JURNAL ILMIAH
MULTIDISIPLIN ILMU
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jimi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id/

DOI: https://doi.org/10.69714/gc2ygz96

TINJAUAN ASPEK KEAMANAN PADA PENGGUNAAN VIRTUAL PRIVATE NETWORK (VPN) GRATISAN BAGI PENGGUNA AWAM

Rendi Wijayakusuma[a*], Abdus Samad[b]
[a] Fakultas Saint dan Teknologi / Jurusan Teknologi Informasi; rendiwk39 @gmail.com, Universitas Ibrahimy Situbondo Jawa Timur
[b] Fakultas Saint dan Teknologi / Jurusan Teknologi Informasi; Saintek.somad @gmail.com, Universitas Ibrahimy Situbondo Jawa Timur
[*] Penulis Korespondensi: Rendi Wijayakusuma

ABSTRACT

Virtual Private Network (VPN) services are widely used by the general public to browse the internet more securely, bypass geographic restrictions, or gain access to blocked services and content. Among the available options, free VPN applications are particularly favored by lay users due to their accessibility and absence of subscription fees. However, behind this convenience lie various security and privacy risks that are often unrecognized by users, ranging from data leaks and weak or non-existent encryption to the practice of selling user data to third parties. This study aims to systematically review the security aspects of free VPN usage, focusing on the understanding and vulnerabilities faced by lay users who generally lack a technical background in cybersecurity. The method used is a literature review of scientific publications, independent research reports, and relevant policy documents on VPN security published within the last five years. The review results indicate that most popular free VPN applications contain significant security flaws, such as IP and DNS leaks, the use of risky third-party libraries, excessive permission requests, and non-transparent logging practices. Low digital literacy exacerbates these risks, as lay users rarely read privacy policies or verify a provider's reputation before installing an application. This study recommends improving digital security literacy, developing practical guidelines for selecting safe VPNs, and establishing clearer regulations for VPN service providers operating in Indonesia.

Keywords: *free VPN; cybersecurity; data privacy; lay users; digital literacy*

Abstrak

Virtual Private Network (VPN) banyak digunakan oleh masyarakat umum untuk mengakses internet secara lebih aman, melewati pembatasan geografis, atau membuka akses terhadap layanan dan konten yang diblokir. Di antara berbagai pilihan yang tersedia, aplikasi VPN gratisan menjadi pilihan favorit pengguna awam karena kemudahan akses dan tidak adanya biaya berlangganan. Akan tetapi, di balik kemudahan tersebut tersimpan berbagai risiko keamanan dan privasi yang sering tidak disadari oleh pengguna, mulai dari kebocoran data (data leak), enkripsi yang lemah atau tidak ada sama sekali, hingga praktik penjualan data pengguna kepada pihak ketiga. Penelitian ini bertujuan untuk meninjau secara sistematis aspek keamanan pada penggunaan VPN gratisan, dengan fokus pada pemahaman dan kerentanan yang dihadapi oleh pengguna awam yang umumnya tidak memiliki latar belakang teknis di bidang keamanan siber. Metode yang digunakan adalah studi literatur (literature review) terhadap publikasi ilmiah, laporan riset independen, dan dokumen kebijakan yang relevan dengan topik keamanan VPN dalam lima tahun terakhir. Hasil tinjauan menunjukkan bahwa sebagian besar aplikasi VPN gratis populer memiliki celah keamanan yang signifikan, seperti kebocoran alamat IP dan DNS, penggunaan pustaka pihak ketiga yang berisiko, permintaan izin akses berlebihan, serta praktik pencatatan (logging) yang tidak transparan. Faktor rendahnya literasi digital memperburuk risiko tersebut karena pengguna awam jarang membaca kebijakan privasi maupun memverifikasi reputasi penyedia layanan sebelum memasang aplikasi. Penelitian ini merekomendasikan

Naskah Masuk 30 Juni 2026; Revisi 20 Juli 2026; Diterima 21 Juli 2026; Tersedia 22 Juli 2026

peningkatan literasi keamanan digital, penyusunan panduan praktis pemilihan VPN yang aman, serta perlunya regulasi yang lebih jelas terhadap penyedia layanan VPN yang beroperasi di Indonesia.

