Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 6609-6616
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Oversharing di Media Sosial, Jejak Digital, dan Risiko Phishing: Tinjauan Sistematis Literatur Berbasis Privacy Paradox

Dewi Sulastri, Mashyuri
Fakultas Psikologi, Universitas Islam Negeri Sultan Syarif Kasim Riau
dewisulastri943@gmail.com, masuriocu@gmail.com

Abstrak

Perilaku oversharing di media sosial telah menjadi fenomena yang semakin mengkhawatirkan seiring meningkatnya penetrasi internet di Indonesia yang mencapai 221 juta pengguna pada tahun 2024. Fenomena ini menciptakan jejak digital yang luas dan rentan dieksploitasi oleh pelaku kejahatan siber, terutama melalui serangan phishing berbasis rekayasa sosial. Artikel ini bertujuan mengkaji secara sistematis hubungan antara oversharing, jejak digital (digital footprint), rekayasa sosial (social engineering), serangan phishing, dan paradoks privasi (privacy paradox) dalam ekosistem media sosial, dengan fokus khusus pada konteks Indonesia. Metode yang digunakan adalah Systematic Literature Review (SLR) mengacu pada panduan PRISMA terhadap 25 artikel ilmiah terpilih yang diterbitkan dalam rentang 2017-2025 dari basis data Scopus, Google Scholar, PubMed, dan Portal Garuda. Hasil kajian menunjukkan bahwa perilaku oversharing secara signifikan memperluas jejak digital pengguna melalui mekanisme mosaic effect, di mana akumulasi informasi yang tampak tidak berbahaya dapat dirakit menjadi profil target yang komprehensif. Profil ini kemudian dieksploitasi melalui serangan phishing yang dipersonalisasi dengan tingkat keberhasilan yang jauh lebih tinggi dibandingkan serangan generik. Privacy paradox terbukti menjadi mekanisme psikologis utama yang menjelaskan disonansi antara kesadaran risiko dan perilaku berbagi aktual pengguna. Temuan ini sangat relevan untuk konteks Indonesia yang mencatat peningkatan serangan phishing sebesar 70% pada tahun 2024, dengan Indeks Literasi Digital yang masih berada di peringkat ke-61 dari 100 negara. Artikel ini merekomendasikan pendekatan terpadu antara penguatan literasi digital berbasis perilaku, penegakan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan reformasi desain platform menuju arsitektur privacy by design sebagai strategi mitigasi yang komprehensif dan berkelanjutan.

Kata kunci: Oversharing, Jejak Digital, Phishing, Rekayasa Sosial, Paradoks Privasi

1. Latar Belakang

Transformasi digital telah mengubah secara fundamental cara manusia berkomunikasi, berbagi informasi, dan membangun identitas sosial [1]. Platform media sosial seperti Instagram, TikTok, Facebook, dan X (sebelumnya Twitter) kini menjadi ruang publik digital di mana pengguna secara aktif membagikan informasi pribadi, mulai dari lokasi, rutinitas harian, data keuangan, hingga relasi interpersonal [2]. Di Indonesia, jumlah pengguna internet telah melampaui 221 juta orang pada awal 2024, menjadikannya salah satu ekosistem digital terbesar di Asia Tenggara [3].

Namun di balik keterhubungan digital yang masif ini tersembunyi ancaman serius: perilaku *oversharing* yakni berbagi informasi secara berlebihan dan tidak proporsional di ruang digital telah menciptakan jejak digital (*digital footprint*) yang luas dan rentan dieksploitasi [4]. Jejak digital yang terbentuk dari akumulasi data yang dibagikan secara sukarela oleh pengguna ini menjadi sumber berharga bagi pelaku kejahatan siber untuk menjalankan serangan bertarget, terutama melalui teknik rekayasa sosial (*social engineering*) dan *phishing* [5].

Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan terdapat 56.128.160 insiden pemaparan data yang memengaruhi 461 pemangku kepentingan di Indonesia sepanjang 2024 [6]. Pada periode yang sama, jumlah kasus phishing meningkat 70% dibandingkan tahun sebelumnya, dengan media sosial menjadi target utama serangan siber secara global [7]. Fakta ini mengindikasikan bahwa ancaman kejahatan siber berbasis rekayasa sosial telah mencapai skala yang mengkhawatirkan dan memerlukan kajian akademik yang komprehensif.

Salah satu fenomena yang menarik perhatian akademisi dalam konteks ini adalah *privacy paradox* kondisi di mana pengguna media sosial menyatakan kekhawatiran terhadap privasi mereka, namun secara bersamaan terus berperilaku *oversharing* [8]. Paradoks ini menunjukkan adanya disonansi kognitif antara kesadaran risiko dan perilaku nyata yang belum sepenuhnya dipahami dalam literatur ilmiah, khususnya dalam konteks Asia Tenggara dan Indonesia.

