

# Literasi Digital dan Kewaspadaan Siber: Analisis Tingkat Kesadaran Privasi Pengguna Terhadap Ancaman *Doxing*

**Nur Azizah** | Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Bung Karno Jakarta  
*nengsirnarasa@gmail.com*

**Bambang Mudjiyanto** | Badan Riset dan Inovasi Nasional (BRIN)  
*bamb065@brin.go.id*

**Fit Yanuar** | Fakultas Ilmu Komunikasi, Universitas SAHID Jakarta  
*fit\_yanuar@usahid.ac.id*

**Nursyamsi** | Fakultas Hukum, Ilmu Sosial dan Ilmu Politik, UNIMUDA Sorong  
*nursyamsi@unimudasorong.ac.id*

**Launa** | Fakultas Ilmu Komunikasi, Universitas SAHID Jakarta  
*launa@usahid.ac.id*

**Abstract.** *Doxing—the forced disclosure of personal data in the digital realm—is currently a serious threat to social media users, especially young people who lack a clear understanding of digital security risks. This qualitative study, using a descriptive-interpretive approach, reveals that privacy awareness and digital literacy among users remain low, while state protection efforts are less than optimal. The study’s findings indicate that preventing doxing requires strong political will, proactive public policies, and multi-stakeholder collaboration. Digital literacy is not merely a technical necessity, but a fundamental right of citizens in a safe, ethical, and inclusive digital ecosystem. Strengthening literacy and privacy protection are essential foundations for a responsible digital society to support the growth of a sustainable digital ecosystem.*

**Keywords:** *Doxing, cybercrime, privacy awareness, digital literacy, social media.*

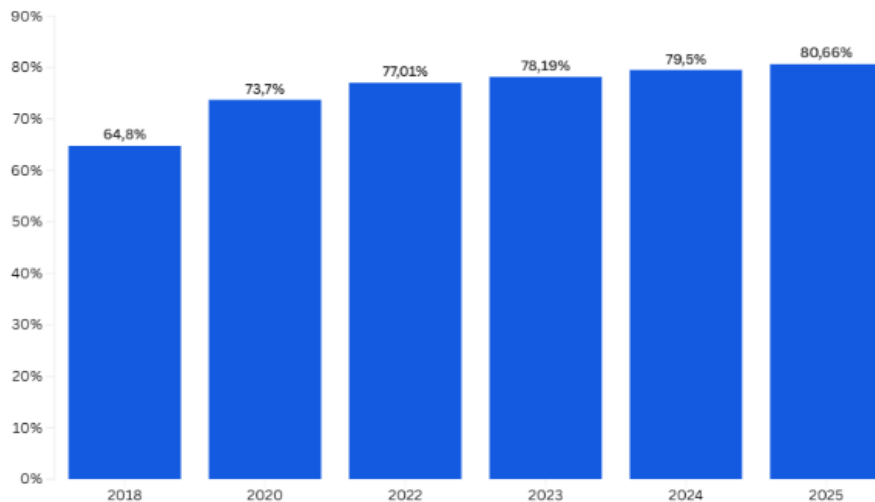
**Abstrak.** *Doxing—pengungkapan paksa data pribadi di ranah digital—saat ini menjadi ancaman serius bagi para pengguna media sosial, terutama kalangan muda yang kurang memahami risiko keamanan digital. Studi kualitatif dengan pendekatan deskriptif-interpretif ini mengungkap bahwa kesadaran privasi dan literasi digital di kalangan pengguna masih rendah, sementara upaya perlindungan dari negara belum maksimal. Temuan studi menunjukkan: pencegahan *doxing* membutuhkan *political will* yang kuat, kebijakan publik yang proaktif, dan kolaborasi multistakeholder. Literasi digital tak hanya soal kebutuhan teknis, melainkan hak dasar warga negara dalam ekosistem digital yang aman, etis, dan inklusif. Penguatan literasi dan perlindungan privasi menjadi fondasi penting bagi masyarakat digital yang bertanggung jawab guna menopang pertumbuhan ekosistem digital yang berkelanjutan.*

**Kata kunci:** *Doxing, kejahatan siber, kesadaran privasi, literasi digital, media sosial.*

## PENDAHULUAN

Dinamika pertumbuhan teknologi informasi dan komunikasi (ITC) yang pesat telah membawa perubahan signifikan di hampir seluruh sektor kehidupan, terutama sejak kemunculan dan meluasnya penggunaan internet. Di Indonesia, media sosial (medsos) telah menjadi sarana utama bagi jutaan pengguna untuk berinteraksi, berbagi informasi, dan mengekspresikan diri tanpa dibatasi ruang dan waktu. Hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan, lebih dari 90% pengguna internet di Indonesia aktif pengguna media sosial. Namun, kemudahan akses dan interaksi di platform digital

tersebut tidak lepas dari risiko, terutama untuk pengguna pemula (*early users*) yang belum memiliki kesadaran privasi dan literasi digital yang memadai. Riset Agustin dan Firdos (2024) juga menunjukkan, mayoritas pengguna pemula media sosial di Indonesia masih minim pemahaman terhadap berbagai modus kejahatan siber, seperti penipuan daring, perundungan siber (*cyberbullying*), penyebaran informasi palsu, serta pencurian data pribadi. Kondisi ini menjadikan kelompok pengguna pemula sebagai sasaran rentan dalam ekosistem kejahatan siber.



**Gambar 1. Tingkat Penetrasi Internet Indonesia 2018-2025**

Sumber: goodstats.id, 2025

Lebih dari itu, Indonesia dikenal sebagai salah satu negara dengan jumlah pengguna media sosial terbesar di dunia. Data statistik tahun 2025 menunjukkan, lebih dari 190 juta penduduk Indonesia merupakan pengguna aktif media sosial. Lima platform paling populer adalah Instagram (150 juta pengguna/user), TikTok (140 juta user), Facebook (120 juta user), Twitter (X) (40 juta user), serta LinkedIn (25 juta user). Rata-rata waktu yang dihabiskan pengguna pemula di media sosial mencapai 3,5 jam per hari. Data ini memosisikan Indonesia sebagai negara dengan tingkat partisipasi medsos tertinggi di dunia (Wisnuadi, 2025).

	Laki laki	Perempuan
Facebook	21,85%	21,28%
Instagram	15,19%	16,75%
Youtube	26,31%	21,00%
Tiktok	32,98%	37,55%
Twitter	0,68%	0,40%
Tidak Tahu	1,27%	1,38%
Lainnya	1,72%	1,64%

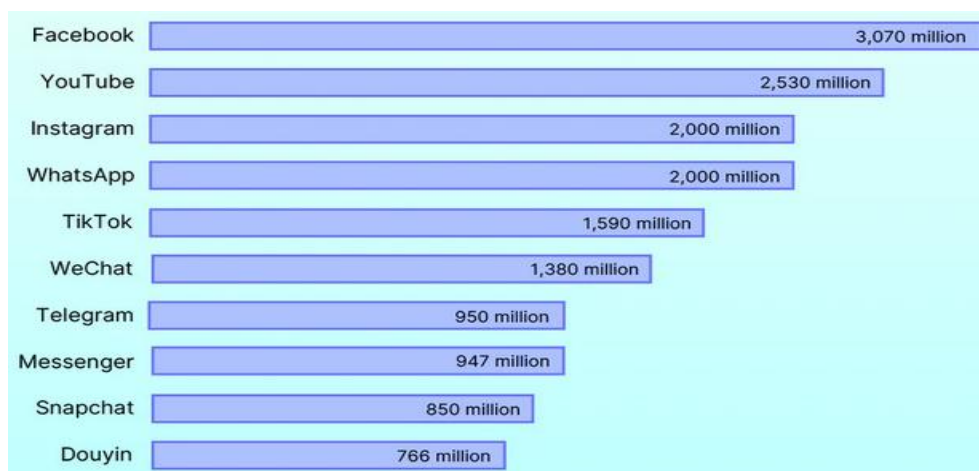
**Gambar 2. Platform Medsos Terpopuler di Indonesia 2025 (Berdasarkan Gender)**

Sumber: Selular.id, 2025

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) juga merilis hasil survei terbaru bertajuk “Survei Profil Internet Indonesia 2025” yang mengungkap lima platform medsos paling banyak diakses pengguna internet di Tanah Air. TikTok, aplikasi besutan ByteDance, menjadi yang terpopuler dengan persentase 35,17%, mengungguli YouTube, Facebook, Instagram, dan Twitter (X) (Selular.id, 2025).

