

# Analisis Kebijakan Privasi dan Perlindungan Data Pribadi dalam Fitur Close Friend di Sosial Media

## [Analysis of Privacy Policy and Personal Data Protection in the Close Friend Feature on Social Media]

Mochammad Hubaib Al Ghifari <sup>1)</sup>, Lidya Shery Muis <sup>\*,2)</sup>

<sup>1)</sup> Program Studi Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

<sup>2)</sup> Program Studi Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

\*Email Penulis Korespondensi: [lidyasherymuis@umsida.ac.id](mailto:lidyasherymuis@umsida.ac.id)

**Abstract.** This study aims to analyze the extent to which the “Close Friend” feature on social media is able to provide protection for users' personal data from a legal perspective in Indonesia. Using normative legal research methods and a comparative approach, this study examines privacy policies on several popular platforms such as Instagram, WhatsApp, TikTok, LINE, Facebook, and Snapchat. The results of the analysis show that the “Close Friend” feature reflects the application of the privacy by design principle that allows users to control access to personal content. However, even though technical protection is available, the risk of content misuse remains if user awareness is low. This feature is in line with the principles in the Personal Data Protection Law (Law No. 27 of 2022), but it needs to be accompanied by digital education and shared responsibility between the platform and users to maintain privacy optimally.

**Keywords** - privacy policy, close friend, social media

**Abstrak.** Penelitian ini bertujuan untuk menganalisis sejauh mana fitur “Close Friend” pada media sosial mampu memberikan perlindungan terhadap data pribadi pengguna dalam perspektif hukum di Indonesia. Dengan menggunakan metode penelitian hukum normatif dan pendekatan komparatif, penelitian ini menelaah kebijakan privasi di beberapa platform populer seperti Instagram, WhatsApp, TikTok, LINE, Facebook, dan Snapchat. Hasil analisis menunjukkan bahwa fitur “Close Friend” mencerminkan penerapan prinsip privacy by design yang memungkinkan pengguna mengontrol akses terhadap konten pribadi. Namun, meskipun tersedia perlindungan teknis, risiko penyalahgunaan konten tetap ada jika kesadaran pengguna rendah. Fitur ini selaras dengan prinsip-prinsip dalam Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022), namun perlu diiringi edukasi digital dan tanggung jawab bersama antara platform dan pengguna untuk menjaga privasi secara optimal.

**Kata Kunci** - kebijakan privasi, close friend, media sosial

### I. PENDAHULUAN

Dalam perkembangan teknologi, media sosial muncul sebagai saran berkomunikasi gaya baru. Hal ini tentu berpotensi terjadi penyalahgunaan data pada saat kegiatan interaksi antara pengguna media sosial. Hal ini dapat terjadi apabila pengguna merasa informasi maupun data yang tertera maupun dicantumkan dalam jejaring sosial tersebut, digunakan oleh pihak lain, untuk tujuan yang dianggap mengganggu, membahayakan bahkan mengancam orang lain. Berdasarkan hal itu maka, pemilik situs jejaring sosial membuat kebijakan privasi (*Privacy Policy*) yang memuat ketentuan mengenai sejauh apa data atau informasi dari pengguna jejaring sosial dapat diakses atau diketahui oleh pihak selain pengguna akun itu sendiri.[1] Dalam era ini, segala sesuatu dapat dikendalikan melalui jaringan internet dan perangkat yang saling terhubung, yang meningkatkan produktivitas, membangun hubungan sosio-ekonomi, dan mempermudah berbagai aspek kehidupan. Revolusi ini telah menciptakan peluang baru sekaligus tantangan, terutama dalam hal privasi dan perlindungan data pribadi. Media sosial, sebagai salah satu produk dari kemajuan TIK, telah menjadi bagian integral dari kehidupan masyarakat.

*Close friend* adalah individu yang memiliki hubungan emosional yang sangat dekat dan personal dengan seseorang, biasanya ditandai dengan tingkat kepercayaan yang tinggi, kedekatan emosional, dan dukungan dalam berbagai aspek kehidupan.[2] Hubungan dengan *close friend* sering kali melibatkan komunikasi yang lebih mendalam, berbagi pengalaman pribadi, serta saling memahami kekuatan dan kelemahan masing-masing tanpa rasa penilaian. Berbeda dengan teman biasa, hubungan *close friend* cenderung lebih intim dan bertahan lama, sering kali menjadi tempat seseorang untuk mendapatkan dukungan moral, berbagi kebahagiaan, atau melewati masa sulit bersama.

Platform seperti *WhatsApp*, *Tiktok*, *Instagram*, *Line*, *facebook* dan *snapchat*, memungkinkan pengguna untuk berinteraksi, berbagi, dan menciptakan konten tanpa batasan ruang dan waktu. Hal ini menunjukkan bahwa media sosial bukan hanya alat komunikasi, tetapi juga menjadi bagian dari gaya hidup dan interaksi sosial masyarakat modern. Fitur ini memberikan rasa aman bagi pengguna untuk berbagi momen pribadi tanpa khawatir dilihat oleh publik luas. Namun, meskipun fitur ini menawarkan rasa privasi yang lebih tinggi, ada kekhawatiran terkait perlindungan data pribadi dan potensi penyalahgunaan konten yang dibagikan. Pengguna masih harus berhati-hati karena data yang dibagikan tetap bisa berisiko jika disalahgunakan oleh pihak yang tidak bertanggung jawab.[3]