Kata Kunci: VPN gratis; keamanan siber; privasi data; pengguna awam; literasi digital

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong masyarakat untuk semakin bergantung pada internet dalam berbagai aktivitas, baik untuk kebutuhan pekerjaan, pendidikan, maupun hiburan. Seiring dengan meningkatnya aktivitas daring, kebutuhan akan keamanan dan privasi data pribadi juga semakin meningkat. Salah satu teknologi yang banyak digunakan untuk menjawab kebutuhan tersebut adalah Virtual Private Network (VPN), yaitu teknologi yang membangun jalur komunikasi terenkripsi (tunnel) antara perangkat pengguna dan server tujuan melalui jaringan publik, sehingga data yang dikirimkan menjadi lebih aman dari penyadapan pihak ketiga.

Di Indonesia, penggunaan VPN tercatat cukup tinggi dibandingkan rata-rata regional. Survei yang dirujuk dalam beberapa kajian hukum menyebutkan bahwa sekitar 38 persen pengguna internet di Indonesia menggunakan VPN, jauh lebih tinggi dibandingkan rata-rata Asia Pasifik yang hanya sekitar 30 persen [1]. Tingginya angka ini tidak lepas dari kebiasaan masyarakat menggunakan VPN gratis untuk mengakses media sosial maupun konten yang dibatasi, sebagaimana terlihat pada peristiwa pembatasan akses media sosial oleh pemerintah pada tahun 2019 yang memicu lonjakan unduhan aplikasi VPN gratis [1].

Masalahnya, sebagian besar pengguna VPN gratis adalah pengguna awam yang memilih aplikasi tersebut semata-mata karena pertimbangan biaya dan kemudahan instalasi, tanpa memahami bagaimana aplikasi tersebut bekerja atau bagaimana data mereka diproses. Berbagai penelitian internasional menunjukkan bahwa kepercayaan ini sering tidak berdasar. Sebuah riset terhadap 283 aplikasi VPN Android berbasis izin VPN bawaan Android menemukan bahwa banyak aplikasi tidak memberikan jaminan keamanan dan privasi yang sesungguhnya kepada pengguna, dan sebagian besar pengguna tidak memiliki pengetahuan praktis mengenai pihak-pihak yang sebenarnya mengakses lalu lintas data mereka [2].

Studi independen yang lebih baru juga memperkuat temuan ini. Pengujian terhadap 100 aplikasi VPN gratis paling populer di Android pada tahun 2024 menemukan bahwa hampir seluruh aplikasi yang diuji mengalami kebocoran data, dengan rincian sekitar 88 persen mengalami kebocoran dalam berbagai bentuk dan hampir satu dari lima aplikasi mengalami lebih dari satu jenis kebocoran sekaligus, seperti kebocoran IPv4, IPv6, DNS, maupun WebRTC [3]. Studi yang sama juga menemukan bahwa 71 persen aplikasi VPN gratis Android berbagi data pribadi pengguna dengan pihak ketiga seperti perusahaan media sosial dan pialang data [3]. Temuan terbaru pada akhir 2025 juga menegaskan bahwa banyak aplikasi VPN gratis masih menggunakan versi OpenSSL yang rentan terhadap celah HeartBleed dan meminta izin akses yang berlebihan, bahkan sebagian memungkinkan terjadinya serangan man-in-the-middle [4].

Permasalahan ini menjadi semakin krusial ketika dikaitkan dengan rendahnya literasi keamanan digital pada masyarakat awam. Pengguna umum sering tidak menyadari bahwa data pribadi mereka terus berpindah melalui berbagai server dan jaringan ketika menggunakan internet, sehingga risiko kebocoran data menjadi sulit dihindari tanpa adanya perlindungan tambahan yang tepat [5]. Literasi mengenai risiko semacam ini umumnya hanya dimiliki oleh kelompok pengguna dengan latar belakang teknologi atau yang pernah mengikuti pelatihan keamanan siber, sementara mayoritas masyarakat hanya menggunakan internet untuk aktivitas harian tanpa memahami bagaimana data mereka sesungguhnya diproses [5].

Berdasarkan latar belakang tersebut, penelitian ini disusun untuk meninjau secara komprehensif aspek-aspek keamanan pada penggunaan VPN gratisan, dengan penekanan khusus pada risiko yang dihadapi oleh pengguna awam. Tinjauan ini diharapkan dapat memberikan gambaran yang jelas mengenai jenis-jenis ancaman yang umum terjadi, faktor-faktor yang menyebabkan pengguna awam rentan terhadap ancaman tersebut, serta rekomendasi praktis yang dapat diterapkan untuk meminimalkan risiko.