Survei dengan metode wawancara tatap muka terhadap 8.700 responden berusia minimal 13 tahun di 38 provinsi antara 10 April hingga 16 Juli 2025 ini menunjukkan pertumbuhan signifikan TikTok dibanding tahun sebelumnya. Platform tersebut naik dari 18,61% pada tahun lalu, sementara platform lain justru mengalami penurunan. YouTube berada di posisi kedua dengan 23,76% (turun dari 27,53%), diikuti Facebook 21,58% (turun dari 34,85%), Instagram 15,94% (turun dari 16,07%), dan X/Twitter 0,56% (turun dari 0,57%). Data ini menegaskan bahwa TikTok adalah satu-satunya platform yang mengalami pertumbuhan positif di antara lima besar (Selular.id, 2025).

Sementara data global tahun 2025 mencatat, Facebook menjadi platform dengan jumlah pengguna aktif terbanyak, mencapai 3.070 juta pengguna (*user*), disusul YouTube 2.530 juta *user*, sementara Instagram dan WhatsApp sama-sama mengantongi 2.000 juta *user*. Di urutan berikut, TikTok masih diposisi kompetitif, dengan 1.590 juta *user*, diikuti oleh WeChat (1.380 juta *user*), Telegram (950 juta *user*), Snapchat (850 juta *user*), dan Douyin (766 juta *user*). Sepuluh platform di atas tetap eksis di tangga popularitasnya. Tren medsos tahun 2025 ini menunjukkan fakta bahwa platform berbasis video, audio, dan pesan instan masih menjadi favorit di kalangan para pengguna medsos global (We Are Social, 2024).



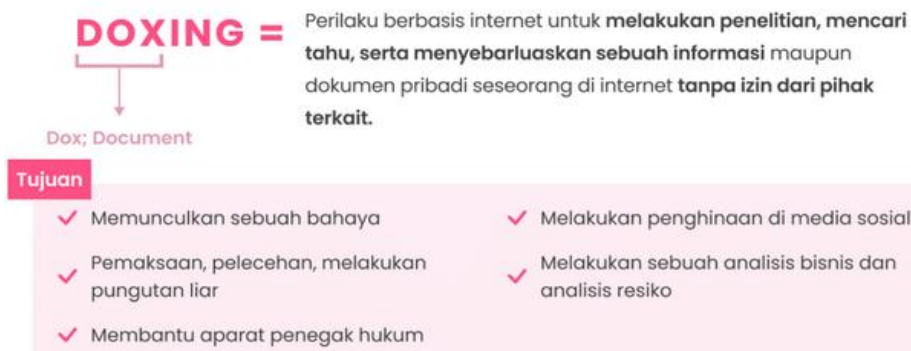
**Gambar 3. Platform Medsos Terpopuler di Dunia (2025)**

Sumber: shopify-com, 2025

Di era digital yang bergerak dinamis dan eksesif, membuat medsos menjadi bagian penting dalam kehidupan masyarakat. Platform, seperti Facebook, Instagram, Twitter, atau TikTok, tak hanya digunakan sebagai sarana komunikasi dan berbagi informasi, tetapi juga alat dalam membangun jejaring sosial, promosi bisnis, hingga akses hiburan (musik, film, drama). Kecepatan penyebaran informasi yang *high speed* membuat medsos menjadi ruang interaksi paling dinamis di dunia saat ini.

*Doxing* adalah praktik pengumpulan, pengungkapan, atau penyebaran informasi pribadi—identitas, alamat, nomor telepon, atau data sensitif lainnya—tentang individu, kelompok, atau organisasi tanpa persetujuan. Informasi tersebut sering diperoleh melalui cara-cara yang tidak sah, termasuk peretasan, rekayasa database publik dan celah keamanan

digital. Tujuannya bisa pelecehan, pemerasan, pencemaran nama baik, hingga mobilisasi serangan siber. *Doxing* tidak hanya melanggar privasi, tetapi juga berpotensi menimbulkan dampak psikologis, sosial, bahkan fisik terhadap korban.



**Gambar 4. Pengertian Sederhana *Doxing***  
Sumber: codingstudio.id, 2023

Namun demikian, di Indonesia masih cukup banyak pengguna pamula medsos yang belum memahami kejahatan *doxing* dan pentingnya menjaga privasi pribadi dan literasi digital yang memadai, seperti potensi kejahatan *doxing* atau bentuk pelanggaran privasi lainnya. Ini menunjukkan kurangnya pengetahuan dan kesadaran perlindungan data pribadi di kalangan pengguna pamula. Selain itu, kurangnya pemahaman mengenai risiko dan cara-cara melindungi diri secara digital menjadi faktor utama yang memperbesar kerentanan pengguna pamula terhadap kejahatan siber.

Kajian ini bertujuan mengidentifikasi tingkat kesadaran privasi dan menganalisis literasi digital pengguna awal (*early users*) medsos di Indonesia dalam menghadapi risiko *doxing* serta ancaman kejahatan digital lainnya. Melalui pendekatan kualitatif, kajian ini berupaya mengintegrasikan data empiris, konsep teoritis, dan kerangka kebijakan terkait perlindungan data pribadi dan keamanan digital guna memberikan pemahaman komprehensif tentang kesiapsiagaan pengguna pamula menghadapi ekosistem medsos yang rentan terhadap kebocoran data dan pencurian informasi pribadi.

## KAJIAN TEORITIS

### A. Latar Sejarah dan Pengertian *Doxing*

Ditelisik dari asal-usul, *doxing* berasal dari budaya online, khususnya dari ‘Forum Diskusi Usenet’. Awalnya, ia digunakan untuk memublikasikan informasi pribadi seseorang dengan tujuan menyebarkan informasi tersebut secara luas. *Doxing* kerap dikaitkan dengan pencurian nama, email, nomor telepon/ponsel, alamat kantor/rumah, atau data pribadi lain. Istilah *doxing* sendiri telah digunakan sejak adanya agregasi pencurian informasi milik publik yang merekam data individu yang diperoleh melalui situs web atau medsos, *phising*, *fraud*, atau cara-cara ilegal lain (Goodrich, 2003).

*Doxing* berasal dari kata ‘menjatuhkan dokumen’ (*dropping dox*) pada seseorang dengan motif jahat. Pada tahun 1990-an, *doxing* banyak digunakan hacker untuk mengungkap identitas orang secara anonim (Honan, 2014). Saat *doxing* makin populer, ia masuk dalam kamus formal. Oxford British dan World English Dictionary misalnya, mendefinisikan *doxing* sebagai “Mencari dan mempublikasi informasi pribadi atau identitas individu lewat internet dengan niat jahat” (Kamus Oxford 2015). Menurut Goodman (2014), *doxing* tidak

harus dimotivasi oleh rasa dendam atau kebencian. Beberapa insiden penting kasus *doxing* justru melibatkan jurnalis dan intelijen untuk mengungkap data pribadi seseorang yang kerap berlindung dibalik dinding kekuasaan.

*Doxing* adalah bentuk perundungan siber (*cyberbullying*), di mana informasi pribadi dicuri dan disebar. Tindakan ilegal yang melanggar privasi ini telah bergerak liar memfasilitasi kejahatan digital global. *Doxing* dianggap kejahatan karena merupakan tindakan yang sengaja melepas atau membocorkan informasi milik pribadi (individu, kelompok, atau organisasi) pada orang lain (Chen et al., 2019: 3); seringkali dengan maksud untuk mempermalukan, mengancam, atau menghukum individu yang menjadi target (Douglas, 2016: 199; Molas 2024: 3-9).

Namun, penggunaan *doxing* saat ini telah jauh berbeda dari masa awal kelahirannya. Jika di masa awal, *doxing* hanya digunakan sebagai konsep kategoris untuk menjelaskan fenomena sederhana (perilaku tidak etis dan berbahaya). Namun, saat ini *doxing* telah digunakan untuk menggambarkan begitu banyak situasi yang berbeda dengan berbagai tingkat kerumitan dunia digital, sehingga konsep aslinya perlahan memudar. Istilah *doxing* yang awalnya berciri kategoris-definisional, saat ini telah berubah menjadi konsep yang mengekspresikan banyak hal seiring dengan evolusi dan maraknya tindak kejahatan *doxing* dan bisnis anti-*doxing*—yang saat ini banyak ditangani oleh industri *cybersecurity* atau bisnis pengamanan data (Tiffany, 2020).

## **B. Kesadaran Privasi**

Perlahan namun pasti, saat ini perangkat digital telah menginvasi dan menganeksasi identitas (privasi) para pengguna jejaring internet melalui situs web atau platform medsos. Sementara para hacker terus mengintip untuk mengambil-alih data kita. Kesadaran privasi diperlukan oleh setiap *early users*, karena ia terkait dengan pema-haman risiko dan kemampuan untuk mengantisipasi dan melindungi data pribadi dan tindak pencurian. Kesadaran privasi bukan hanya sekedar tahu apa itu data pribadi (nama, alamat email, atau nomor ponsel), namun juga paham dan sadar bagaimana data pribadi dikelola secara efektif dan diproteksi (Jia Ee, 2023).