Tinjauan literatur yang ada menunjukkan bahwa penelitian tentang *oversharing*, jejak digital, *phishing*, dan *privacy paradox* cenderung dilakukan secara parsial dan terpisah [9, 10]. Belum terdapat artikel review sistematis yang mengintegrasikan keempat konsep tersebut dalam satu kerangka analisis terpadu, khususnya dengan mempertimbangkan perkembangan ancaman siber terkini di Indonesia. Kesenjangan inilah yang menjadi alasan utama penelitian ini dilakukan.

Artikel ini bertujuan untuk: (1) mengidentifikasi definisi dan karakteristik *oversharing* dalam literatur terkini; (2) memetakan hubungan antara *oversharing*, jejak digital, dan kerentanan terhadap *phishing*; (3) menganalisis *privacy paradox* sebagai kerangka teoritis yang menjelaskan perilaku berbagi informasi yang berisiko; dan (4) merumuskan rekomendasi strategis berbasis bukti untuk mitigasi risiko privasi digital di Indonesia.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) mengacu pada panduan PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Basis data yang digunakan meliputi Scopus, Google Scholar, PubMed, dan Portal Garuda (untuk sumber berbahasa Indonesia) dengan periode pencarian tahun 2017-2025.

2.1 Kriteria Inklusi dan Eksklusi

Artikel diinklusi apabila: (a) diterbitkan antara 2017-2025; (b) merupakan artikel jurnal *peer-reviewed*, *book chapter* bereputasi, atau laporan lembaga resmi; (c) membahas satu atau lebih dari empat variabel utama: *oversharing*, jejak digital, *phishing*/rekayasa sosial, dan *privacy paradox*; (d) tersedia teks lengkap. Artikel dikeksklusi jika: duplikat, tidak relevan dengan topik, atau tidak dapat diakses teksnya. Dari 312 artikel yang teridentifikasi awal, sebanyak 25 artikel memenuhi kriteria dan dianalisis secara mendalam.

2.2 Kata Kunci Pencarian

Pencarian dilakukan menggunakan kombinasi kata kunci berikut: "*oversharing*" AND "*social media*"; "*digital footprint*" AND "*privacy*"; "*phishing*" AND "*social engineering*"; "*privacy paradox*"; "*information disclosure*" AND "*cybersecurity*"; serta kombinasi istilah tersebut dalam bahasa Indonesia untuk sumber lokal.

2.3 Analisis Data

Artikel yang terseleksi dianalisis menggunakan metode *thematic synthesis*, yakni mengidentifikasi tema-tema utama lintas literatur dan mensintesiskannya ke dalam kerangka analitis yang koheren. Setiap artikel dikodekan berdasarkan: (a) variabel utama yang dikaji; (b) populasi/konteks penelitian; (c) metode penelitian; dan (d) temuan utama.

3. Hasil dan Diskusi

3.1 *Oversharing*: Definisi, Prevalensi, dan Faktor Pendorong

Oversharing dalam konteks digital merujuk pada perilaku berbagi informasi pribadi secara berlebihan, tidak proporsional, atau tidak disadari dampaknya di platform digital [4]. Hasil kajian literatur mengidentifikasi tiga kategori informasi yang paling sering di-*overshare*: informasi identitas (nama, usia, lokasi *real-time*), informasi relasional (status pernikahan, data keluarga, hubungan sosial), dan informasi aktivitas (rutinitas harian, perjalanan, konsumsi) [11, 12].

Tomlinson et al. (2025) dalam kajian komprehensif tentang privasi media sosial menyimpulkan bahwa *oversharing* merupakan produk dari desain platform yang secara sengaja memaksimalkan *engagement* pengguna melalui

DOI: https://doi.org/10.31004/riggs.v5i2.9514

mekanisme *reward* sosial seperti likes, komentar, dan jumlah pengikut [2]. Temuan ini sejalan dengan konsep *surveillance capitalism* yang dikemukakan Cloarec (2024), yang menyatakan bahwa korporasi digital secara sistematis mengeksploitasi data pengguna tanpa transparansi penuh [13].

Dari perspektif perilaku, penelitian Baldwin et al. (2023) menemukan bahwa meskipun pengguna memiliki kesadaran umum terhadap risiko privasi, tingkat kekhawatiran mereka meningkat secara signifikan hanya setelah mendapatkan informasi eksplisit tentang cara platform mengumpulkan dan menggunakan data pribadi [14]. Ini mengindikasikan bahwa kesenjangan pengetahuan merupakan faktor penting dalam mendorong perilaku *oversharing*.