1.1. Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah penelitian ini adalah: (1) apa saja risiko keamanan dan privasi yang umum ditemukan pada aplikasi VPN gratisan; (2) bagaimana karakteristik pengguna awam

memengaruhi tingkat kerentanan mereka terhadap risiko tersebut; serta (3) langkah dan strategi apa yang dapat diterapkan untuk mengurangi risiko keamanan bagi pengguna awam yang menggunakan VPN gratisan.

1.2. Tujuan Penelitian

Penelitian ini bertujuan untuk: (1) mengidentifikasi dan mengklasifikasikan risiko keamanan utama pada penggunaan VPN gratisan berdasarkan temuan-temuan penelitian terdahulu; (2) menganalisis hubungan antara rendahnya literasi digital pengguna awam dan tingkat eksposur mereka terhadap risiko keamanan VPN; serta (3) merumuskan rekomendasi praktis dan kebijakan yang dapat membantu pengguna awam dalam memilih dan menggunakan layanan VPN secara lebih aman.

1.3. Manfaat Penelitian

Secara teoretis, penelitian ini diharapkan dapat memperkaya kajian akademik di bidang keamanan siber, khususnya yang berfokus pada perilaku dan kerentanan pengguna akhir (end-user) non-teknis. Secara praktis, hasil tinjauan ini dapat dimanfaatkan oleh masyarakat umum sebagai bahan edukasi dalam memilih layanan VPN, oleh pengembang aplikasi sebagai acuan dalam membangun layanan yang lebih transparan, serta oleh pembuat kebijakan dalam menyusun regulasi yang relevan terhadap penyedia layanan VPN yang beroperasi di Indonesia.

2. TINJAUAN PUSTAKA

2.1. Konsep Dasar Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah teknologi yang memungkinkan pembentukan jaringan privat di atas infrastruktur jaringan publik melalui mekanisme tunneling dan enkripsi data. Pada awalnya, VPN dikembangkan untuk kebutuhan korporasi dan instansi pemerintahan guna menghubungkan kantor cabang dengan kantor pusat secara aman melalui jaringan internet, dan bukan untuk penggunaan komersial perorangan [6]. Beberapa protokol VPN yang umum digunakan antara lain *Point to Point Tunneling Protocol* (PPTP), *Internet Protocol Security* (IPSec), OpenVPN, dan protokol yang lebih modern seperti WireGuard. Hasil pengujian empiris menunjukkan bahwa WireGuard memiliki efisiensi lebih baik dibandingkan OpenVPN dari sisi latensi, meskipun setiap protokol memiliki karakteristik keseimbangan keamanan dan performa yang berbeda-beda [7].

Dalam praktiknya, layanan VPN yang ditujukan untuk konsumen umum terbagi menjadi dua kategori besar, yaitu layanan berbayar (premium) dan layanan gratis. Layanan gratis umumnya didanai melalui model bisnis alternatif seperti penayangan iklan, penjualan data pengguna kepada pihak ketiga, atau sebagai versi terbatas (freemium) yang mendorong pengguna beralih ke layanan berbayar.

2.2. Perbandingan VPN Gratis dan VPN berbayar

Perbedaan mendasar antara VPN gratis dan berbayar terletak pada model bisnis dan implikasinya terhadap keamanan dan privasi pengguna. VPN berbayar memperoleh pendapatan dari biaya langganan pengguna, sehingga tidak memiliki insentif ekonomi untuk menjual data pengguna atau memasukkan iklan yang mengganggu. Model bisnis ini memungkinkan penyedia VPN berbayar untuk berinvestasi pada infrastruktur server yang lebih baik, protokol enkripsi yang lebih mutakhir, serta tim keamanan yang responsif terhadap kerentanan yang ditemukan.

Sebaliknya, VPN gratis harus memperoleh pendapatan melalui cara alternatif. Beberapa penyedia menggunakan model freemium dengan membatasi bandwidth, kecepatan, atau jumlah server yang dapat diakses, kemudian mendorong pengguna untuk meningkatkan ke berbayar. Namun, banyak penyedia VPN gratis yang sepenuhnya gratis mengandalkan pendapatan dari iklan atau penjualan data pengguna kepada pihak ketiga, termasuk pialang data dan perusahaan periklanan [3]. Praktik ini secara langsung bertentangan dengan tujuan utama penggunaan VPN, yaitu melindungi privasi pengguna.