*Instagram*, *Tiktok*, *WhatsApp*, *Line*, *Facebook* dan *Snapchat* sangat populer di penduduk Indonesia menggunakan platform ini. Kebijakan privasi *Instagram* menjadi fokus utama dalam memastikan data pribadi pengguna terlindungi dengan baik. Beberapa hal mengenai kebijakan privasi yang perlu diketahui fitur *close friend* memungkinkan pengguna untuk membatasi konten yang dibagikan agar hanya bisa dilihat oleh orang-orang tertentu. Dan juga Pengguna dapat memilih siapa saja yang bisa melihat unggahannya, dengan pilihan "Everyone" (semua orang) atau "Close Friends". Sehingga pengaturan fitur *close friends* tidak akan memengaruhi privasi akun *Instagram* atau mengubah preferensi berbagi konten di *Facebook*. Meskipun tidak ada cara langsung untuk mengetahui apakah seseorang sudah menambahkan nama pengguna dalam daftar *close friends*. *Instagram* tidak memberikan notifikasi ketika seseorang menambahkan nama pengguna dalam daftar *close friends*. Dengan meningkatnya kasus kebocoran data dan penyalahgunaan informasi pribadi, ada kebutuhan mendesak untuk kebijakan privasi yang lebih ketat dan edukasi yang lebih baik bagi pengguna. Kesadaran pengguna tentang pentingnya menjaga data pribadi mereka sering kali masih rendah, yang membuat mereka rentan terhadap berbagai bentuk penipuan dan penyalahgunaan data.

Sedangkan perbandingan kebijakan privasi pada aplikasi *WhatsApp* menyediakan berbagai fitur keamanan untuk melindungi privasi pengguna, seperti enkripsi *end-to-end*, yang memastikan hanya penerima pesan yang dapat membaca kontennya, termasuk *WhatsApp* sendiri; kunci chat, yang memungkinkan pengguna mengamankan percakapan tertentu dengan kode unik, sidik jari, atau *Face ID*; verifikasi dua langkah, yang menambah lapisan keamanan dengan PIN enam digit; dan pengaturan privasi, yang memungkinkan pengguna mengontrol siapa saja yang dapat melihat status online, foto profil, dan informasi pribadi lainnya.[4]

Dan yang terakhir kebijakan privasi pada aplikasi *TikTok* memberikan pengguna kontrol privasi yang lebih besar melalui fitur *close friends*, memungkinkan mereka memilih siapa saja yang dapat melihat konten pribadi mereka, sekaligus menggunakan enkripsi untuk melindungi data saat transit dan saat istirahat di pusat data yang aman. Informasi yang dikumpulkan dari fitur ini digunakan untuk meningkatkan pengalaman pengguna, merekomendasikan konten relevan, dan menjaga keamanan akun dengan memitigasi spam serta aktivitas berbahaya. Selain itu, *TikTok* berkomitmen melindungi privasi pengguna melalui kebijakan privasi yang komprehensif, mendorong pengguna untuk memahaminya agar mengetahui bagaimana data mereka dikelola. Pada keamanan setiap aplikasi juga berbeda beda yang dimana *Instagram* menawarkan keamanan melalui enkripsi pada pesan dan *stories*. Hanya orang yang ada dalam daftar yang dapat melihat konten yang dibagikan. *TikTok* telah memperketat privasi dengan menyediakan pengaturan bagi satu pengguna untuk memilih siapa yang bisa melihat video mereka, mengomentari, dan berinteraksi dengan konten. *WhatsApp* mengimplementasikan enkripsi *end-to-end* untuk semua pesan dan status, sehingga hanya penerima yang dimaksud dapat melihat konten.[5]

Kebocoran data pribadi dapat menimbulkan konsekuensi serius, termasuk pencurian identitas, penipuan, dan pelanggaran privasi lainnya. Fitur "*Close Friend*" pada platform komunikasi seperti *Line* dirancang untuk memberikan pengalaman berbagi yang lebih personal dan terarah. Namun, penggunaan fitur ini membawa tantangan tersendiri terkait kebijakan privasi dan perlindungan data pribadi. Dalam fitur ini, pengguna dapat memilih lingkup audiens terbatas untuk berbagi konten, sehingga menciptakan ruang yang lebih privat dibandingkan dengan berbagi ke seluruh daftar kontak. Kebijakan privasi yang mendasari fitur ini bertujuan untuk melindungi informasi pribadi pengguna dari penyalahgunaan, baik oleh pihak lain dalam daftar kontak maupun oleh pihak ketiga.[6] Hal ini melibatkan pengaturan akses, perlindungan terhadap pelacakan data, dan transparansi terkait bagaimana data pengguna dikelola oleh platform.

Dalam konteks ini, penting untuk mengevaluasi apakah implementasi fitur "*Close Friend*" di *Line* sudah sesuai dengan prinsip perlindungan data pribadi, termasuk mematuhi regulasi seperti *General Data Protection Regulation (GDPR)* atau Undang-Undang Perlindungan Data Pribadi di Indonesia, untuk memastikan keamanan dan privasi pengguna tetap terjaga. Fitur *close friend* di *Facebook* merupakan salah satu mekanisme yang dirancang untuk memberikan pengguna kontrol lebih atas informasi yang mereka bagikan di platform. Dalam fitur ini, pengguna dapat memilih lingkaran pertemanan tertentu untuk menerima konten yang lebih personal atau eksklusif, seperti pembaruan status, foto, atau video.[7] Namun, seiring dengan peningkatan penggunaan fitur ini, muncul pula perhatian terhadap aspek privasi dan perlindungan data pribadi. Kebijakan privasi yang diterapkan harus memastikan bahwa data yang dibagikan melalui fitur *close friend* hanya dapat diakses oleh individu yang diizinkan, tanpa adanya risiko penyalahgunaan atau pelanggaran.