Kesadaran privasi digital tak hanya soal pemahaman tentang bagaimana data pribadi dikumpulkan, digunakan, disimpan, dan dibagikan secara online, namun juga kesadaran pentingnya melindungi data pribadi dari pencurian. Hal ini mencakup pengetahuan teknis dan kesadaran kritis potensi risiko yang terkait dengan berbagi data pribadi di lingkungan digital (Chandra Das, 2022). Tingkat kesadaran privasi digital yang tinggi memungkinkan pengguna untuk membuat keputusan tepat tentang aktivitas online mereka, *manage* pengaturan privasi, berhati-hati dengan informasi yang mereka bagikan, dan memahami potensi kejahatan dan konsekuensi dari tindakan online yang dilakukan (Mansur, 2020).

## **C. Literasi Digital**

Literasi digital adalah kemampuan seseorang dalam menggunakan, memahami, mengevaluasi, dan menciptakan informasi melalui teknologi digital; termasuk kemampuan untuk mencari, menganalisis, mengkomunikasikan, dan berinteraksi di dunia digital secara aman, etis, dan bertanggung jawab. Dengan kata lain, literasi digital adalah keterampilan yang diperlukan untuk berpartisipasi secara aktif dalam ekosistem masyarakat digital. Literasi digital menjadi skill terpenting saat ini karena ia dapat melindungi integritas pribadi individu,

mendorong kepercayaan dalam interaksi digital, menjunjung tinggi hak-hak dasar individu di dunia yang kian digerakkan oleh data berbasis digital (Tobin, 2024).

UNESCO mendefinisikan literasi digital sebagai: *“the ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital technologies for employment, decent jobs, and entrepreneurship. It includes competences that are variously referred to as computer literacy, ICT literacy, information literacy and media literacy”* (UNESCO, 2018).

Literasi digital tak hanya mencakup kapasitas teknis, tetapi juga mencakup berpikir kritis, pemahaman etis teknologi, dan *skill* berkomunikasi dan berkolaborasi di lingkungan dunia digital. Literasi digital memungkinkan seseorang mengelola identitas dan privasi secara bijak; termasuk mencari informasi secara efektif, menilai kredibilitas sumber, dan menavigasi konten hipertext secara kritis (Kady & Vadeboncoeur, 2024).



**Gambar 5. Empat Pilar Utama Literasi Digital Versi Kominfo/Komdigi RI**

Sumber: Kusumah, 2021

Menurut data Kominfo/Komdigi RI (2023), literasi digital adalah *“Kemampuan untuk menggunakan teknologi, alat komunikasi, atau jaringan digital untuk mengakses, mengelola, mengintegrasikan, menganalisis, dan mengevaluasi informasi secara kritis”*. Terdapat empat pilar utama dalam literasi digital versi Kominfo/Komdigi RI, yakni: *digital skill, digital culture, digital ethics, dan digital safety* (lihat gambar 5 di atas).

#### **D. New Media**

*New media* atau media baru merujuk pada jejaring teknologi informasi dan komunikasi berbasis online yang ditandai oleh interaktivitas tinggi, keterhubungan, dan fleksibilitas. Berbeda dengan media konvensional, media baru memungkinkan pengguna tidak hanya sebagai penerima pasif, tetapi juga sebagai produsen dan kurator konten. Karakteristik utamanya meliputi dinamisme, partisipasi aktif, serta kemampuan pengguna untuk secara mandiri memilih, mengontrol, dan menyebarkan informasi atau berita sesuai kebutuhan pribadi maupun publik. Dengan demikian, media baru menciptakan ruang komunikasi yang lebih demokratis, responsif, namun sekaligus tanggung jawab digital yang lebih besar dari para penggunanya (Flew & Smith, 2008).

Di sisi lain, Lister et. al (2008) mendefinisikan media baru sebagai perubahan penting dalam tata cara produksi, distribusi, dan penggunaan media yang berkaitan dengan teknologi,

nilai sosial, dan sistem budaya. Perubahan versi Lister itu, menurut Fachruddin (2019) setidaknya memicu hadirnya 7 karakteristik baru berikut:

1. *Digitalized*: seluruh data bisa diinput dan dikonversi ke dalam bentuk angka, sehingga lebih mudah digunakan dibanding data analog.
2. *Interactivity*: mudah dikendalikan, hemat waktu, dan berlangsung dua arah.
3. *Hypertextual*: ada potongan teks yang jika diakses dapat memberi sambungan pada halaman situs lainnya (teks yang saling terhubung dengan teks lainnya).
4. *Dispersal* (menyebar): publik bisa berperan ganda, sebagai produsen, distributor, atau konsumen informasi.
5. *Virtuality*: memungkinkan manusia berhadapan langsung dengan objek secara virtual.
6. *Simulation*: tiruan/imitasi dari peristiwa atau sesuatu yang nyata, namun dalam penyajiannya diberi efek tertentu supaya lebih terlihat dramatis.
7. *Networked*: arus perpindahan data lewat jaringan internet, yang memungkinkan *user* bisa mengirim dan menerima data.

## METODE PENELITIAN

Kajian ini berpijak pada ancangan paradigma konstruktivis, yang memandang realitas sosial—termasuk fenomena kejahatan digital seperti *doxing*—bukan sebagai entitas objektif yang tetap, melainkan sebagai hasil konstruksi sosial yang dibentuk melalui interaksi, interpretasi, dan konteks budaya pengguna media digital (Crotty, 1998; Charmaz, 2014). Dalam perspektif ini, makna atas privasi, ancaman digital, dan tanggung jawab pengguna tidak bersifat universal, melainkan dipahami lewat narasi, praktik wacana, pergulatan nilai, dan interaksi yang berlangsung di ruang digital.



**Gambar 5. Model Riset Kualitatif Dengan Objek Kajian Fenomena *Doxing* di Medsos**

Sumber: Spradley (1997: 35)

Secara metodologis, kajian ini mengadopsi pendekatan kualitatif interpretif dengan orientasi *social construction of reality* (Berger & Luckmann, 2013), yang memungkinkan eksplorasi lebih mendalam terhadap pengguna medsos—khususnya pengguna pamula—bagaimana mereka memahami, menafsirkan, dan merespons risiko *doxing* sebagai ancaman serius dunia siber. Data dikumpulkan melalui analisis dokumen berupa studi literatur akademis, kebijakan publik terkait perlindungan data, serta konten medsos (unggahan, komentar, laporan korban) yang relevan dengan fenomena *doxing* di Indonesia. Pendekatan ini memungkinkan peneliti untuk merekonstruksi makna sosial di balik praktik digital sekaligus mengungkap celah dalam kesadaran privasi dan literasi digital.

Studi literatur digunakan untuk memberi latar masalah (*setting of problem*) terkait fenomena *doxing* sebagai praktik kejahatan digital era virtual, terutama bagi pengguna pamula (*early users*) sosmed. Adapun sumber data kajian sepenuhnya bersandar pada data sekunder, yakni observasi non-partisan yang berasal dari konten medsos dan temuan data kualitatif yang relevan dari hasil studi pustaka, kajian dokumen, dan sumber penunjang lainnya. Metode observasi non-partisipan digunakan untuk mengamati fenomena *doxing* yang beroperasi senyap di ruang medsos. Sementara studi literatur digunakan untuk memetakan fenomena *doxing* yang berlangsung di ranah sosial-aktual.

Observasi non-partisipan dan studi literatur sengaja dipilih sebagai model analisis untuk menjaga objektivitas penelitian (Hasanah, 2017). Hasil observasi data—baik data hasil penambangan dari konten medsos maupun data kualitatif hasil studi pustaka. Data kemudian dianalisis secara deskriptif, interpretif, dan tematik melalui empat langkah berikut: (1) pengumpulan dan pengorganisasian data; (2) identifikasi dan kategorisasi data; (3) interpretasi dan analisis data; dan (4) penarikan kesimpulan/verifikasi.

## PEMBAHASAN

Pembahasan dalam kajian ini diarahkan pada tiga aspek saling terkait yang diduga menjadi akar ancaman digital. *Pertama*, fenomena kejahatan *doxing* sebagai bentuk kekerasan digital yang memanfaatkan keterbukaan informasi dan celah keamanan di medsos. *Kedua*, tingkat kesadaran privasi pengguna, yang mencerminkan sejauh mana individu memahami risiko eksposur data pribadi dan pentingnya keamanan digital. *Ketiga*, tingkat literasi digital, yang menentukan kapasitas pengguna dalam mengenali, mencegah, dan merespons ancaman seperti *doxing* secara kritis dan bertanggung jawab. Ketiga dimensi ini menjadi cermin kesiapan masyarakat digital Indonesia dalam membangun ekosistem daring yang aman, etis, dan berkelanjutan.