Dari sisi kebijakan privasi, VPN berbayar yang kredibel umumnya menerapkan kebijakan no-log yang ketat dan bersedia menjalani audit independen untuk memverifikasi klaim mereka. Sementara itu, sebagian besar VPN gratis tidak memiliki kebijakan privasi yang jelas, atau jika ada, kebijakan tersebut ditulis secara ambigu dan memungkinkan pengumpulan serta pembagian data pengguna secara luas [9]. Perbedaan ini menjadikan VPN berbayar sebagai pilihan yang jauh lebih aman, terutama untuk aktivitas yang melibatkan data sensitif seperti transaksi perbankan atau komunikasi pekerjaan.

2.2.1. Bukti Empiris Kerentanan VPN Gratis

Sejumlah riset independen secara konsisten menunjukkan tingkat kerentanan yang tinggi pada aplikasi VPN gratis, khususnya di platform mobile. Pengujian komprehensif pada 100 aplikasi VPN gratis Android paling populer menemukan bahwa 88 persen di antaranya mengalami kebocoran data dalam berbagai bentuk, sementara kegagalan enkripsi ditemukan pada sekitar satu dari sepuluh aplikasi yang diuji [3]. Riset lanjutan mengenai insiden pembatasan internet juga menemukan bahwa sekitar 80 persen VPN yang naik popularitasnya pada masa krisis tersebut membagikan atau mencatat alamat IP asli penggunanya [3].

Penelitian akademik berskala besar yang menganalisis 283 aplikasi VPN Android dari korpus lebih dari 1,4 juta aplikasi di Google Play menemukan adanya praktik pelacakan pengguna oleh pihak ketiga serta akses terhadap izin sensitif Android, meskipun mayoritas aplikasi yang diteliti mengklaim menyediakan layanan keamanan dan privasi [2]. Studi tersebut juga menunjukkan bahwa aplikasi VPN populer tertentu yang mengklaim memberikan keamanan dan anonimitas pada praktiknya tidak efektif dalam melindungi pengguna dari pengawasan maupun pihak-pihak berniat jahat [2].

Survei literatur yang lebih komprehensif terhadap berbagai metode evaluasi keamanan VPN juga menyoroti adanya kebocoran lalu lintas DNS pada sekitar 66 persen aplikasi yang diuji dan kebocoran IPv6 pada sekitar 84 persen aplikasi, di samping penggunaan protokol yang tidak aman dan praktik intersepsi TLS (TLS interception) [8]. Sejumlah aplikasi yang diuji bahkan ditemukan menyisipkan program JavaScript untuk melacak aktivitas pengguna demi kepentingan periklanan, meskipun temuan tersebut terbatas pada aplikasi gratis berbasis Android dan belum mencakup aplikasi berbayar maupun platform iOS [8].

Temuan terbaru pada tahun 2025 mengonfirmasi bahwa masalah ini belum banyak berubah. Riset Zimperium zLabs menemukan bahwa sejumlah aplikasi VPN gratis masih menggunakan versi OpenSSL lama yang rentan terhadap celah keamanan HeartBleed, sementara hampir 1 persen aplikasi yang diuji memungkinkan terjadinya intersepsi man-in-the-middle [4]. Pada platform iOS, lebih dari 6 persen aplikasi diketahui meminta izin akses tingkat sistem (private entitlements) yang berpotensi memberikan akses mendalam ke perangkat, sementara seperempat aplikasi yang diuji tidak memiliki dokumen privasi (privacy manifest) sebagaimana diwajibkan oleh Apple [4]. Para peneliti menyimpulkan bahwa banyak aplikasi VPN gratis gagal melindungi pengguna dan justru berpotensi membuka peluang pengawasan, kompromi perangkat secara penuh, hingga pencurian kredensial [4].

2.2.2. Faktor Pengguna Awam dan Literasi Digital

Selain faktor teknis pada aplikasi itu sendiri, aspek perilaku dan literasi pengguna turut memainkan peran besar dalam tingkat eksposur terhadap risiko keamanan VPN. VPN sering dianggap sebagai teknologi yang terlalu teknis dan sulit dijangkau oleh pengguna awam, sehingga banyak pengguna yang bahkan tidak menyadari bahwa data pribadi mereka terus berpindah melalui berbagai server dan jaringan ketika sedang terhubung ke internet [5]. Literasi mengenai risiko ini pada umumnya hanya dimiliki oleh kelompok pengguna yang memiliki latar belakang teknologi atau pernah mengikuti pelatihan keamanan siber tertentu [5].