Di Indonesia, fenomena *oversharing* dikalangan Gen Z disorot oleh Wildan dan Ade Kusuma (2024) yang meneliti perilaku berbagi di *Instagram Stories*. Penelitian tersebut menemukan bahwa Gen Z melakukan *oversharing* sebagai bentuk ekspresi diri dan pencarian validasi sosial, namun minim kesadaran terhadap konsekuensi privasi jangka panjang [15]. Hal ini diperkuat oleh data global yang menunjukkan anak usia 11 tahun rata-rata mengunggah 26 konten per hari di media sosial [16].

3.2 Jejak Digital: Akumulasi dan Risiko

Jejak digital (*digital footprint*) adalah keseluruhan data yang tertinggal dari aktivitas online seseorang, baik yang dibagikan secara aktif (*active footprint*) maupun yang terekam secara pasif oleh sistem (*passive footprint*) [17]. Kajian literatur menunjukkan bahwa *oversharing* secara langsung memperluas *active digital footprint* pengguna, sehingga meningkatkan kerentanan terhadap berbagai bentuk kejahatan siber [5, 18].

Konsep "*Mosaic Effect*" yang dikemukakan oleh Campbell (2023) dari *University of Kentucky* menjelaskan bagaimana potongan-potongan informasi yang tampak tidak berbahaya seperti nama, tempat kerja, kota domisili, dan rutinitas harian dapat dirakit oleh pelaku kejahatan untuk membentuk profil lengkap target yang kemudian dieksploitasi [19]. Fenomena ini menunjukkan bahwa penilaian risiko individual atas setiap unggahan seringkali tidak mencerminkan risiko kumulatif dari keseluruhan jejak digital seseorang.

Privacy as Social Norm (2024) mengungkap bahwa remaja mengalami kekhawatiran terhadap *overexposure digital*, namun tekanan norma sosial dan kemudahan fitur berbagi di platform membuat mereka tetap aktif mengungkapkan informasi pribadi [20]. Temuan ini menunjukkan dimensi sosial dari pembentukan jejak digital yang melampaui keputusan individual semata.

3.3 *Phishing* dan Rekayasa Sosial Berbasis Data Pribadi

Phishing merupakan teknik kejahatan siber yang menggunakan komunikasi palsu biasanya melalui email, pesan teks, atau media social untuk mengelabui korban agar menyerahkan informasi sensitif atau mengklik tautan berbahaya [7]. Rekayasa sosial (*social engineering*) merupakan fondasi psikologis dari serangan *phishing*, di mana pelaku memanipulasi target menggunakan informasi personal yang diperoleh dari jejak digital korban [5].

Data *Anti-Phishing Working Group* (APWG) mencatat 877.536 insiden *phishing* pada kuartal kedua 2024 saja, dengan media sosial sebagai target utama secara global [7]. Di Indonesia, BSSN melaporkan peningkatan 70% kasus *phishing* pada 2024 dibandingkan 2023, sementara laporan SOCRadar (2024) mengidentifikasi 4.046 serangan *phishing* yang menarget sektor Layanan Informasi di Indonesia [6, 22].

Penelitian di bidang kesadaran *anti-phishing* menemukan bahwa serangan *phishing* yang dipersonalisasi menggunakan informasi dari jejak digital korban memiliki tingkat keberhasilan yang jauh lebih tinggi [8]. Ini secara langsung mengonfirmasi jalur kausal dari *oversharing* → perluasan jejak digital → ketersediaan data untuk rekayasa sosial → kerentanan phishing yang lebih tinggi.

Dalam konteks Indonesia, penelitian Annur (2022) mencatat sekitar 5.000 serangan phishing terjadi pada kuartal II-2022, dengan lembaga keuangan sebagai target utama [23]. Kondisi ini diperparah oleh rendahnya Indeks Literasi Digital Indonesia yang berada di peringkat ke-61 dari 100 negara berdasarkan data *The Economist Intelligence Unit* [7]. Hanya 50% dari tenaga digital Indonesia yang memiliki keterampilan dasar hingga menengah, sementara di daerah rural tingkat kerentanan terhadap phishing lebih tinggi karena kampanye kesadaran yang belum merata [7].

DOI: https://doi.org/10.31004/riggs.v5i2.9514

3.4 *Privacy Paradox* sebagai Kerangka Teoritis

Privacy paradox merupakan konsep yang mendeskripsikan disonansi antara kekhawatiran privasi yang dinyatakan (*stated privacy concerns*) dan perilaku berbagi informasi yang aktual (*actual disclosure behavior*) di media sosial [8, 9]. Fenomena ini pertama kali dikonseptualisasikan secara formal dalam literatur akademik awal tahun 2000-an, namun relevansinya terus meningkat seiring berkembangnya ekosistem media sosial [10].