### A. Telaah Ringkas Studi Terdahulu

Hasil-hasil studi terdahulu terkait fenomena kejahatan *doxing*—seperti studi Eckert & Metzger (2020); Fardiah (2021); Vitak et al. (2023); hasil survei SAFEnet (2024); serta studi Lee & Chen (2025)—akan dibahas secara ringkas untuk memberi landasan konseptual dan perspektif teoritis kajian ini.

(1) Fokus Kajian	(2) Metode Penelitian	(3) Temuan Utama
Doxing sebagai alat pelecehan terhadap perempuan, jurnalis, dan aktivis di ruang digital (Eckert & Metzger, 2020)	Analisis wacana terhadap 1.200 laporan korban kejahatan siber di Amerika, Eropa, dan Asia Tenggara	68% kasus <i>doxing</i> bertujuan membungkam suara kritis melalui ancaman berbasis identitas pribadi
<b>(4) Implikasi/Rekomendasi:</b> <i>Doxing</i> merupakan bentuk kekerasan sistemik-struktural yang memperkuat ketimpangan gender dan kejahatan digital		
(1) Fokus Kajian	(2) Metode Penelitian	(3) Temuan Utama
Tingkat literasi digital remaja Indonesia dalam merespons dampak penggunaan media sosial (Fardiah, 2021)	Kajian deskriptif terhadap remaja pengguna platform digital	Remaja aktif menggunakan media sosial tetapi minim pemahaman tentang etika digital, privasi data, dan sikap kritis terhadap konten
<b>(4) Implikasi/Rekomendasi:</b> perlunya penguatan literasi digital berbasis sekolah dan keluarga sebagai benteng penyelamat (filter preventif)		



(1) Fokus Kajian	(2) Metode Penelitian	(3) Temuan Utama
Kebijakan moderasi konten terhadap <i>doxing</i> di lima platform media sosial besar (Vitak et al., 2023)	Analisis kebijakan dan respons platform terhadap laporan kejahatan <i>doxing</i>	Hanya 31% laporan <i>doxing</i> ditindaklanjuti dalam 48 jam; definisi ‘informasi pribadi’ bervariasi antar-platform
<b>(4) Implikasi/Rekomendasi:</b> diperlukan regulasi global yang mewajibkan standar perlindungan data pribadi yang seragam dan transparan		
(1) Fokus Kajian	(2) Metode Penelitian	(3) Temuan Utama
Peningkatan kasus <i>doxing</i> terhadap aktivis lingkungan, jurnalis independen, dan mahasiswa (2023–2024) (SAFE-net, 2024)	Survei lapangan dan pemantauan kasus <i>doxing</i>	Peningkatan 40% kasus <i>doxing</i> ; banyak melibatkan peretasan akun atau eksploitasi data dari situs pemerintah yang tidak terenkripsi
<b>(4) Implikasi/Rekomendasi:</b> lemahnya implementasi UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP); minimnya mekanisme pelaporan yang responsif dari pihak terkait; korban PDP sering kali tidak mendapat perlindungan hukum		
(1) Fokus Kajian	(2) Metode Penelitian	(3) Temuan Utama
Efektivitas modul edukasi berbasis simulasi <i>doxing</i> di Singapura dan Malaysia (Lee & Chen, 2025)	Eksperimen edukasi dengan skenario simulasi pencurian data	Modul simulasi mampu meningkatkan kesadaran privasi hingga 52% dalam 4 minggu; peserta lebih cenderung menggunakan 2FA dan membatasi jejak digital
<b>(4) Implikasi/Rekomendasi:</b> Pendekatan edukatif proaktif lebih efektif dibanding pendekatan responsif dalam kebijakan literasi digital nasional		

## B. Kejahatan *Doxing* di Indonesia

Saat ini, Indonesia menempati posisi sebagai salah satu negara dengan jumlah pengguna medsos terbesar di dunia, mencerminkan integrasi mendalam platform digital ke dalam kehidupan sehari-hari masyarakat—khususnya generasi muda, *early users* dalam ekosistem digital. Namun, pertumbuhan pesat adopsi medsos tersebut tidak diimbangi secara proporsional oleh tingkat kesadaran privasi maupun kapasitas literasi digital yang memadai. Akibatnya, kelompok pengguna ini rentan terhadap berbagai ancaman kejahatan siber, termasuk *doxing* serta bentuk eksploitasi digital lain yang memanfaatkan celah dalam pemahaman dan praktik keamanan daring. Kesenjangan antara penetrasi teknologi dan kesiapan pengguna menjadi tantangan struktural dalam upaya membangun masyarakat digital Indonesia yang aman, etis, dan berkelanjutan.

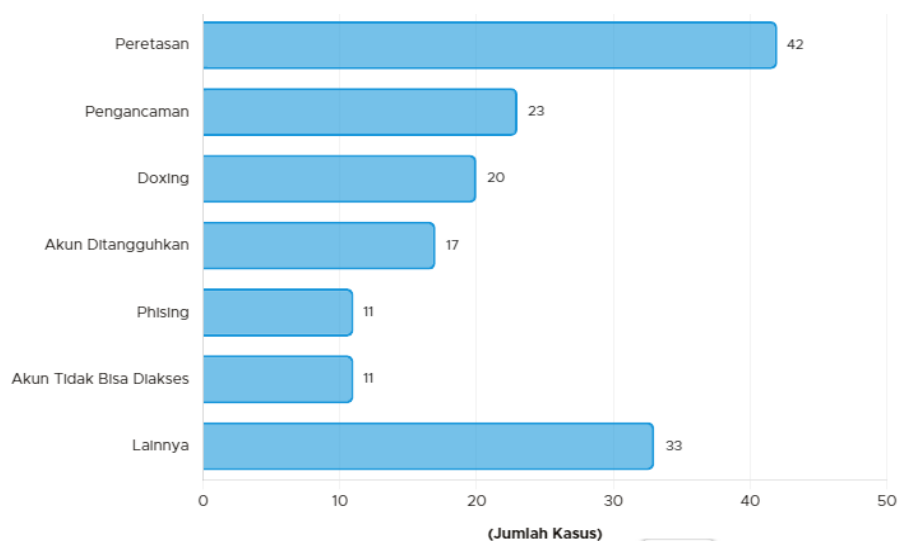
Setidaknya terdapat lima contoh kasus *doxing* anak muda sepanjang tahun 2025 yang viral dan menjadi atensi publik. *Pertama*, kasus dua jurnalis muda CNN Indonesia berinisial ‘AM’ dan ‘YA’ yang menjadi korban *doxing*. Identitas pribadi kedua jurnalis ini disebar secara ilegal. Impaknya, kedua jurnalis muda itu menjadi sasaran kebencian publik dan kerap merasa terancam keselamatannya (Tempo.co, 2025). *Kedua*, kasus *doxing* yang menimpa peneliti ICW berinisial ‘DA’. Peneliti ICW itu ter-*doxing* setelah ia menulis berita Presiden Jokowi masuk daftar nominator tokoh terkorup dunia versi OCCRP. Pasca itu, data pribadi ‘DA’ seperti NIK dan nomor ponsel tersebar di medsos, diikuti dengan intimidasi dan ancaman fisik (Kompas.id, 2025).

*Ketiga*, *doxing* terhadap jurnalis muda Tempo, yang juga menjadi korban *doxing* berupa ancaman dan serangan digital. Kasus ini menunjukkan pola serangan yang menargetkan jurnalis, aktivis, dan tokoh publik yang kritis terhadap pemerintah (Tempo.co, 2025). Keempat, kasus *doxing* terhadap jurnalis muda berinisial ‘AR’ (Pemred *Selasar.co*) di Samarinda. Ia melaporkan kasus *doxing* yang terjadi setelah kritik terhadap penyebaran data pribadi seorang influencer lokal (inisial @kingtae.life). *Doxing* tak hanya menasar data pribadi ‘AR’, data pribadi istrinya pun ikut disebar.

*Kelima*, kasus *doxing* yang menimpa aktivis YLBHI. Selain individu, lembaga advokasi hukum ini juga kerap menjadi target *doxing* dan peretasan data. Upaya *doxing* atas individu kritis adalah bagian dari otoriterisme secara digital. Ini menunjukkan, *doxing* tidak hanya menasar individu, tetapi juga menasar organisasi yang aktif mengadvokasi isu politik, HAM, dan isu demokrasi (Tempo, 2025).

Laporan SAFENet (2024) juga menunjukkan, terkait isu kebebasan berekspresi, sepanjang Juli-September 2024 terdapat 42 kasus pelanggaran dengan jumlah terlapor atau korban sebanyak 33 orang. Dua kasus yang mengemuka adalah tuntutan terhadap Christina Rumahlatu, aktivis perempuan yang dituduh melakukan pencemaran nama saat menyuarakan kerusakan alam di Halmahera, Maluku Utara. Kasus lain terjadi pada Septia, buruh yang mengkritik perusahaannya yang saat masuk persidangan. Selama Juli-September 2024, serangan dan insiden keamanan digital juga terus terjadi meskipun jumlahnya menurun dibandingkan periode sebelumnya, dari 90 kali menjadi 80 kali.