Kondisi ini diperparah oleh kebiasaan pengguna yang jarang membaca syarat layanan (Terms of Service) maupun kebijakan privasi penyedia VPN secara teliti sebelum menggunakannya, sehingga banyak pengguna yang tidak menyadari konsekuensi dari penggunaan IP address mereka sebagai exit node bagi pengguna lain, atau dari klausul pengumpulan data yang sebenarnya tercantum namun ditulis secara ambigu [9]. Temuan dari berbagai jurnal internasional juga menunjukkan bahwa banyak pengguna tidak menyadari ancaman teknis seperti pelacakan (tracking), pembuatan profil (profiling), pencurian identitas, atau penyadapan lalu lintas data ketika menggunakan layanan daring [5].

2.2.3. Aspek Regulasi di Indonesia

Dari sisi regulasi, penggunaan VPN di Indonesia bersinggungan dengan beberapa ketentuan hukum, di antaranya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang dalam Pasal 15 mewajibkan setiap penyelenggara sistem elektronik untuk menyelenggarakan sistemnya secara andal, aman, dan bertanggung jawab [9]. Selain itu, Surat Edaran Menteri Komunikasi dan Informatika Nomor 3 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau Konten melalui Internet (Over The Top) juga mengatur tanggung jawab penyedia layanan Over The Top, termasuk yang berkaitan dengan

kewajiban penggunaan Bahasa Indonesia dalam layanan sesuai ketentuan perundang-undangan yang berlaku [9].

Meskipun demikian, regulasi yang secara spesifik mengatur penyedia layanan VPN gratis—baik yang berasal dari dalam maupun luar negeri—masih memerlukan penguatan, khususnya terkait kewajiban perizinan dan perlindungan data pribadi penggunanya [9]. Ketiadaan kerangka regulasi yang tegas menjadikan tanggung jawab perlindungan data sebagian besar bergantung pada kebijakan internal masing-masing penyedia layanan, yang kualitas dan transparansinya sangat beragam.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif melalui metode studi literatur (literature review). Metode ini dipilih karena tujuan penelitian adalah memetakan dan mensintesiskan temuan-temuan yang telah ada mengenai risiko keamanan VPN gratis, bukan menghasilkan data primer baru melalui eksperimen atau survei lapangan.

3.1. Sumber dan Kriteria Data

Data yang digunakan dalam penelitian ini berasal dari tiga kategori sumber, yaitu: (1) artikel jurnal ilmiah dan prosiding terindeks yang membahas keamanan, privasi, dan kinerja VPN; (2) laporan riset independen dari lembaga riset keamanan siber yang melakukan pengujian langsung terhadap aplikasi VPN; serta (3) dokumen regulasi dan kebijakan yang relevan dengan penyelenggaraan layanan VPN di Indonesia. Pemilihan sumber diprioritaskan pada publikasi lima tahun terakhir, dengan tetap mempertimbangkan beberapa rujukan klasik yang relevan secara konseptual.

Pencarian literatur dilakukan pada basis data akademik terpercaya, meliputi Google Scholar, Scopus, IEEE Xplore, dan SpringerLink. Selain itu, penelusuran juga dilakukan pada laporan riset independen dari lembaga keamanan siber terkemuka seperti Top10VPN, Zimperium zLabs, serta publikasi dari ACM Digital Library. Kata kunci yang digunakan dalam pencarian meliputi "free VPN security", "VPN data leak", "VPN privacy risk", "Android VPN vulnerability", serta "keamanan VPN gratis" untuk literatur berbahasa Indonesia. Kombinasi kata kunci tersebut diterapkan dengan operator Boolean (AND/OR) untuk memaksimalkan hasil pencarian yang relevan.

3.2. Tahapan Analisis

Tahapan analisis dalam penelitian ini terdiri dari empat langkah. Pertama, identifikasi, yaitu mengumpulkan literatur yang membahas keamanan VPN dengan kata kunci seperti “free VPN security”, “VPN data leak”, dan “keamanan VPN gratis”. Kedua, penyaringan (screening), yaitu menyeleksi literatur berdasarkan relevansi topik, kredibilitas sumber, dan kemutakhiran data. Ketiga, ekstraksi data, yaitu mencatat temuan-temuan kunci terkait jenis risiko, metode pengujian, dan persentase kerentanan yang dilaporkan. Keempat, sintesis, yaitu mengelompokkan temuan ke dalam kategori risiko teknis, risiko privasi, dan faktor perilaku pengguna untuk dianalisis secara naratif.