Perlindungan data pribadi menjadi sangat penting untuk menjaga kepercayaan pengguna, menghindari kebocoran informasi, dan memenuhi standar hukum yang berlaku, seperti yang diatur dalam undang-undang perlindungan data

di berbagai negara. Dengan demikian, pendekatan yang transparan dan komprehensif terhadap kebijakan privasi akan menjadi fondasi utama dalam menjaga keamanan dan kenyamanan pengguna. Fitur "teman dekat" telah menjadi elemen penting dalam berbagai aplikasi media sosial untuk memberikan pengguna pengalaman yang lebih personal. Fitur ini memungkinkan pengguna untuk berbagi konten secara selektif dengan grup tertentu sambil menjaga privasi dan memungkinkan interaksi yang lebih personal. Fitur ini telah diterapkan dalam berbagai bentuk dan nama di aplikasi populer seperti *WhatsApp*, *Instagram*, *TikTok*, *Line*, *Facebook*, dan lainnya. Setiap platform memiliki fitur uniknya sendiri yang memungkinkannya merancang fungsi ini sesuai dengan kebutuhan dan kebiasaan penggunanya. Di *WhatsApp*, fitur teman dekat sering kali diterapkan melalui opsi "status khusus", yang memungkinkan pengguna memilih siapa yang dapat melihat status mereka. *Instagram* kini secara eksplisit memperkenalkan fitur "*close friend*". Hal ini memungkinkan pengguna untuk berbagi cerita hanya dengan daftar teman dekat yang telah ditentukan sebelumnya. *TikTok* memberi penekanan kuat pada konten publik, tetapi memberi Anda opsi untuk berbagi video hanya dengan teman-teman tertentu melalui pengaturan privasi.

Aplikasi *Line* mengambil pendekatan serupa dengan fitur pengaturan timeline, yang memungkinkan pengguna menentukan audiens tertentu untuk setiap unggahan. *Facebook* sekarang menjadi platform yang lebih matang, dengan fitur teman khusus yang memungkinkan pengguna mengontrol siapa yang dapat melihat kiriman mereka. Pendekatan-pendekatan yang berbeda ini mencerminkan upaya platform untuk memberi pengguna kontrol lebih besar atas privasi mereka sambil tetap menjaga aspek sosial yang menjadi inti media sosial. Memahami karakteristik masing-masing fitur "*close friend*" aplikasi dapat memberikan pemahaman lebih mendalam tentang bagaimana platform teknologi membentuk pola interaksi digital dan preferensi pengguna.[8]

Penelitian ini bertujuan untuk memahami sejauh mana fitur "*close friend*" menawarkan perlindungan terhadap data pribadi dan privasi pengguna dalam perspektif hukum yang berlaku. Penelitian ini juga bertujuan untuk mengeksplorasi mekanisme hukum yang tersedia bagi pengguna ketika konten yang dibagikan dalam fitur "*close friend*" disebarluaskan tanpa izin. Maka dari itu peneliti membahas penelitian yang berjudul analisis kebijakan privasi dan perlindungan data pribadi dalam fitur *close friend* di social media.

## II. METODE

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif dengan pendekatan perundang-undangan dan juga menggunakan metode komparatif dengan membandingkan kebijakan privasi dan perlindungan data pribadi pada fitur serupa *Close Friends* di berbagai aplikasi media sosial, seperti *WhatsApp*, *Instagram*, *LINE*, *TikTok*, *Facebook* dan *Snapchat*. Perbandingan ini mencakup aspek pengaturan akses, perlindungan terhadap penyebaran ulang konten, konsekuensi hukum yang tercantum dalam kebijakan layanan, serta transparansi pengelolaan data pribadi. Metode ini dipilih karena sesuai dengan tujuan penelitian untuk mengkaji kebijakan privasi dan perlindungan data pribadi dalam fitur *Close Friends* di *Instagram*, yang sangat berkaitan dengan aturan hukum yang berlaku di Indonesia. Pendekatan normatif ini memungkinkan peneliti untuk mengeksplorasi dan menganalisis bahan hukum yang ada guna mendapatkan gambaran yang komprehensif tentang bagaimana undang-undang dan peraturan terkait diimplementasikan dalam konteks perlindungan data pribadi di media sosial. Langkah pertama dalam penelitian ini adalah mengumpulkan bahan hukum primer dan sekunder. Bahan hukum primer mencakup undang-undang, peraturan, dan kebijakan yang berlaku, seperti Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Sumber-sumber ini menjadi dasar utama dalam analisis karena memberikan kerangka hukum yang jelas terkait dengan perlindungan data pribadi di Indonesia. Selain itu, bahan hukum sekunder seperti jurnal ilmiah, artikel, dan laporan penelitian sebelumnya juga dikumpulkan untuk mendukung analisis dan memberikan perspektif tambahan. Setelah bahan hukum terkumpul, langkah selanjutnya adalah mengkaji dan menganalisis isi dari undang-undang dan peraturan tersebut. Penelitian ini menggunakan teknik analisis isi (content analysis) untuk memahami bagaimana ketentuan hukum yang ada mengatur perlindungan data pribadi di platform media sosial, khususnya *Instagram*. Analisis ini mencakup penelaahan mendalam terhadap pasal-pasal yang relevan dalam UU ITE dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016.