Serangan digital selama periode ini banyak terjadi pada elemen aktivis, mahasiswa, dan organisasi masyarakat sipil. Bentuk serangannya antara lain berupa intimidasi melalui *doxing*, seperti terjadi pada LBH Bandung dan LBH Makassar. Ancaman serupa juga terjadi pada beberapa pesohor kritis, seperti Pandji Pragiwaksono dan Andovi da Lopez. Terakhir, kekerasan berbasis gender online (KBGO) selama periode Juli-September juga masih berlangsung marak, dengan 599 rincian kasus. Korban terbanyak adalah perempuan (47,4%) dibandingkan korban laki-laki (42,7%). Dari sisi sebaran wilayah, Jawa Barat masih paling banyak dengan 142 aduan, kemudian Jawa Tengah (72 aduan), Jawa Timur (65 aduan) dan luar Indonesia (22 aduan) (SAFENet, 2024).

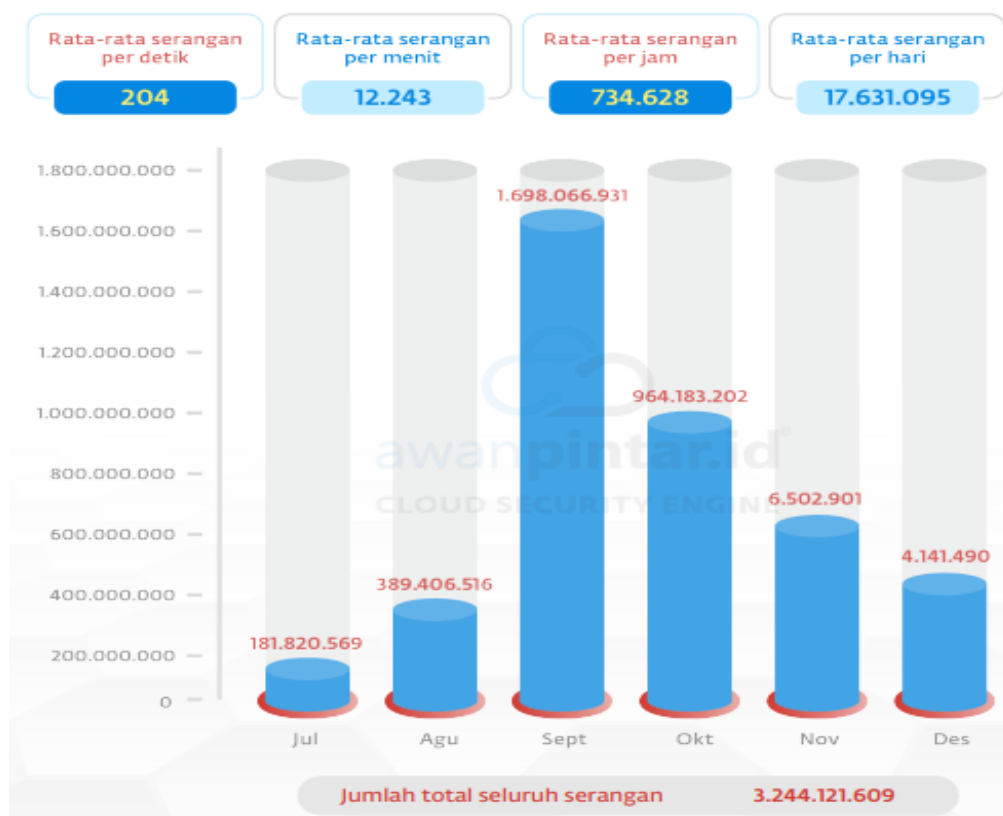


**Gambar 6. Variasi Kasus Serangan Digital Indonesia (Triwulan I 2025)**

Sumber: goodstats.id, 2025

Menurut Douglas (2016), saat ini setidaknya ada tiga tipe kejahatan *doxing*: deanonimisasi, penargetan, dan delegitimasi. Deanonimisasi adalah modus kejahatan *doxing* yang dilakukan melalui *share* informasi untuk mengungkap identitas seseorang yang sebelumnya anonim atau dengan nama samaran (*pseudonim*). Penargetan adalah modus kejahatan *doxing* melalui pengungkapan informasi spesifik tentang keberadaan seseorang secara fisik dengan menunjukkan lokasi keberadaannya, seperti membagi lokasi via GPS atau foto rumah korban. Calon korban dalam tipe penargetan lebih rentan menghadapi serangan fisik langsung. Sedangkan delegitimasi adalah tipe *doxing* melalui *share* informasi identitas pribadi untuk merusak kredibilitas, reputasi, atau karakter korban. *Doxing* jenis ini bertujuan ganda: mempermalukan korban, misalnya mengungkap rahasia keuangan/ hutang-piutang pribadi, atau mengungkap preferensi/orientasi seksual korban.

Di sisi lain, Matthews (2014) mendefinisikan *doxing* tidak hanya sekedar aktivitas berbasis niat jahat (*dolus malus*) untuk mempublikasi secara tidak sah informasi individu yang ditarget dengan maksud menyebarkan rasa malu, menghina, merusak citra dan privasi korban agar dikonsumsi publik, namun juga menyertakan informasi untuk mempermalukan, menghina, dan merusak citra orang lain di sekitar korban, seperti anggota keluarga, teman dekat, atau rekan kerja korban.

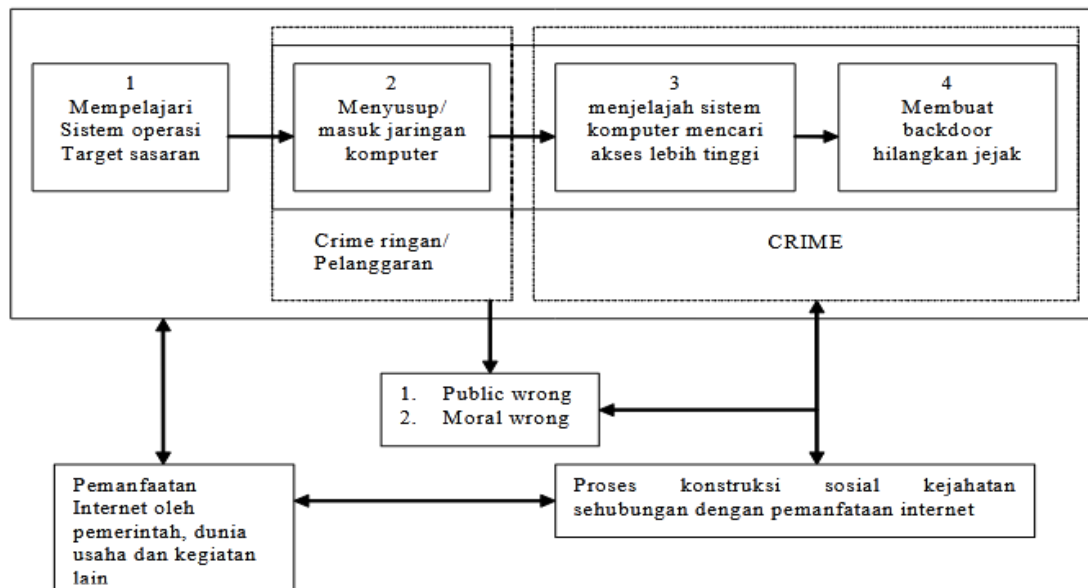


**Gambar 7. Akumulasi Serangan Siber di Indonesia (Triwulan I 2025)**

Sumber: awanpintar.id, 2024

Sementara itu, laporan Southeast Asia Freedom of Expression Network (SAFE Net) juga mencatat peningkatan serangan *doxing*, dimana warga negara (terutama aktivis, jurnalis, akademisi, peneliti, dan para pegiat demokrasi) menjadi kelompok target paling rentan menghadapi serangan *doxing*. Hal ini memperkuat dugaan publik bahwa pelanggaran privasi

dan pencurian data telah digunakan sebagai instrumen untuk mengancam kebebasan pers, ekspresi, dan demokrasi (Kompas.id, 2025).



**Gambar 8. Konstuksi Tindak Kejahatan *Doxing***

Sumber: Rahardjo, 2022

Laporan riset awanpintar.id menunjukkan, memasuki semester 2 tahun 2024 serangan siber di Indonesia melemah dibandingkan akhir semester sebelumnya. Jika ditilik dari bulan ke bulan, serangan siber yang terjadi sangat fluktuatif. Meski demikian, dengan total serangan sebesar 3.244.121.609 keamanan digital di Indonesia masih berada pada kondisi yang lebih buruk dari semester sebelumnya. Catatan khusus ada di bulan September dan Oktober, dimana serangan siber meningkat tajam seiring dengan meningkatnya diskusi mengenai pelarangan judi online.