3.3. Batasan Penelitian

Penelitian ini memiliki sejumlah keterbatasan. Pertama, sebagai studi literatur, hasil tinjauan ini sepenuhnya bergantung pada temuan yang telah dipublikasikan oleh peneliti lain dan tidak melibatkan pengujian teknis independen terhadap aplikasi VPN tertentu. Kedua, sebagian besar data kuantitatif yang dirujuk berfokus pada platform Android, sehingga gambaran risiko pada platform lain seperti iOS, desktop, maupun ekstensi peramban masih relatif terbatas. Ketiga, lanskap aplikasi VPN bersifat sangat dinamis, sehingga temuan mengenai aplikasi tertentu dapat berubah seiring waktu akibat pembaruan kebijakan maupun perbaikan teknis oleh penyedia layanan.

4. HASIL DAN PEMBAHASAN

4.1. Klasifikasi Risiko Keamanan pada VPN Gratisan

Berdasarkan sintesis terhadap berbagai literatur yang ditinjau, risiko keamanan pada penggunaan VPN gratisan dapat dikelompokkan ke dalam empat kategori utama, sebagaimana dirangkum pada Tabel 1.

Tabel 1. Klasifikasi Risiko Keamanan pada Aplikasi VPN Gratisan

Kategori Risiko	Deskripsi	Contoh Temuan

Kebocoran data teknis	Kegagalan menyembunyikan alamat IP, lokasi, atau permintaan DNS asli pengguna akibat konfigurasi tunnel yang tidak sempurna.	88% aplikasi Android mengalami kebocoran data; 84% kebocoran IPv6; 66% kebocoran DNS [3], [8]
Enkripsi lemah / tidak ada	Penggunaan standar enkripsi usang atau pustaka kriptografi yang memiliki celah keamanan dikenal.	Penggunaan OpenSSL rentan HeartBleed; sekitar 10% aplikasi mengalami kegagalan enkripsi [4]
Praktik privasi tidak transparan	Pencatatan (logging) aktivitas pengguna yang tidak sesuai klaim pemasaran, serta pembagian data ke pihak ketiga.	71% aplikasi membagikan data pribadi ke pihak ketiga seperti media sosial dan pialang data [3]
Risiko pada level aplikasi/perangkat	Permintaan izin akses berlebihan, potensi malware, dan kerentanan terhadap serangan man-in-the-middle.	Sekitar 20% aplikasi ditandai berisiko oleh antivirus; lebih dari 6% aplikasi iOS meminta entitlement sensitif [4]

Sumber: diolah dari berbagai referensi [3], [4], [8]

Keempat kategori risiko tersebut saling berkaitan satu sama lain. Kebocoran data teknis, misalnya, sering terjadi akibat kombinasi antara enkripsi yang lemah dan konfigurasi tunnel yang tidak sempurna, sementara praktik privasi yang tidak transparan umumnya baru dapat terungkap melalui audit independen karena pengguna awam tidak memiliki kemampuan teknis untuk memeriksanya secara mandiri.

4.2. Mengapa Pengguna Awam Lebih Rentan

Tinjauan literatur menunjukkan bahwa kerentanan pengguna awam terhadap risiko keamanan VPN gratisan bukan semata-mata disebabkan oleh kelemahan teknis aplikasi, melainkan juga oleh sejumlah faktor perilaku dan kognitif, di antaranya: (1) minimnya kebiasaan membaca kebijakan privasi dan syarat layanan sebelum memasang aplikasi, sehingga pengguna tidak menyadari klausul pengumpulan dan pembagian data yang sebenarnya tercantum di dalamnya; (2) anggapan bahwa semua aplikasi VPN secara otomatis memberikan perlindungan privasi, padahal nama dan ikon "gembok" pada aplikasi tidak selalu mencerminkan tingkat keamanan yang sesungguhnya; (3) keterbatasan kemampuan teknis untuk memverifikasi reputasi penyedia layanan, struktur kepemilikan perusahaan, maupun lokasi server yang digunakan; serta (4) preferensi terhadap kemudahan dan biaya nol, yang mendorong pemilihan aplikasi berdasarkan peringkat unduhan atau ulasan toko aplikasi tanpa mempertimbangkan aspek keamanan secara mendalam.