## III. HASIL DAN PEMBAHASAN

### A. Fitur *Close Friend* Secara Hukum Memberikan Perlindungan Privasi

Fitur "*close friend*" dan fitur serupa di berbagai platform media sosial seperti *Instagram*, *TikTok*, *Facebook*, *WhatsApp*, *LINE*, dan *Snapchat* adalah contoh nyata dari prinsip *privacy by design*. Prinsip ini adalah cara pengembangan sistem yang sejak awal memperhatikan perlindungan privasi pengguna. Dengan adanya fitur ini, pengguna bisa mengatur siapa saja yang boleh melihat konten tertentu terutama konten yang bersifat pribadi atau

sensitif. Hal ini membantu pengguna menjalankan hak mereka sebagai subjek data untuk mengontrol informasi pribadi mereka, sesuai dengan UU No 27/2022 tentang Perlindungan Data Pribadi di Indonesia. Dalam konteks ini, fitur close friend berfungsi sebagai alat teknis yang mendukung penerapan.[9]

UU No. 27/2022 menekankan bahwa setiap individu memiliki hak untuk membatasi, mengatur, bahkan menarik kembali data pribadi yang telah mereka bagikan. Fitur seperti *close friend* di Instagram atau "hanya bagikan dengan..." di WhatsApp, memberikan ruang aktualisasi atas hak-hak tersebut. *platform* ini menjalankan kewajiban sebagai pengendali data (data controller) yang harus memberikan sarana kepada pengguna untuk mengatur arus data pribadi mereka secara aman dan selektif. Ketika fitur-fitur ini digunakan secara tepat, risiko penyalahgunaan atau distribusi data tanpa izin menjadi lebih kecil.

Fitur *close friend* memberikan instrumen teknis untuk melindungi privasi, perlindungan hukum tidak hanya bergantung pada desain sistem, tetapi juga pada perilaku pengguna dan pengawasan platform. UU PDP juga menekankan pentingnya prinsip minimisasi data dan pembatasan tujuan (purpose limitation), yang berarti data pribadi tidak boleh dibagikan atau digunakan di luar dari tujuan yang telah ditentukan oleh pemilik data. Namun, dalam praktiknya, masih terdapat celah penyalahgunaan seperti tangkapan layar atau penyebaran ulang oleh pihak ketiga. Oleh karena itu, penting bagi platform untuk memberikan edukasi kepada pengguna tentang risiko residu privasi dan pentingnya kesadaran digital dalam penggunaan fitur seperti *close friend*, agar perlindungan privasi dapat tercapai secara maksimal.[10]

Fitur *close friend* dan variasinya secara keseluruhan menunjukkan perkembangan *platform* media sosial dalam menciptakan ruang digital yang lebih pribadi dan terkendali. Dalam hal hukum, fitur ini membantu memenuhi hak atas data pribadi dan menunjukkan bahwa platform mematuhi regulasi perlindungan data. Keberadaan fitur ini menunjukkan bahwa media sosial tidak hanya digunakan untuk berkomunikasi secara umum, tetapi juga bisa sebagai tempat berkomunikasi yang lebih dekat dan pribadi, yang harus diatur dengan etika perlindungan data. Oleh karena itu, fitur *close friend* bisa dianggap sebagai bentuk teknologi yang mendukung perlindungan privasi, selama pengguna dan platform saling bertanggung jawab dalam menjaga keamanan data serta transparansi dalam mengelola datanya.[11]

Social Media	Application Massanger
<p>Instagram</p> <ul style="list-style-type: none"> <li>a. Fungsi fitur <i>close friend</i></li> <li>b. Pengaturan daftar teman dekat</li> <li>c. Privasi dan kontrol</li> <li>d. Pelanggaran dan penyalahgunaan</li> <li>e. Ketentuan dan penegakan hukum</li> <li>f. Tanggung jawab pengguna</li> </ul> <p>Tiktok</p> <ul style="list-style-type: none"> <li>a. Pengaturan visibilitas konten</li> <li>b. Direct message (DM)</li> <li>c. Kepatuhan terhadap regulasi perlindungan data</li> <li>d. Tanggung jawab pengendali data (data controller)</li> <li>e. Arah dan edukasi privasi</li> </ul> <p>Facebook</p> <ul style="list-style-type: none"> <li>a. Pengaturan akun</li> <li>b. Konten bersifat sementara</li> <li>c. Perlindungan privasi akun</li> <li>d. Kesadaran pengguna</li> </ul>	<p>Whatsapp</p> <ul style="list-style-type: none"> <li>a. Pengaturan privasi fitur status</li> <li>b. Sistem chat dan privasi</li> <li>c. Fitur privasi tambahan</li> <li>d. Keterhubungan dengan nomor telepon</li> <li>e. Kelemahan dalam perlindungan privasi</li> </ul> <p>Line</p> <ul style="list-style-type: none"> <li>a. Fitur line story dan privasi yang ketat</li> <li>b. Penhapus line voom sebagai langkah praktisi</li> </ul> <p>Snapchat</p> <ul style="list-style-type: none"> <li>a. Pemilihan akun</li> <li>b. Jumlah story terbatas</li> <li>c. Kolaborasi konten</li> <li>d. Perlindungan privasi</li> <li>e. Transparasi interaksi</li> </ul>

Tabel 1. Perbedaan Media Sosial dengan Aplikasi Perpesanan

Sebagaimana dapat dilihat pada Tabel 1 bahwa media sosial lebih menekankan pada pengaturan visibilitas konten dan kontrol terhadap audiens, dengan risiko penyebaran konten yang lebih luas apabila tidak diatur secara tepat oleh pengguna. *Platform* seperti Instagram, TikTok, dan Facebook memberikan kebebasan lebih besar dalam memilih siapa yang dapat mengakses konten, tetapi hal ini juga menuntut tanggung jawab yang tinggi dari pengguna untuk menjaga keamanan dan etika dalam berbagi informasi. Di sisi lain, aplikasi messenger seperti WhatsApp, LINE, dan Snapchat lebih fokus pada keamanan komunikasi personal melalui fitur yang membatasi interaksi hanya dengan kontak tertentu.