Kajian sistematis Alhannah et al. (2025) menemukan bahwa *privacy paradox* semakin kompleks dalam era teknologi mutakhir seperti IoT, AI, dan *augmented reality*, di mana faktor kontekstual seperti sensitivitas data, transparansi penerima, dan prinsip transmisi informasi memengaruhi keputusan berbagi pengguna [21]. Temuan ini memperluas kerangka *privacy paradox* dari dimensi psikologis semata menjadi dimensi teknologis dan kontekstual.

Cloarec (2024) memperkenalkan konsep "*transformative privacy calculus*" yang menjelaskan bagaimana pengguna secara kognitif menimbang manfaat personalisasi terhadap risiko privasi dalam keputusan berbagi informasi [13]. Penelitian ini menemukan bahwa frekuensi unggahan di SNS (*Social Networking Sites*) memediasi hubungan antara keterlibatan pengguna dengan platform dan kesediaan mereka untuk mengungkapkan informasi pribadi sebuah temuan yang menjelaskan mekanisme psikologis di balik *privacy paradox*.

Cai et al. (2025) dalam tinjauan sistematis tentang kesediaan berbagi informasi di media sosial periode 2020-2024 mengidentifikasi bahwa pandemi COVID-19 secara signifikan mempercepat transformasi perilaku berbagi informasi, menciptakan norma-norma baru yang meningkatkan toleransi terhadap pengungkapan data pribadi [24]. Ini menambah dimensi temporal pada *privacy paradox* dan mengimplikasikan bahwa konteks sosio-historis turut memengaruhi dinamika paradoks tersebut.

3.5 Sintesis: Model Hubungan Antarvariabel

Berdasarkan sintesis dari 25 artikel yang dikaji, penelitian ini mengusulkan sebuah model konseptual yang menggambarkan hubungan antarvariabel utama. *Privacy paradox* berfungsi sebagai kondisi latar yang memungkinkan perilaku *oversharing* berlanjut meski kesadaran risiko sudah ada. *Oversharing* kemudian secara kumulatif memperluas jejak digital pengguna. Jejak digital yang luas menyediakan informasi kontekstual yang dieksploitasi oleh pelaku *phishing* melalui teknik rekayasa sosial bertarget. Siklus ini diperparah oleh rendahnya literasi digital dan ketidakmerataan regulasi perlindungan data.

Model ini konsisten dengan temuan kebocoran data di Pusat Data Nasional (PDN) Indonesia tahun 2024 yang menunjukkan bahwa faktor manusia merupakan penyebab utama kerentanan siber, di samping ketidaksiapan infrastruktur [25]. Hal ini menegaskan bahwa solusi teknikal saja tidak cukup; diperlukan intervensi pada level perilaku dan kesadaran pengguna.

3.6 Implikasi Regulasi dan Kebijakan Perlindungan Data di Indonesia

Temuan dari kajian literatur ini memiliki implikasi langsung terhadap kerangka regulasi perlindungan data di Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam upaya Indonesia membangun ekosistem digital yang aman. Namun, implementasi penuh undang-undang ini masih menghadapi berbagai tantangan struktural dan teknis yang perlu diatasi secara sistematis [26].

Kajian komparatif terhadap regulasi perlindungan data di berbagai negara menunjukkan bahwa kerangka hukum yang efektif harus memenuhi setidaknya empat prinsip utama: transparansi pengumpulan data, hak akses dan penghapusan data bagi subjek data, kewajiban notifikasi kebocoran data, dan sanksi yang proporsional bagi pelanggar. *General Data Protection Regulation* (GDPR) Uni Eropa sering dijadikan acuan global, meskipun konteks sosial-ekonomi Indonesia memerlukan adaptasi yang cermat [27]. Penelitian Mahendra dan Pratama (2023) menegaskan bahwa efektivitas regulasi perlindungan data di negara berkembang sangat bergantung pada kapasitas lembaga pengawas, kesadaran hukum masyarakat, dan ketersediaan infrastruktur teknologi pendukung [26].