Rendahnya literasi keamanan digital ini konsisten dengan temuan bahwa pemahaman mengenai risiko siber pada umumnya terbatas pada kelompok masyarakat dengan latar belakang teknologi atau yang pernah mendapatkan pelatihan keamanan siber, sementara mayoritas pengguna internet sehari-hari tidak menyadari bagaimana data mereka diproses ketika menggunakan layanan daring [5]. Kesenjangan literasi ini menjadikan pengguna awam sebagai kelompok yang secara struktural lebih rentan, terlepas dari aplikasi VPN spesifik apa pun yang mereka gunakan.

4.3. Risiko Spesifik pada Konteks Indonesia

Konteks Indonesia memiliki karakteristik tersendiri yang memperbesar eksposur masyarakat terhadap risiko VPN gratisan. Tingkat penggunaan VPN yang tinggi—sekitar 38 persen pengguna internet—sebagian besar didorong oleh kebutuhan mengakses konten yang dibatasi secara geografis maupun melewati pemblokiran sementara terhadap layanan tertentu [1]. Pola penggunaan yang bersifat reaktif dan mendesak ini, seperti yang terjadi pada peristiwa pembatasan media sosial tahun 2019, membuat pengguna cenderung memasang aplikasi VPN gratis secara cepat tanpa mempertimbangkan aspek keamanan, semata-mata demi memperoleh akses secepat mungkin [1].

Di sisi lain, kerangka regulasi yang ada saat ini, meskipun telah mengatur tanggung jawab umum penyelenggara sistem elektronik melalui UU ITE, belum secara spesifik mengatur kewajiban perizinan dan standar keamanan minimum bagi penyedia layanan VPN gratis yang beroperasi di Indonesia [9]. Kekosongan regulasi spesifik ini berkontribusi pada minimnya akuntabilitas penyedia layanan terhadap praktik pengumpulan dan pengelolaan data penggunanya.

4.4. Rekomendasi Praktis bagi Pengguna Awam

Berdasarkan hasil tinjauan di atas, beberapa langkah praktis dapat direkomendasikan bagi pengguna awam yang tetap memilih menggunakan VPN gratis karena pertimbangan biaya, yaitu: (1) memilih penyedia VPN yang secara transparan mempublikasikan kebijakan no-log dan, jika memungkinkan, telah menjalani audit keamanan independen oleh pihak ketiga; (2) memeriksa izin akses (permission) yang diminta aplikasi pada saat instalasi, dan mewaspadai aplikasi yang meminta izin tidak relevan dengan fungsi VPN, seperti akses ke kontak atau galeri foto; (3) menghindari aplikasi VPN gratis yang tidak jelas identitas perusahaan pengembangnya atau yang memiliki ulasan pengguna yang mencurigakan secara massal; (4) memanfaatkan fitur uji kebocoran (leak test) yang tersedia secara daring untuk memeriksa apakah alamat IP atau DNS asli pengguna masih terekspos saat VPN aktif; serta (5) mempertimbangkan opsi VPN berbayar dengan reputasi baik atau alternatif tepercaya lainnya untuk kebutuhan yang melibatkan data sensitif, seperti transaksi perbankan atau pekerjaan.

Selain langkah individual, diperlukan pula upaya kolektif dalam bentuk edukasi literasi digital yang menyasar masyarakat umum, termasuk melalui kurikulum pendidikan, kampanye kesadaran publik oleh pemerintah maupun lembaga swadaya masyarakat, serta penguatan kerangka regulasi yang mewajibkan transparansi praktik data bagi seluruh penyedia layanan VPN yang beroperasi di Indonesia.

5. KESIMPULAN DAN SARAN

Berdasarkan tinjauan literatur yang telah dilakukan, dapat disimpulkan tiga hal utama. **Pertama**, penggunaan VPN gratisan menyimpan risiko keamanan dan privasi yang signifikan, meliputi kebocoran data teknis (IP dan DNS), enkripsi yang lemah, praktik pencatatan dan pembagian data yang tidak transparan, serta risiko pada level aplikasi seperti permintaan izin berlebihan. Berbagai studi independen secara konsisten menemukan bahwa mayoritas aplikasi VPN gratis populer mengandung setidaknya satu bentuk kerentanan tersebut.