Di bulan September, terjadi serangan siber terhadap institusi pemerintah. Untuk bulan Oktober, catatan penting politik di tanah air adalah adanya pergantian Presiden. Kendati di akhir tahun mengalami depresiasi yang sangat luar biasa, menurunnya serangan siber bisa berarti bahwa penyerang lebih fokus dalam menentukan target serangan. Ini seperti ketenangan sebelum badai, dimana serangan berikutnya biasanya akan meningkat dengan dampak yang lebih buruk (lihat gambar 7).

*Doxing* adalah pintu masuk dari kejahatan dunia maya lebih lanjut, seperti pencurian *credit card* dan penipuan kartu debit, *phishing*, peretasan, atau kejahatan virtual lainnya. Maraknya kasus *doxing* sejak dua dekade lalu kian menambah panjang daftar panjang kejahatan *doxing* yang merugikan warga negara, terutama yang berstatus sebagai pengguna pamula. Hal ini tentu memberi *warning* pada isu keamanan digital Indonesia, bahwa regulasi dan instrumen perlindungan yang telah selama ini diupayakan pemerintah untuk mengantisipasi kejahatan *doxing* yang terus menyasar privasi warga negara yang posisi tawarnya masih relatif lemah.

### C. Tingkat Kesadaran Privasi

Secara teoritis, asumsi teori *new media*—seperti telah dipaparkan di atas—menekankan pentingnya kesadaran privasi sebagai bagian integral dari literasi digital agar para pengguna, terutama pengguna pemula, dapat memahami konsekuensi dari aktivitas

digital untuk melindungi diri dari ancaman *doxing* dan *cybercrime* (Srivastava, A. et al., 2024). Sebab, fenomena *doxing* dan *cybercrime* adalah implikasi dari perkembangan teknologi digital yang memungkinkan interaktivitas, interkoneksi, dan partisipasi aktif pengguna sosmed dalam produksi dan distribusi konten.

Dalam konteks ini, pengguna medsos tidak lagi hanya sebagai konsumen pasif, melainkan juga aktor atau produsen informasi yang memberi pengaruh dalam peningkatan akses dan partisipasi; yang otomatis membawa implikasi dan risiko baru, terutama terkait pelanggaran privasi dan penyalahgunaan data pribadi (Ravi & Sudharshan, 2024).

Namun demikian, hasil riset yang dilakukan di kalangan mahasiswa dan pengguna medsos pemula menunjukkan bahwa tingkat kesadaran privasi *early users* masih tergolong rendah. Studi Nopriandi (2024) dan IDN Media (2024) juga mengungkap, meski para *early user* medsos sadar pentingnya menjaga keamanan data, praktik pengaturan privasi di medsos masih minim dan belum optimal.

Share Konten	Frekuensi Share (%)
Foto pribadi	70
Lokasi	55
Informasi kontak	35
Status/perasaan	60
Riwayat perjalanan	45

**Gambar 9. Share Konten Data Pribadi**

Sumber: Nopriandi, 2022

Rentang Kesadaran	Persentase (%)
Rendah (Sko2 1–2)	70
Sedang (Sko2 3)	55
Tinggi (Sko2 4–5)	35

**Gambar 10. Rentang Kesadaran Privasi Mahasiswa**

Sumber: Nopriandi, 2022

Hasil penelitian Nopriandi (2024: 93) menunjukkan bahwa dari 300 reponden mahasiswa yang di survei di Yogyakarta, 60%-nya masih sering berbagi informasi pribadi di medsos, seperti *share* foto, status, dan informasi pribadi lainnya tanpa menimbang pengaturan privasi secara ketat (52% responden mengaku tidak pernah memeriksa atau mengubah secara berkala pengaturan privasi akun mereka).

Hal serupa juga ditemukan dalam survei Kominfo (2021) yang menyebut sebagian besar pengguna medsos Indonesia dengan mudah membagikan informasi pribadi, seperti tanggal lahir (67,4%) dan nomor telepon (53,7%) di akun sosmed mereka. Data ini mengindikasikan lemahnya pengguna pamula dalam memahami risiko kebiasaan *sharing* data yang dapat memicu pencurian identitas, *phising*, *doxing*, dan penyalahgunaan data lainnya

Laporan survei IDN Media (2024) juga mengungkap, sebanyak 89% pengguna medsos, terutama Gen Z, merasa kurang nyaman dengan kondisi keamanan medsos saat ini akibat maraknya kasus *doxing*. Sementara itu, 11% Gen Z menyatakan ketidakpuasan atas sistem perlindungan data di Indonesia yang dinilai masih sangat lemah.

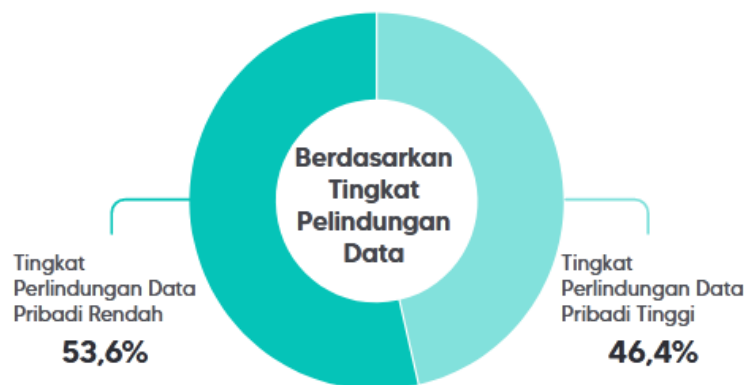
Rilis survei Katadata Insight Center juga menunjukkan, kesadaran warga Indo-nesia pengguna medsos terkait perlindungan data pribadi masih rendah (53,6%), sementara warga negara yang memiliki tingkat perlindungan data pribadi tinggi hanya 46,4% (Katadata.co.id, 2022). Sementara, hasil survei KedaiKOPI (Goodstats.id, 2025) juga mengungkap, 90% responden pengguna pamula internet menggunakan paket data untuk mengakses sosmed, dengan aktivitas utama mencari informasi, *update* berita, menonton konten-konten digital,

dan kurang *care* terhadap *Doxing*. Sikap ini, dus lemahnya rutinitas pengaturan privasi, potensial menjadi target pencurian data pribadi dan *doxing*.

#### D. Tingkat Literasi Digital

Literasi digital bukan sekadar kemampuan menggunakan perangkat teknologi, melainkan mencakup kemampuan kritis dalam mengakses, menggunakan, dan mengevaluasi informasi secara bijak dan bertanggung jawab. Studi Kominfo (2025) menunjukkan bahwa meskipun penetrasi internet dan medsos tinggi, tingkat literasi digital di Indonesia masih belum merata. Pengguna pamula, khususnya anak-anak dan remaja, sering kali mengalami kesulitan dalam memilah informasi dan memilih berita yang bebas dari pengaruh hoaks atau konten negatif.

Hasil survei Kominfo menunjukkan, indeks literasi digital nasional baru mencapai skor 3,78 dari skala 5. Data ini menunjukkan, kendati terjadi peningkatan literasi digital nasional, namun secara rerata masih rendah, baik pada aspek *security* maupun *ethics*. Temuan survei juga menunjukkan, kesadaran para pengguna pamula terkait pentingnya menjaga privasi dan mengenali risiko kejahatan digital masih rendah, sehingga *early users* berada pada posisi paling rentan dari daftar korban penyalahgunaan data dan kejahatan digital (Kominfo, 2025).



**Gambar 11. Rentang Literasi Digital**

Sumber: katadata.co.id, 2021

Selain itu, ada sekitar 35% responden yang menambahkan info lokasi terkini, unduh aplikasi tanpa tahu siapa pembuat atau pengirimnya, dan mengunggah foto KTP. Dapat disimpulkan, masih ada 53,6% masyarakat yang memiliki rentang pelindungan data pribadi yang rendah. Survei IMDI 2025 juga menunjukkan kendati ada peningkatan skor literasi digital dari 37,80 pada 2022 menjadi 43,34 pada 2024, namun, peningkatan skor ini masih menyimpan tantangan besar terkait agenda literasi digital secara menyeluruh, terutama di daerah terpencil dan kalangan pengguna pemula yang rentan terhadap risiko keamanan dan penyalahgunaan data. Rilis Badan Siber dan Sandi Negara (BSSN) juga melaporkan, tingkat kesadaran keamanan siber di kalangan generasi Z (usia 14-18 tahun) masih berada di skor indeks 2,855 dari skala 4. Temuan ini menunjukkan bahwa tingkat literasi digital berada di posisi yang 'cukup baik', namun masih butuh perbaikan, terutama dalam kebiasaan mengganti password dan pengenalan otoritas keamanan siber (Yulistia, 2024).