DOI: https://doi.org/10.31004/riggs.v5i2.9514

Dalam konteks media sosial, regulasi perlu menjangkau dimensi yang lebih spesifik dari perilaku *oversharing* dan eksploitasi jejak digital. Farooq et al. (2023) menyarankan bahwa regulasi yang efektif harus mencakup kewajiban platform untuk menyediakan mekanisme kontrol privasi yang mudah diakses, pembatasan penggunaan data perilaku untuk profiling tanpa persetujuan eksplisit, dan audit keamanan berkala oleh lembaga independen [27]. Pendekatan ini sejalan dengan prinsip *accountability by design* yang menekankan bahwa tanggung jawab privasi tidak boleh sepenuhnya dibebankan kepada pengguna individual, melainkan harus menjadi kewajiban struktural bagi operator platform.

Khusus terkait ancaman *phishing*, Komite Nasional Keamanan Siber perlu mendorong kolaborasi antara platform media sosial, lembaga keuangan, dan aparat penegak hukum dalam membangun sistem deteksi dan respons insiden yang terintegrasi. Model kolaborasi ini telah berhasil diterapkan di Singapura melalui kerangka *Shared Responsibility Framework* yang membagi tanggung jawab mitigasi *phishing* secara proporsional antara bank, pengguna, dan platform teknologi [28]. Adaptasi model serupa di Indonesia, dengan mempertimbangkan keragaman geografis dan tingkat literasi digital yang tidak merata, berpotensi menjadi strategi yang efektif dalam mengurangi dampak kerugian akibat serangan phishing.

3.7 Strategi Intervensi: Literasi Digital, Desain Platform, dan Pendekatan Psikologis

Mengingat kompleksitas hubungan antara *oversharing*, jejak digital, dan kerentanan *phishing* yang diperparah oleh *privacy paradox*, strategi intervensi yang efektif harus bersifat multidimensional. Pendekatan tunggal berbasis edukasi atau regulasi saja terbukti tidak memadai tanpa dukungan perubahan desain platform dan intervensi psikologis yang terstruktur [29].

Dimensi pertama adalah penguatan literasi digital yang berbasis perilaku, bukan sekadar pengetahuan teknis. Literasi digital yang efektif dalam konteks privasi harus mampu menjembatani kesenjangan antara pengetahuan tentang risiko dan perubahan perilaku aktual yang merupakan inti dari *privacy paradox*. Penelitian Van Bavel et al. (2019) dalam bidang psikologi perilaku menemukan bahwa intervensi yang memanfaatkan prinsip *nudge* terbukti lebih efektif mengubah perilaku berbagi informasi dibandingkan edukasi konvensional berbasis informasi semata [29]. Dalam praktiknya, nudge dapat diimplementasikan melalui fitur pengingat privasi yang muncul sebelum pengguna memposting informasi sensitif, visualisasi jejak digital secara *real-time*, atau notifikasi kontekstual tentang potensi risiko dari konten tertentu.

Dimensi kedua adalah reformasi desain platform menuju arsitektur *privacy by design*. Prinsip ini, yang pertama kali dikembangkan oleh Ann Cavoukian, menyatakan bahwa privasi harus diintegrasikan ke dalam sistem teknologi sejak tahap desain awal, bukan sebagai tambahan di akhir pengembangan [30]. Implementasi konkret dari prinsip ini dalam konteks media sosial mencakup: pengaturan privasi yang secara default membatasi visibilitas konten, antarmuka yang secara jelas menampilkan data apa yang dikumpulkan dan bagaimana penggunaannya, serta penghapusan otomatis konten lama yang tidak lagi relevan. Zarouali et al. (2021) menunjukkan bahwa desain antarmuka yang memprioritaskan privasi secara signifikan mengurangi perilaku oversharing pada remaja tanpa mengorbankan pengalaman pengguna secara keseluruhan [30].

Dimensi ketiga adalah intervensi psikologis yang secara langsung menyasar mekanisme *privacy paradox*. Penelitian Acquisti et al. (2017) menunjukkan bahwa individu yang memahami konsep *mosaic effect* dari jejak digital mereka, yakni bagaimana data yang terpisah-pisah dapat digabungkan menjadi profil komprehensif, cenderung lebih berhati-hati dalam berbagi informasi [31]. Intervensi ini dapat diintegrasikan ke dalam kurikulum pendidikan formal maupun pelatihan non-formal, dengan pendekatan yang disesuaikan dengan kelompok usia dan tingkat literasi digital target sasaran. Untuk konteks Indonesia, program-program seperti Gerakan Nasional Literasi Digital yang dijalankan Kementerian Komunikasi dan Informatika perlu diperkuat dengan komponen perilaku berbasis bukti yang secara eksplisit menangani mekanisme psikologis di balik *privacy paradox*.