Terdapat celah dalam perlindungan metadata, terutama yang berkaitan dengan keterkaitan identitas pengguna dengan nomor telepon, yang dapat dimanfaatkan secara tidak sah jika tidak dikelola dengan baik.

Kepatuhan terhadap UU No. 27/2022 menjadi tolak ukur penting dalam menilai tanggung jawab platform digital sebagai pengendali data pribadi. Prinsip-prinsip seperti transparansi, pembatasan tujuan pemrosesan data, keamanan sistem, serta perlindungan hak subjek data menjadi fondasi yang harus dijunjung tinggi oleh setiap penyedia layanan digital. Selain itu, peningkatan edukasi dan kesadaran privasi kepada pengguna menjadi hal yang krusial, mengingat peran aktif masyarakat sangat berpengaruh dalam menjaga keamanan data pribadi mereka sendiri. Regulasi perlindungan data pribadi harus diterapkan secara konsisten oleh seluruh penyedia layanan digital. Penerapan tersebut harus dibarengi dengan pengawasan dan pembinaan yang ketat dari otoritas berwenang, guna menjamin terciptanya lingkungan digital yang aman, transparan, dan nyaman bagi seluruh pengguna.[12]

WhatsApp dipilih sebagai salah satu platform yang relevan dalam penerapan regulasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya setelah perubahan melalui UU No. 1/2024, karena secara teknis dan sistemik telah mengadopsi berbagai prinsip perlindungan data pribadi dan keamanan informasi elektronik sebagaimana diatur dalam pasal-pasal dalam UU tersebut. Salah satu alasan utamanya adalah fitur privasi yang kuat, seperti pengaturan visibilitas status (“hanya dibagikan kepada...”), *enkripsi end-to-end*, verifikasi dua langkah, dan kunci chat, yang mencerminkan penerapan prinsip *privacy by design* dan pengendalian akses data oleh subjek data, sejalan dengan Pasal 26 ayat (1) UU ITE yang mewajibkan penggunaan data pribadi atas persetujuan pemilik data. WhatsApp memberikan pengguna kemampuan untuk menghapus pesan yang telah dikirim baik dari sisi pengirim maupun penerima (fitur “hapus untuk semua”), yang sejalan dengan Pasal 26 ayat (2) UU ITE yang menyatakan bahwa individu berhak meminta penghapusan informasi yang tidak sesuai. WhatsApp juga memastikan bahwa tidak ada pihak ketiga yang dapat mengakses isi komunikasi antar pengguna berkat sistem enkripsi yang canggih, yang menjawab ketentuan Pasal 30 tentang larangan akses ilegal terhadap sistem elektronik orang lain.[13]

Kemudian untuk penyebaran ulang konten seperti status pribadi yang dibagikan melalui pengaturan terbatas mirip fitur “*Close Friend*”, WhatsApp menegaskan pentingnya persetujuan dan etika dalam berbagi ulang konten digital. Jika pelanggaran terjadi, seperti penyebaran konten pribadi tanpa izin, maka pengguna yang menyalahgunakan tersebut dapat dijerat dengan Pasal 27 ayat (1) tentang distribusi konten yang melanggar kesesuaian atau privasi, serta Pasal 32 tentang perusakan atau pemindahan informasi elektronik tanpa hak. Oleh karena itu, WhatsApp dianggap sebagai platform yang tidak hanya menyediakan fitur teknis untuk perlindungan privasi, tetapi juga secara substansi memfasilitasi pemenuhan hak-hak hukum pengguna sesuai ketentuan dalam UU ITE.

Berdasarkan analisis fitur-fitur perlindungan privasi dalam kategori selektif berbagi seperti *Close Friend*, WhatsApp dan Instagram menunjukkan pendekatan yang serupa tetapi keduanya memiliki tingkat keamanan yang berbeda. WhatsApp menyediakan fitur berbagi status dengan pengaturan “hanya dibagikan kepada...” yang secara fungsi sebanding dengan fitur *Close Friend* di Instagram.[14] Tetapi keunggulan utama WhatsApp terletak pada penggunaan *enkripsi end-to-end* untuk semua pesan dan status yang dibagikan, sehingga hanya pengirim dan penerima yang dapat melihat konten tersebut. Selain itu, WhatsApp juga menyediakan fitur penghapusan pesan dua arah, kunci chat, dan verifikasi dua langkah yang memperkuat kontrol pengguna terhadap data pribadinya. Penerapan fitur-fitur ini sejalan dengan ketentuan Pasal 26 ayat (1) dan (2) UU ITE tentang persetujuan dan hak penghapusan data pribadi, serta Pasal 30 sampai 32 UU ITE tentang larangan akses ilegal terhadap sistem elektronik. Sementara fitur *Close Friend* di Instagram memungkinkan pengguna membagikan konten hanya kepada daftar teman dekat yang telah dipilih, memberikan perlindungan berbasis kontrol akses. Fitur ini mendukung prinsip pembatasan tujuan penggunaan data, hak atas akses terbatas, dan akuntabilitas pengendali data sebagaimana diatur dalam Pasal 16, 20, dan 33 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Secara teknis Instagram tidak menggunakan *enkripsi end-to-end* pada konten *Close Friend*, sehingga potensi penyalahgunaan seperti tangkapan layar atau perekaman layar oleh pihak ketiga tetap menjadi celah keamanan.[15] Apabila dibandingkan secara menyeluruh dari sisi regulasi dan perlindungan teknis, WhatsApp dapat dinilai sebagai platform yang paling aman dalam implementasi fitur selektif berbagi, sedangkan Instagram tetap unggul dalam kategori media sosial, tetapi dengan tingkat perlindungan yang lebih terbatas secara teknis.