Data poling literasi digital yang dirilis tahun 2025 (yang melibatkan 20.123 responden) juga mengungkap bahwa sebagian besar masyarakat Indonesia sangat khawatir pada isu judi online, hoaks, dan privasi digital. Simpulan hasil poling merekomendasi peningkatan literasi

digital menjadi indikator penting untuk meningkatkan pemahaman publik terkait bahaya ‘judi online’ (Judol) dan ‘pinjaman online (Pinjol) sebagai agenda penting menghadapi tantangan krusial dunia digital yang makin kompleks, rumit, dan disruptif (Internetsehat.id, 2025).

Sajian data empiris terkait tingkat literasi digital di atas menunjukkan, Indonesia adalah salah satu negara dengan jumlah pengguna internet dan medsos terbesar di dunia, dengan dominasi signifikan dari kelompok generasi muda. Namun, tingginya penetrasi penggunaan digital tersebut tidak sebanding dengan tingkat kesadaran privasi dan kapasitas literasi digital yang memadai. Praktik perlindungan data pribadi serta pemahaman kritis terhadap risiko keamanan siber—terutama ancaman *doxing*—masih relatif rendah alias belum maksimal.

Kesenjangan ini menempatkan negara pada posisi krusial untuk memperkuat tanggung jawab kebijakan publik: pemerintah memiliki kewajiban konstitusional dan normatif untuk secara sistematis, berkelanjutan, dan komprehensif meningkatkan literasi digital warga negara, sejalan dengan prinsip hak atas privasi dan keamanan dalam ekosistem digital yang ke depan akan kian rumit dan kompleks.

## **KESIMPULAN**

Dewasa ini, istilah *doxing* semakin populer seiring dengan meningkatnya kompleksitas kejahatan digital yang bersifat masif dan multidimensi. Seluruh entitas—masyarakat, pemerintah, lembaga pendidikan, dunia usaha, serta kelompok strategis lainnya—merasa rentan terhadap ancaman *doxing* maupun phishing. Kedua istilah tersebut kini telah menjadi frasa yang menimbulkan kekhawatiran publik, bahkan menggeser kecemasan terhadap isu korupsi atau terorisme. Keamanan digital, perlindungan privasi, serta penguatan literasi digital kini menjadi tuntutan warga negara yang wajib diwujudkan, dijalankan, dan dipertahankan oleh negara.

Untuk melindungi ruang publik digital dari ancaman kejahatan siber, diperlukan kemauan politik (*political will*), kolaborasi efektif, serta sinergi antarpihak terkait. Literasi digital dan program keamanan siber yang berkelanjutan menjadi agenda mendesak. Selain peningkatan literasi dan edukasi, penguatan kesadaran privasi serta kebijakan perlindungan data pribadi juga perlu mendapat perhatian serius. Implementasi UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) misalnya, masih memerlukan pengawasan berkelanjutan, evaluasi ketat, serta sanksi yang lebih konkret dan progresif. Di sisi lain, pemerintah perlu menyusun cetak biru komprehensif untuk memastikan setiap platform digital yang digunakan masyarakat patuh terhadap regulasi yang berlaku.

Mengingat perlindungan privasi merupakan pilar penting dalam menjaga martabat dan kebebasan pribadi setiap warga negara, literasi digital menjadi kebutuhan mendesak. Kesadaran privasi akan membentuk ekosistem digital yang aman, yang pada gilirannya mendukung terwujudnya masyarakat digital yang efektif, etis, produktif, dan dinamis—sekaligus menciptakan lingkungan digital yang bertanggung jawab, kompetitif, dan berkelanjutan.

## **DAFTAR PUSTAKA**

Agustin, N. A., & Firdos, R. M. (2024) Studi Literatur: Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman Kejahatan Digital. *Jasmatika: Jurnal Mahasiswa Teknik Informatika*, 3(1), 126-131. doi: 10.35473/jamastika.v3i1.2841.

- Awanpintar.id (2024) Indonesia Waspada: Laporan Anaman Digital Indonesia Semester 2 dan Analisis Serangan 2024—*Ringkasan Eksekutif*. Available at: <https://www.awanpintar.id/wp-content/uploads/2025/02/2024/AwanPintar.id-Laporan-Ancaman-Digital-2024-Green.pdf>.
- Berger, Peter L., & Luckmann, Thomas (2013) *Tafsir Sosial Atas Kenyataan: Risalah Tentang Sosiologi Pengetahuan* (Cetakan ke-10). Jakarta: LP3ES.
- Callula, S. A., Nolani, P. S., Ramadhan, M. R. (2022) Strategi Mempertahankan Budaya Ondel-Ondel dalam Revitalisasi Kebudayaan Betawi. *ARIF: Jurnal Sastra dan Kearifan Lokal*, 1(2), 304–317. doi: 10.21009/Arif.012.08.
- Charmaz, K. (2014) *Constructing Grounded Theory* (2nd ed.). Los Angeles: SAGE Publications Ltd.
- Chen, Mengtong et al (2019) Doxing: What Adolescents Look for and Their Intentions. *International Journal of Environmental Research and Public Health (IJERPH)*, 16(2), 1-14. doi: 10.3390/ijerph16020218.
- Codingstudio.id (2023, August 04) *Apa Itu Doxing? Pengertian, Tujuan dan Cara Mencegahnya*. Available at: <https://codingstudio.id/blog/apa-itu-doxing/>
- Crotty, M. (1998) *The Foundations of Social Research: Meaning and Perspective in the Research Process*. London: SAGE Publications Inc.
- Das, M. C. (2022) Data Privacy on the Internet: A Study on Awareness and Attitudes among the Students of the University of Chittagong in Bangladesh. *Advances in Journalism and Communication*, 10(02), 70-80. doi: 10.4236/ajc.2022.102006.
- Douglas, D. M. (2016) Doxing: A Conceptual Analysis. *Ethics and Information Technology*, 18(3), 199-209. doi: 10.1007/s10676-016-9406-0.
- Eckert, S., & Metzger, J. (2020) Doxxing, Privacy and Gendered Harassment: The Shock and Normalization of Veillance Cultures. *Medien & Kommunikation swissenshaft*, 68(3), 273-287. doi: 10.5771/1615-634X-2020-3-273.
- Entas, D. et al. (2022) Degradasi Budaya Betawi Pada Atraksi Ondel-Ondel Jalanan. *Tourism Scientific Journal*, 7(2), 242–251. doi: 10.32659/tsj.v7i2.183.
- Fachruddin, A. (2019) *Journalism Today*. Jakarta: Kencana.
- Fardiah, D. (2021) Anticipating Social Media Effect: Digital Literacy among Indonesian Adolescents. *International Journal of Multidisciplinary and Current Educational Research*, 3(3), 206-218. [https://www.ijmcer.com/wp-content/uploads/2023/07/IJM CER\\_X0330206218.pdf](https://www.ijmcer.com/wp-content/uploads/2023/07/IJM CER_X0330206218.pdf).
- Flew, T., & Smith, R. (2014) *New Media: An Introduction*. Second Edition. Don Mills ON: Oxford University Press.
- Fuady, M. E. (2005) 'Cybercrime': Fenomena Kejahatan Melalui Internet di Indonesia. *MediaTor: Jurnal Komunikasi*, 6(2), 255-263. doi: 10.29313/mediator.v6i2.1194.
- Goodrich, R. (2023) *What Is Doxing?* Available at: <http://www.technewsdaily.com/17590-what-is-doxing.html>.
- Goodstats.id (2025, May 28) *Pola Akses Internet Indonesia 2025: Provider Mana Terfavorit?* Available at: <https://goodstats.id/article/pola-akses-internet-indonesia-2025-provider-mana-terfavorit-08DMH>.
- Goodstats.id (2025, July 11) *Peretasan Jadi Bentuk Serangan Digital Terbanyak Awal 2025*. Available at: <https://data.goodstats.id/statistic/peretasan-jadi-bentuk-serangan-digital-terbanyak-awal-2025-1EbKH>.