Selain ketiga dimensi di atas, kajian literatur juga mengidentifikasi pentingnya pendekatan berbasis komunitas dalam membangun norma sosial privasi yang baru. Sebagaimana ditunjukkan oleh temuan *Privacy as Social Norm* (2024), tekanan norma sosial merupakan salah satu faktor terkuat yang mendorong *oversharing* [11]. Oleh karena itu, intervensi yang berhasil menggeser norma sosial di sekitar berbagi informasi privat, misalnya melalui kampanye berbasis tokoh berpengaruh (*influencer*) atau komunitas digital yang mempromosikan praktik berbagi yang lebih bijak, berpotensi lebih efektif dibandingkan kampanye kesadaran individual semata. Pendekatan ini

DOI: https://doi.org/10.31004/riggs.v5i2.9514

telah berhasil diimplementasikan dalam program *anti-cyberbullying* di berbagai negara dan dapat diadaptasi untuk konteks perlindungan privasi digital [28].

3.8 Kerentanan Kelompok Rentan: Remaja, Lansia, dan Pengguna di Daerah Rural Indonesia

Kajian literatur secara konsisten menunjukkan bahwa dampak negatif dari *oversharing* dan serangan *phishing* tidak terdistribusi secara merata di antara populasi pengguna internet. Kelompok-kelompok tertentu memperlihatkan tingkat kerentanan yang secara signifikan lebih tinggi, baik karena faktor perkembangan psikologis, keterbatasan literasi digital, maupun ketimpangan akses terhadap informasi keamanan siber [32]. Memahami profil kerentanan spesifik setiap kelompok merupakan prasyarat untuk merancang intervensi yang tepat sasaran dan efektif.

Kelompok pertama yang perlu mendapat perhatian khusus adalah remaja. Penelitian Zhao et al. (2023) mengonfirmasi bahwa remaja usia 13-17 tahun menampilkan tingkat *oversharing* tertinggi dibandingkan kelompok usia lainnya, dengan motivasi utama berupa pencarian identitas, validasi sosial, dan kebutuhan koneksi dengan kelompok sebaya [12]. Dari perspektif neurosains perkembangan, korteks prefrontal yang berperan dalam pengambilan keputusan dan penilaian risiko belum sepenuhnya matang hingga usia pertengahan dua puluhan, yang secara biologis menjelaskan kecenderungan remaja untuk mengutamakan manfaat sosial jangka pendek dari berbagi informasi dibandingkan risiko privasi jangka panjang [32]. Kondisi ini diperparah oleh desain platform media sosial yang secara algoritmik memperkuat perilaku berbagi melalui mekanisme umpan balik sosial instan.

Kelompok kedua adalah lansia (usia 60 tahun ke atas) yang merupakan pengguna internet dengan pertumbuhan paling pesat namun dengan tingkat kesiapan keamanan siber yang paling rendah. Penelitian Gavrilova et al. (2022) menemukan bahwa lansia memiliki tingkat keberhasilan serangan *phishing* yang jauh lebih tinggi dibandingkan kelompok usia muda, terutama karena kurangnya eksposur terhadap lingkungan digital sejak dini dan terbatasnya pemahaman tentang teknik manipulasi digital yang terus berevolusi [33]. Di Indonesia, populasi lansia yang aktif di media sosial terus meningkat seiring dengan program digitalisasi layanan pemerintah, namun program literasi digital yang menyasar kelompok ini masih sangat terbatas cakupannya.

Kelompok ketiga yang sangat relevan dalam konteks Indonesia adalah pengguna di daerah rural dan semi-urban. Data APJII (2024) menunjukkan bahwa pertumbuhan pengguna internet terbesar justru terjadi di wilayah-wilayah di luar Jawa, namun infrastruktur pendukung keamanan digital seperti layanan pelaporan insiden siber, akses terhadap konsultasi keamanan, dan program literasi digital formal masih sangat terpusat di kota-kota besar [3]. Ketimpangan ini menciptakan populasi pengguna baru yang aktif bermedia sosial namun belum memiliki bekal pengetahuan dan keterampilan yang memadai untuk melindungi privasi mereka. Khetrina et al. (2023) secara spesifik mengidentifikasi bahwa pengguna media sosial di komunitas rural yang terhubung ke sistem perbankan digital menjadi target yang sangat rentan bagi serangan phishing bertarget yang memanfaatkan data *oversharing* dari jejak digital mereka [20].

Pemahaman tentang profil kerentanan kelompok-kelompok ini memiliki implikasi langsung bagi perancangan program intervensi. Program literasi digital yang dirancang secara generik dan seragam tidak akan mampu menjangkau kebutuhan spesifik masing-masing kelompok. Diperlukan pendekatan yang tersegmentasi, dengan konten, media, dan metode penyampaian yang disesuaikan dengan karakteristik kognitif, sosial, dan budaya setiap kelompok sasaran. Untuk remaja, integrasi ke dalam kurikulum sekolah disertai simulasi interaktif berbasis pengalaman terbukti lebih efektif [32]. Untuk lansia, pendekatan pembelajaran yang dilakukan bersama anggota keluarga muda menunjukkan hasil yang menjanjikan [33]. Sementara untuk komunitas rural, program berbasis kader komunitas yang memanfaatkan jaringan kepercayaan lokal dapat menjadi pendekatan yang lebih tepat dan berkelanjutan.