## B. Apa Upaya Hukum Yang Dapat Dilakukan Apabila Konten Dalam Fitur Close Friend Disebarluaskan Tanpa Izin

Penyebaran konten pribadi yang dibagikan melalui fitur terbatas tanpa izin dari pemiliknya merupakan pelanggaran hak privasi yang serius di semua *platform* digital, baik itu Instagram, Facebook, TikTok, WhatsApp, LINE, maupun Snapchat. Masing-masing aplikasi menyediakan fitur yang memungkinkan pengguna membagikan konten kepada audiens tertentu saja seperti fitur *Close Friends* di Instagram, *Custom Audience* di Facebook, *private video settings* di TikTok, *Status* di WhatsApp, *Story privacy* di LINE, dan *private Story* di Snapchat. Fitur-fitur ini memberikan kendali atas siapa yang dapat melihat informasi yang bersifat pribadi atau sensitif.[16] Dalam praktiknya kepercayaan terhadap *audiens* terbatas ini tidak selalu dijaga. Banyak kasus di mana konten yang dibagikan secara terbatas disimpan menggunakan *screenshot* atau *screen recording*, lalu disebarluaskan ke pihak ketiga tanpa

persetujuan pemilik konten. Tindakan ini menciptakan apa yang dalam teori *Communication Privacy Management* disebut sebagai turbulensi privasi, yaitu pelanggaran atas aturan privasi yang sebelumnya telah disepakati secara implisit antara pemilik informasi dan penerima. Jika konten yang disebarluaskan tersebut mengandung unsur data pribadi, hal yang memalukan, atau bersifat merugikan secara psikologis maupun reputasi, korban dapat menempuh sejumlah upaya hukum. Secara administratif, pelanggaran ini dapat dilaporkan kepada masing-masing platform melalui fitur *report* atau pusat bantuan pengguna. Selain itu, korban dapat melaporkan kejadian tersebut kepada Kementerian Komunikasi dan Informatika (Kominfo) melalui situs [aduankonten.id](http://aduankonten.id). Dari sisi hukum pidana, penyebaran konten pribadi tanpa izin dapat diberat melalui Pasal 26 dan Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik, serta Pasal 65 UU No 27/2022 tentang Perlindungan Data Pribadi (UU PDP) yang melindungi hak atas kendali data pribadi di ruang digital. Jika korban mengalami kerugian, ia juga dapat mengajukan gugatan perdata berdasarkan Pasal 1365 KUHPerdata atas dasar perbuatan melawan hukum (PMH). Dalam kasus khususnya bila pelaku dikenal secara personal, korban juga dapat memulai langkah non-litigasi seperti mengirimkan surat somasi atau melakukan mediasi.[17]

Dalam menghadapi pelanggaran privasi seperti penyebaran konten terbatas tanpa izin pada platform Instagram, Facebook, TikTok, WhatsApp, LINE, dan Snapchat, pengguna juga dapat menempuh jalur hukum perdata untuk menuntut ganti rugi. Berdasarkan Pasal 26 UU No. 19/2016 tentang Perubahan atas UU NO 1/2024, setiap orang berhak atas perlindungan data pribadi dalam sistem elektronik. Jika pelanggaran tersebut menyebabkan kerugian secara materiil maupun immateriil, korban dapat mengajukan gugatan ke pengadilan negeri atas dasar perbuatan melawan hukum (PMH) sebagaimana diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata). Untuk memperkuat posisi hukum, sebaiknya korban didampingi oleh pengacara, serta mengumpulkan bukti penyebaran dan identitas pelaku secara lengkap dan sah.[18]