- Goodstats.id (2025, August 17) *Tingkat Penetrasi Internet Indonesia Tembus 80% pada 2025*. Available at: <https://goodstats.id/article/tingkat-penetrasi-internet-indonesia-tembus-80-pada-2025-rape>.
- Hasanah, H. (2017) Teknik-teknik Observasi (Sebuah Alternatif Metode Pengumpulan Data Kualitatif Ilmu-ilmu Sosial). *At-Taqaddum*, 8(1), 21-46. doi: 10.21580/at.v8i1.1163.
- IDN Media Research Institute (2024) *Indonesia Gen Z Report 2024: Understanding and Uncovering the Behavior, Challenges, and Opportunities*. Available at: <https://cdn.idntimes.com/content-documents/indonesia-gen-z-report-2024.pdf>.
- IEEE (2023, November 01) *What is Digital Literacy?* Available at: <https://ctu.ieee.org/blog/2023/01/11/what-is-digital-literacy/>
- Internetsehat.id (2025, January 03) *Digital Literacy Hope 2025*. Available at: <https://internetsehat.id/2025/01/03/digital-literacy-hope-2025/>
- Jia Ee. C. (2023) Analysis of Privacy Awareness among Social Media Users in Malaysia *Jurnal Pengajian Media Malaysia*, 25(1), 67-80. doi: 10.22452/jpmm.vol25no1.6.
- Kady, H. R., & Vadeboncoeur, J. A. (2024) *Digital Literacy*. Available at: <https://www.ebsco.com/research-starters/education/digital-literacy>.
- Kaltimkece.id (2025, May 21) *Kasus Doxing Jurnalis Selasar Dilaporkan ke Polresta Samarinda*. Available at: <https://kaltimkece.id/warta/hukum/kasus-doxing-jurnalis-selasar-dilaporkan-ke-polresta-samarinda>.
- Katadata.co.id (2022) *Pelindungan Data Pribadi Warga RI Masih Tergolong Rendah*. Available at: <https://databoks.katadata.co.id/pelindungan-data-pribadi-warga-ri-masih-tergolong-rendah>.
- Katadata.co.id (2021) *Status Literasi Digital di Indonesia 2021*. Available at: [https://katadata.co.id/media/microsites/litdik/Status\\_Literasi\\_Digital\\_diIndonesia\\_2021\\_190122.pdf](https://katadata.co.id/media/microsites/litdik/Status_Literasi_Digital_diIndonesia_2021_190122.pdf).
- Khaini, M. N. (2025) Fungsi Ondel-Ondel Betawi di Masa Kini: Studi Kasus Kampung Betawi Setu Babakan, Jagakarsa, Jakarta Selatan (*Skripsi*). Padang: Universitas Andalas.
- Kominfo RI (2021) *Literasi Digital: Roadmap 2021-2024*. Available at: <https://wp-content/uploads/Roadmap-Literasi-Digital-2021.pdf>.
- Kompas.id (2020, December 23) *Jurnalis dan Aktivis Jadi Sasaran "Doxing"*. Available at: <https://www.kompas.id/baca/gaya-hidup/2020/12/23/jurnalis-dan-aktivis-rentan-terhadap-doxing>.
- Kusumah, W. (2021, September 10) *Literasi Digital*. Available at: <https://wijayalabs.com/2021/09/10/literasi-digital/>
- Lister, M., et al. (2008). *New Media: A Critical Introduction*. London: Routledge.
- Masur, P. K. (2020) How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information. *Media and Communication*, 8(2), 258–269. doi: 10.17645/mac.v8i2.2855.
- Mansur, S. et al. (2022) Commodification of Betawi Culture of Palang Pintu Festival. *Informasi*, 52(1), 97–118. doi: 10.21831/informasi.v52i1.48825.
- Matthews, R. S. (2014) *A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations*. Available at: [https://era.library.ualberta.ca/items/f9e\\_a399e-0c90-4301-8777-6dffa37fb15b](https://era.library.ualberta.ca/items/f9e_a399e-0c90-4301-8777-6dffa37fb15b).

- Molas, B. (2024) *Doxing: A Literature Review (ICCT Project Report)*. Available at: <https://icct.nl/sites/default/files/2024-12/Molas-Doxing-A-Literature-Review.pdf>.
- Nopriandi (2024) Menjaga Privasi Digital: Studi Tentang Kesadaran Mahasiswa dalam Perlindungan Data Pribadi di Media Sosial. *Polygon: Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam*, 2(6), 87-97. doi: 10.62383/polygon.v2i6.297.
- Raharjo, A. (2002) *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti.
- Ravi, I. A., & Sudharshan, G. M. (2022) A Study on Impact of Social Media Marketing Influence Over Consumers Purchasing Decisions with Special Reference to Chikkamagaluru, Karnataka. *International Journal of Latest Technology In Engineering, Management & Applied Science (IJLTEMAS)*, 12(5), 109-122. doi: 10.51583/IJLTEMAS.
- SAFEnet.or.id (2020, December 22) *Peningkatan Serangan Doxing di Indonesia*. Available at: <https://safenet.or.id/wp-content/uploads/2020/12/Peningkatan-Serangan-Doxing-SAFEnet.pdf>.
- SAFEnet (2024, May 15) *Laporan Pemantauan Situasi Hak-hak Digital di Indonesia Triwulan I 2023–2024*. Available at: <https://safenet.or.id/id/2024/05/laporan-pemantauan-situasi-hak-hak-digital-di-indonesia-triwulan-i-2024/>
- SAFENet (2024, October 21) *Laporan Pemantauan Hak-hak Digital di Indonesia Triwulan III 2024*. Available at: <https://safenet.or.id/id/2024/10/laporan-pemantauan-situasi-hak-hak-digital-di-indonesia-triwulan-iii-2024/>
- Shahab, Y. Z. (1994) *The Creation of Ethnic Tradition: The Betawi of Jakarta (PhD Dissertation)*. London: School of Oriental and African Studies, University of London.
- Selular.id (2025, August 28) *Survei APJII Beberkan Media Sosial Terpopuler di Indonesia 2025*. Available at: <https://selular.id/2025/08/survei-apjii-beberkan-media-sosial-terpopuler-di-indonesia-2025/>
- Shopify-com (2025, May 14) *Top 10 Most Popular Social Media Platforms in 2025*. Available at: <https://www-shopify-com/most-popular-social-media-platforms?>
- Srivastava, A. et al. (2024). Threats and Challenges Regarding Digital Literacy: Generation Z's Approach. *Journal of Communications Finance*, 1(1), 47-61. Retrieved from <https://nicf.gov.in/wp-content/uploads/2025/09/JOURNAL.pdf>.
- Surfshark.com (2025, February 04) *Global Data Breach Statistics: A 2024 Recap*. Available at: <https://surfshark.com/research/study/data-breach-recap-2024#>
- Suyahya, I. (2019) *Ondel-Ondel Show: Between Local Wisdom Preservation And Damage To Betawi Culture (Proceedings 4<sup>th</sup> International Seminar on Social Studies and History Education—ISSSHE 2019)*. [https://repository.upi.edu/47321/41/SPS\\_PRO\\_PIPS\\_ISSSHE\\_2019\\_Indra\\_Suyahya.pdf](https://repository.upi.edu/47321/41/SPS_PRO_PIPS_ISSSHE_2019_Indra_Suyahya.pdf).
- Tempo.co (2025, January 04) *Peneliti ICW Kena Doxing, YLBHI: Kami Khawatir Ini Bagian dari Operasi Pembungkaman*. Available at: <https://www.tempo.co/politik/peneliti-icw-kena-doxing-ylbhi-kami-khawatir-ini-bagian-dari-operasi-pembungkaman-1189802>.
- Tempo.co (2025, January 15) *Sederet Kasus Doxing Menimpa Jurnalis dan Aktivistis, Terakhir Data Pribadi Peneliti ICW Disebar ke Publik*. Available at: <https://www.tempo.co/hukum/sederet-kasus-doxing-menimpa-jurnalis-dan-aktivis-terakhir-data-pribadi-peneliti-icw-disebar-ke-publik-1194270>.

- Tiffany, K. (2022, April 22) *Doxxing Means Whatever You Want It To*. Available at: <https://www.theatlantic.com/technology/archive/2022/04/doxxing-meaning-libs-of-tiktok/629643/>
- Tobin, D. (2024, December 21) *What is Data Privacy—and Why Is It Important?* Available at: <https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/>
- UNESCO (2018) *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2*. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000265403.locale=en>.
- Vitak, J. et al. (2023) “They Posted My Address”: Platform Responses to Doxing and the Limits of Content Moderation. *Proceedings of the ACM on Human-Computer Interaction (CSCW)*, No. 7, Article 387. <https://doi.org/10.1145/3610198>.
- Wisnuadi, K. (2025, April 05) *Statistik Menarik Industri Digital di Indonesia Tahun 2025*. Available at: <https://dipstrategy.co.id/blog/statistik-menarik-industri-digital-di-indonesia-tahun-2025/>
- Yudiana, T. C., et al. (2022) The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia. *Padjajaran: Jurnal Ilmu Hukum*, 9(1), 24-45. doi: 10.22304/pjih.v9n1.a2.
- Yulistia, C. (2025, February 20) *Analisis Korelasi Kesadaran, Perilaku, dan Keamanan Siber*. Available at: <https://id.linkedin.com/pulse/analisis-korelasi-kesadaran-perilaku-dan-keamanan-chandra-qrtnc>.