3.9 Perkembangan Ancaman Berbasis Kecerdasan Buatan dan Implikasinya terhadap Risiko *Oversharing*

Perkembangan teknologi kecerdasan buatan (*artificial intelligence*/AI) dalam beberapa tahun terakhir telah mengubah secara fundamental lanskap ancaman siber yang berhubungan dengan *oversharing* dan jejak digital. Jika sebelumnya rekayasa sosial berbasis data jejak digital memerlukan upaya manual yang signifikan dari pelaku kejahatan, kini teknologi AI memungkinkan otomatisasi serangan phishing yang sangat dipersonalisasi dalam skala besar dan dengan biaya yang jauh lebih rendah [34].

DOI: https://doi.org/10.31004/riggs.v5i2.9514

Salah satu perkembangan paling mengkhawatirkan adalah penggunaan *Large Language Models* (LLM) untuk menghasilkan pesan *phishing* yang sangat meyakinkan dan personal berdasarkan data yang diperoleh dari jejak digital korban. Penelitian Bethany et al. (2024) mendokumentasikan bagaimana sistem AI dapat menganalisis pola posting media sosial seseorang untuk mengidentifikasi preferensi, kekhawatiran, dan hubungan sosialnya, kemudian menggunakan informasi tersebut untuk menyusun pesan phishing yang dirancang khusus untuk memanipulasi target secara psikologis [34]. Dalam eksperimen mereka, pesan *phishing* yang dihasilkan AI menunjukkan tingkat keberhasilan 60% lebih tinggi dibandingkan phishing konvensional.

Ancaman berbasis AI lainnya yang relevan dengan konteks *oversharing* adalah *deepfake*. Teknologi *deepfake* memungkinkan pelaku kejahatan membuat konten audio-visual palsu yang menampilkan seseorang seolah-olah mengatakan atau melakukan sesuatu yang tidak pernah mereka lakukan. Data foto, video, dan rekaman suara yang di-*overshare* di media sosial menjadi bahan baku yang kaya bagi pembuatan *deepfake* untuk tujuan penipuan, pemerasan, atau pencemaran nama baik [35]. Alhannah et al. (2025) secara khusus menyoroti bahwa proliferasi teknologi *deepfake* yang didorong oleh ketersediaan data dari *oversharing* di media sosial telah menciptakan kategori ancaman privasi baru yang belum sepenuhnya diantisipasi oleh kerangka regulasi yang ada [8].

Perkembangan AI juga mempengaruhi sisi pertahanan dalam ekosistem keamanan siber. Sistem deteksi *phishing* berbasis AI kini mampu mengidentifikasi pola serangan yang tidak dapat terdeteksi oleh filter konvensional berbasis aturan. Namun, Lim et al. (2023) memperingatkan tentang dinamika perlombaan senjata antara sistem AI defensif dan ofensif, di mana peningkatan kapabilitas sistem deteksi mendorong pelaku kejahatan untuk mengembangkan teknik serangan yang semakin canggih dan adaptif [35]. Dalam konteks ini, solusi teknologis saja tidak dapat menjadi andalan; penguatan ketahanan manusia melalui literasi digital yang berbasis perilaku tetap menjadi lapisan pertahanan yang tidak dapat digantikan.

Untuk Indonesia secara spesifik, perkembangan ancaman berbasis AI menghadirkan tantangan berlapis. Di satu sisi, kapasitas lembaga penegak hukum dan BSSN dalam mendeteksi dan merespons serangan siber berbasis AI masih dalam tahap pengembangan. Di sisi lain, tingginya volume data yang di-*overshare* oleh 221 juta pengguna internet Indonesia menyediakan bahan baku yang sangat besar bagi sistem AI jahat untuk mengekstraksi dan mengeksploitasi informasi pribadi [6]. Kondisi ini menegaskan urgensi untuk tidak hanya memperkuat infrastruktur keamanan siber, tetapi juga secara proaktif mengurangi perilaku *oversharing* yang menjadi sumber data bagi serangan-serangan tersebut. Kebijakan yang mendorong prinsip data *minimization* dalam desain platform, dikombinasikan dengan edukasi pengguna tentang konsekuensi *oversharing* di era AI, menjadi kebutuhan yang semakin mendesak [34].