Terdapat jalur hukum pidana juga dapat ditempuh apabila konten yang disebarluaskan mengandung unsur kesusilaan, pencemaran nama baik, atau akses ilegal. Pasal 27 ayat (1) dan Pasal 45 ayat (1) UU No 1/2024 dapat digunakan jika isi konten melanggar kesusilaan, sedangkan Pasal 30 hingga 32 dapat diterapkan jika akses terhadap konten dilakukan secara tanpa hak atau melanggar keamanan sistem elektronik. Lebih jauh, Pasal 65 UU No. 27/2022 tentang Perlindungan Data Pribadi memberikan dasar hukum yang kuat untuk menindak pelaku pelanggaran privasi secara pidana maupun administratif. Korban bisa melaporkan kasusnya ke unit Siber Polisi (Direktorat Tindak Pidana Siber Bareskrim Polri) atau ke Kementerian Komunikasi dan Informatika (Kominfo) untuk meminta pemutusan akses atau penghapusan konten yang sudah menyebar.[19] Selain itu, jika korban tidak ingin mengambil jalur peradilan, mereka juga bisa memilih jalur non-peradilan seperti somasi atau mediasi, terutama jika pelaku dikenal secara pribadi. Somasi bisa berupa surat peringatan hukum yang meminta pelaku menghapus konten yang disebarluaskan dan tidak mengulanginya lagi. Sementara itu, mediasi informal dapat dilakukan melalui pihak ketiga sebagai cara menyelesaikan masalah secara damai, agar konflik tidak membesar. Dalam era digital, pengguna sebaiknya memanfaatkan fitur seperti *Close Friend* atau pengaturan privasi dengan sangat hati-hati, hanya untuk orang-orang yang benar-benar bisa dipercaya. Lebih baik hindari berbagi konten sensitif, meskipun dalam lingkungan yang terbatas atau terenkripsi. Selain itu, perlu dilakukan pengecekan rutin terhadap daftar audiens privat untuk memastikan tidak ada pihak yang bisa menyalahgunakan kepercayaan. Pengguna juga bisa menggunakan akun pribadi yang hanya terbuka untuk orang tertentu, atau bahkan memisahkan akun publik dengan akun pribadi, agar bisa membatasi batasan antara kehidupan pribadi dan dunia online.[20]

#### IV. SIMPULAN

Berdasarkan hasil penelitian, perlindungan data pribadi pengguna melalui fitur *Close Friend* di media sosial telah menerapkan prinsip *privacy by design* yang memberi pengguna kendali atas siapa yang dapat mengakses konten pribadi. Penerapan ini selaras dengan ketentuan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, meskipun efektivitasnya tetap bergantung pada kesadaran dan perilaku pengguna serta komitmen platform dalam menjaga keamanan data. Apabila konten dalam fitur *Close Friend* disebarluaskan tanpa izin, pengguna memiliki beberapa jalur upaya hukum yang dapat ditempuh, antara lain jalur pidana berdasarkan ketentuan UU ITE dan UU PDP untuk menindak pelaku penyebaran tanpa izin, jalur perdata melalui gugatan *perbuatan melawan hukum* sebagaimana diatur dalam Pasal 1365 KUHPerdata untuk menuntut ganti rugi, serta jalur administratif dengan melapor ke platform penyedia layanan atau Kementerian Komunikasi dan Informatika. Selain itu, upaya non-litigasi seperti somasi atau mediasi juga dapat dilakukan apabila pelaku dikenal secara personal. Dengan demikian, fitur *Close Friend* dapat dipandang sebagai inovasi teknologi yang mendukung perlindungan privasi pengguna, asalkan didukung oleh regulasi yang efektif, pengawasan ketat, serta edukasi digital yang memadai.

## UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Universitas Muhammadiyah Sidoarjo, khususnya Program Studi Ilmu Hukum, yang telah memberikan dukungan akademik, fasilitas, serta akses terhadap sumber hukum dan literatur yang relevan dalam penyusunan penelitian ini. Dukungan institusi ini menjadi fondasi penting dalam kelancaran proses analisis dan penyusunan naskah.

Ucapan terima kasih juga disampaikan kepada pihak-pihak yang telah membantu dalam penyediaan data, baik berupa referensi regulasi, publikasi ilmiah, maupun dokumen pendukung lainnya yang menjadi sumber informasi utama dalam penelitian ini. Kontribusi tersebut sangat membantu dalam memastikan bahwa analisis yang dilakukan didasarkan pada data yang valid dan terkini, sehingga hasil penelitian dapat memberikan manfaat bagi pengembangan kajian hukum terkait perlindungan data pribadi di era digital.

Akhir kata, penulis menyadari bahwa skripsi ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk perbaikan di masa yang akan datang. Semoga penelitian ini dapat memberikan kontribusi positif terhadap pemahaman hukum perlindungan data pribadi, khususnya dalam konteks fitur-fitur digital seperti *Close Friend* yang semakin relevan di era media sosial.

