis*, *4*(2), 281–294. https://doi.org/10.37481/jmh.v4i2.754

Syahri, N. R. (2024). *Tinjauan hukum pidana terhadap penyalahgunaan aplikasi tinder yang menimbulkan tindak pidana penipuan*. Universitas Muhammadiyah Sumatera Utara.

tinder. (2024). *Keamanan di Tinder*. Https://Policies.Tinder.Com.

Titin, A., Nursanthy, R., & Kursiswanti, E. T. (2024). *Love Scamming Dalam Jerat Hukum Pidana*. *VIII*(2), 592–598.

Undang-Undang Dasar Negara Republik Indonesia 1945, 105 (1945).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Introduction to Turkish Business Law 457 (2022).

Widyarto, E. Y., & Hapsari, D. K. (2022). Analisis Modus Operandi Tindak Kejahatan Menggunakan Teknik Komunikasi Love Scam Sebagai Ancaman pada Keamanan Sistem Informasi. *Syntax Idea*, *4*(9), 1352. https://doi.org/10.36418/syntax-idea.v4i9.1959

Wijaya, A. D., & Anggriawan, T. P. (2022). Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi di Smartphone. *Inicio Legis*, *3*(1), 63–72. https://doi.org/10.21107/il.v3i1.14873

Wijayanti, L., & Hafidz, J. (2020). Penegakan Hukum Pelaku Tindak Pidana Dengan Modus Penipuan Berkedok Cinta Di Dunia Maya (Scammer Cinta) Law Enforcement of Criminal Actors Wit. *Konferensi Ilmiah Mahasiswa Unissula (Kimu) 3*, 278–292.

Zahra, R. A., Gunawan, R. S. P., & Fauzianti, N. A. (2022). Catfishing dan Implikasinya terhadap Romance Scam oleh Simon Leviev dalam Dokumenter Netflix “The Tinder Swindler” Menurut Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Kitab Undang- Undang Hukum Pidana. *Padjadjaran Law Review*, *10*(1), 1–52. https://doi.org/10.21608/pshj.2022.250026