Kedua, pengguna awam menghadapi risiko yang lebih besar bukan karena perbedaan aplikasi yang digunakan, melainkan karena keterbatasan literasi digital yang menyebabkan mereka jarang memeriksa kebijakan privasi, reputasi penyedia layanan, maupun indikator keamanan teknis lainnya. Faktor perilaku seperti preferensi terhadap kemudahan dan biaya nol, serta pola penggunaan yang reaktif terhadap pembatasan akses, memperburuk tingkat kerentanan mereka.

Ketiga, upaya pengurangan risiko memerlukan pendekatan kombinasi antara edukasi literasi keamanan digital bagi masyarakat umum, pengembangan panduan praktis pemilihan VPN yang aman, serta penguatan kerangka regulasi yang mewajibkan transparansi dan standar keamanan minimum bagi seluruh penyedia layanan VPN yang beroperasi di Indonesia.

Saran Untuk penelitian Lanjutan

Penelitian lanjutan disarankan untuk melakukan pengujian teknis langsung terhadap aplikasi VPN gratis yang populer di kalangan pengguna Indonesia, guna memverifikasi temuan dari studi internasional dalam konteks lokal. Pengujian ini dapat mencakup analisis kebocoran data, evaluasi implementasi enkripsi, serta pemeriksaan praktik pengumpulan dan pembagian data melalui metode network traffic analysis.
Selain itu, diperlukan penelitian empiris yang mengkaji tingkat pemahaman dan perilaku pengguna awam di Indonesia terhadap risiko keamanan VPN, melalui metode survei skala besar atau wawancara terstruktur. Penelitian semacam ini dapat mengidentifikasi faktor-faktor spesifik yang memengaruhi keputusan pengguna dalam memilih layanan VPN, serta mengukur efektivitas berbagai bentuk intervensi edukasi yang mungkin diterapkan.

Studi komparatif antara platform yang berbeda (Android, iOS, desktop, ekstensi peramban) juga diperlukan untuk memberikan gambaran risiko yang lebih komprehensif, mengingat sebagian besar penelitian yang ada saat ini masih terfokus pada platform Android. Terakhir, penelitian mengenai efektivitas kebijakan regulasi di negara-negara yang telah memiliki kerangka hukum spesifik untuk penyedia layanan VPN dapat menjadi rujukan berharga bagi pengembangan regulasi di Indonesia.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah mendukung penyelesaian tinjauan literatur ini, termasuk institusi pendidikan tempat penulis bernaung serta seluruh peneliti yang karyanya dirujuk dalam artikel ini.

DAFTAR PUSTAKA

[1] D. Abeywickrama, T. Perera, and N. Jayasena, “Security Risks and Privacy Concerns in Virtual Private Network (VPN) Services: A Comprehensive Analysis,” ResearchGate, Jul. 2019.
[2] Penyusun Jurnal Supremasi Hukum, “Penggunaan Aplikasi Virtual Private Network (VPN) dan Perlindungan Data Pribadi di Indonesia,” Supremasi Hukum: Jurnal Penelitian Hukum, p-ISSN: 1693-766X, e-ISSN: 2579-4663.
[3] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, “An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps,” in Proc. ACM Internet Measurement Conference (IMC), 2016.
[4] Top10VPN, “Are Free VPNs Safe? Over 80% Leak & 70% Share Data,” Free VPN Risk Index Report, 2024. [Online]. Available: https://www.top10vpn.com/research/free-vpn-investigations/
[5] SC Media, “Study Warns Free VPN Apps Pose Severe Risks,” Oct. 3, 2025. [Online]. Available: https://www.scworld.com/brief/study-warns-free-vpn-apps-pose-severe-risks
[6] Security Assessment and Evaluation of VPNs Research Team, “Security Assessment and Evaluation of VPNs: A Comprehensive Survey,” ACM Computing Surveys, 2023, doi: 10.1145/3579162.
[7] Tim Penulis JAREKOM, “Pengaruh Virtual Private Network (VPN) terhadap Performa dan Keamanan Jaringan,” Jurnal JAREKOM, vol. 1, no. 1, Jun. 2025.
[8] Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[9] Menteri Komunikasi dan Informatika Republik Indonesia, Surat Edaran Nomor 3 Tahun 2016 tentang Penyediaan Layanan Aplikasi dan/atau Konten melalui Internet (Over The Top).