## REFERENSI

- [1] F. Faridah, M. Yusuf, and N. Setiawati, ““Etika Keterbukaan dan Perlindungan Privacy di Media Sosial,” *J. An-nasyr J. Dakwah Dalam Mata Tinta*, vol. 9, no. 1, pp. 36–47, 2022, doi: <https://doi.org/10.54621/jn.v9i1.252>.
- [2] J. Natasya and N. Yulianita, “Oversharing Behaviour di Media Sosial Instagram,” *Bandung Conf. Ser. Public Relations*, vol. 3, no. 1, doi: 10.29313/bcsp.v3i1.5830.
- [3] F. N. Kamilah, “Manajemen Privasi pada Pengguna Media Sosial Instagram,” *jurnal interaksi online*, vol. 9, no. 1, pp. 98–108, 2020.
- [4] Y. Septiani, E. Aribbe, and R. Diansyah, “Analisis Kualitas Layanan Sistem Informasi Akademik Universitas Abdurrahman Terhadap Kepuasan Pengguna Menggunakan Metode Sevqual (Studi Kasus : Mahasiswa Universitas Abdurrahman Pekanbaru),” *JTOS*, vol. 3, no. 1, pp. 131–143, Jun. 2020, doi: 10.36378/jtos.v3i1.560.
- [5] M. T. Multazam and A. E. Widiarto, “Digitalization of the Legal System: Opportunities and Challenges for Indonesia,” *Rechtsidéee*, vol. 11, no. 2, Dec. 2023, doi: 10.21070/jhr.v12i2.1014.
- [6] A. P. B. A. Amanda, “Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau Dari Privacy Policy Facebook Dan Undang–Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik),” PhD Thesis, Brawijaya University, 2013. Accessed: Jan. 17, 2025. [Online]. Available: <https://www.neliti.com/publications/34738/tinjauan-yuridis-perlindungan-data-pribadi-dari-penyalahgunaan-data-pribadi-pada>
- [7] P. Sriwahyuni and W. O. Seprina, “Manajemen Privasi Komunikasi Pada Fenomena Batasan Diri Generasi Z di Instagram,” *Jurnal Ilmu Komunikasi UHO : Jurnal Penelitian Kajian Ilmu Komunikasi dan Informasi* Volume 9. No. 4. (2024), hlm 845-865 ISSN Online : 2527-9173.
- [8] E. S. Allysa Devia Naomira, “Implementasi Nilai-Nilai Kebangsaan Bersumber UUD 45 dan NKRI Pada Peran Manajemen Sekuriti Guna Meningkatkan Kesadaran, Keamanan Data Pribadi Media Sosial Instagram,” *Media Hukum Indonesia (MHI)* Published by Yayasan Daarul Huda Krueng Mane May 2024, doi: 10.5281/ZENODO.11209977.
- [9] U. Sugiyanti and A. Pambudi, “Perlindungan Data Privasi dan Kebebasan Informasi dalam Platform WhatsApp,” *Jurnal IPI (Ikatan Pustakawan Indonesia)*, vol. 7, no. 2, pp. 60–70, 2022.
- [10] R. Angela, “Analisis Self Disclosure Melalui Fitur Close Friend Di Instagram Mahasiswa Ilmu Komunikasi Angkatan 2020 Universitas Buddhi Dharma,” Skripsi Program Studi Ilmu Komunikasi Fakultas Sosial Dan Humaniora Universitas Buddhi Dharma Tangerang. 2024.
- [11] V. Varlina and T. L. K. Duma, “Privacy Crisis on Instagram: a Factor Analysis Approach on Motivation Behind Privacy Disclosure in Adolescents,” *J. Komun. Ikat. Sarj. Komun. Indones.*, vol. 7, no. 1, pp. 176–186, Jun. 2022, doi: 10.25008/jkiski.v7i1.613.
- [12] M. B. Satrio and M. W. Widiatno, “Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia),” *JCA of Law*, vol. 1, no. 1, 2020, Accessed: Jan. 17, 2025. [Online]. Available: <https://jca.esaunggul.ac.id/index.php/law/article/view/6>
- [13] V. Dianiya, “Management Privacy dalam Penggunaan Fitur ‘Close Friend’ di Instagram,” *Jurnal Studi Komunikasi*, 5 (1), pp. 244–266, 2021, doi: <https://doi.org/10.25139/jsk.v5i1.2652>.
- [14] S. S. Heuvelman, R. M. N. Betaubun, and S. Pujiati, “Konstruksi Identitas Keluarga di Media Sosial: Analisis Sosiologi Hukum tentang Perlindungan Privasi dan Dampak Regulasi Digital,” *Papsel Law Journal*, 1:2 (2025), pp. 67-75.

- [15] O. C. Chiquita and P. Febriana, "Analisis Fenomena Hyperhonest Penggunaan Fitur Instagram Close Friends Dalam Batasan Privasi," *Komunikatif: Jurnal Ilmu Komunikasi* Volume 12 Nomor 1 (2023) 25-36 DOI: 10.33508/jk.v12i1.4454 <http://jurnal.wima.ac.id/index.php/KOMUNIKATIF> E-ISSN 2597-6699 (Online)
- [16] M. P. Aprilia and S. Angelina, "Manajemen Privasi Komunikasi pada Instagram Stories Remaja di Yogyakarta," *Connected: Jurnal Ilmu Komunikasi*, *Connected: Jurnal Ilmu Komunikasi*, vol. 3, no. 1, pp. 1–14, 2022, doi: <https://doi.org/10.52423/jikuho.v9i4.324>.
- [17] D. Mawarsari , "Pengelolaan Privasi Informasi dalam Akun Kedua Instagram di Kalangan Mahasiswa, Studi Kasus Pengelolaan Privasi Informasi dalam Akun Kedua Instagram Mahasiswa FISIP UNS)." Skripsi, Program Studi Ilmu Komunikasi, Fakultas Ilmu Sosial dan Politik, Universitas Sebelas Maret Surakarta. 2021, doi: <https://digilib.uns.ac.id/dokumen/detail/85975/>
- [18] F. Zulfaramadhan, "Dramaturgi Pada Media Sosial: Penggunaan Fitur Close Friends Di Instagram," Vol 11 No 2 (2023): December DOI: <https://doi.org/10.21070/jihr.v12i2.1014>.
- [19] Marchelfia Pratiwi P, Emy Rosnawati, Mochamad Tanzil Multazam, and Noor Fatimah Mediawati, "Personal Data Collection: Recent Developments in Indonesia," *KnE Social Sciences*, no. 2, pp. 52–63, doi: 10.18502/Kss.v7i12.11503.
- [20] D. Revilia and N. Irwansyah, "Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness," *Jurnal PKOP*, vol. 24, no. 1, Jul. 2020, doi: 10.33299/jpkop.24.1.2375.

**Conflict of Interest Statement:**

*The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.*