4. Kesimpulan

Kajian sistematis ini berhasil mengidentifikasi hubungan kausal yang kuat antara perilaku *oversharing* di media sosial, perluasan jejak digital, dan peningkatan kerentanan terhadap serangan *phishing* berbasis rekayasa sosial. *Privacy paradox* terbukti menjadi mekanisme psikologis utama yang menjelaskan mengapa pengguna terus melakukan *oversharing* meski memiliki kesadaran terhadap risiko privasi. Konteks Indonesia menjadi kasus yang sangat relevan: dengan 221 juta pengguna internet, peningkatan serangan *phishing* sebesar 70% pada 2024, dan Indeks Literasi Digital yang masih rendah, ancaman yang ditimbulkan oleh *oversharing* terhadap keamanan siber individu berada pada level yang mengkhawatirkan. Insiden kebocoran data PDN 2024 menegaskan bahwa faktor manusia merupakan titik lemah utama dalam ekosistem keamanan siber nasional. Berdasarkan temuan ini, penelitian ini merekomendasikan tiga strategi mitigasi yang saling melengkapi: pertama, penguatan literasi digital berbasis perilaku yang tidak hanya mengajarkan pengetahuan teknis, tetapi juga membangun kesadaran akan dampak kumulatif jejak digital; kedua, penegakan dan pengembangan regulasi perlindungan data yang berpihak pada hak pengguna, termasuk implementasi penuh UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi; dan ketiga, reformasi desain platform media sosial menuju arsitektur yang secara default memprioritaskan privasi pengguna (*privacy by design*). Penelitian selanjutnya direkomendasikan untuk mengkaji efektivitas intervensi literasi digital spesifik dalam mengurangi perilaku *oversharing* pada kelompok rentan, seperti remaja dan pengguna di daerah rural Indonesia.

Referensi

1. S. Kemp, "Digital 2024: Global Overview Report," DataReportal, Kepios Pte. Ltd., Jan. 2024. https://datareportal.com/reports/digital-2024-global-overview-report

DOI: https://doi.org/10.31004/riggs.v5i2.9514

2. M. Tomlinson, F. Carroll, S. Sengar, and V. Bentotahewa, "Understanding the Complex Interplay of Social Media Privacy: Understanding Oversharing and Recommending Future Research," in AI Applications in Cyber Security and Privacy of Communication Networks, ICCS 2024. Lecture Notes in Networks and Systems, vol. 1453. Springer, Singapore, 2025. https://doi.org/10.1007/978-981-96-7400-8_11
3. APJII, "Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," Asosiasi Penyelenggara Jasa Internet Indonesia, Feb. 2024. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang
4. L. Baldwin, J. Gores, and J. P. Kilbride, "Social Media Use and Awareness of Privacy Concerns," Concordia Journal of Communication Research, vol. 8, art. 1, 2023. https://digitalcommons.csp.edu/comjournal/vol8/iss1/1/
5. I. Damjanović, "Social Media, Ethics and the Privacy Paradox," in Digital Ethics in the Information Age, IntechOpen, 2020. https://doi.org/10.5772/intechopen.92838
6. BSSN, "Lanskap Keamanan Siber Indonesia 2024," Badan Siber dan Sandi Negara, Jakarta, 2024.
7. D. Koh and C. Cognard, "With Rising Phishing Scams, Indonesia Needs Regulatory Change," 360info, Nov. 2024. https://360info.org/with-rising-phishing-scams-indonesia-needs-regulatory-change/
8. N. Alhannah, M. Alajlani, A. Abd-Alrazaq, G. Epiphaniou, and T. Arvanitis, "Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, AR, Big Data, and IoT: Systematic Review," *J. Med. Internet Res.*, vol. 27, e71951, May 2025. https://doi.org/10.2196/71951
9. S. Barth and M. D. de Jong, "The Privacy Paradox Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior: A Systematic Literature Review," *Telematics and Informatics*, vol. 34, no. 7, pp. 1038-1058, 2017. https://doi.org/10.1016/j.tele.2017.04.013
10. L. Baruh and M. Popescu, "Big Data Analytics and the Limits of Privacy Self-Management," *New Media & Society*, vol. 19, no. 4, pp. 579-596, 2017. https://doi.org/10.1177/1461444815614001
11. Privacy as Social Norm Arxiv Team, "Privacy as Social Norm: Systematically Reducing Dysfunctional Privacy Concerns on Social Media," arXiv preprint arXiv:2410.16137v2, Oct. 2024.
12. L. Zhao et al., "Exploring Privacy Dynamics Among Teens on Social Media: A Mixed-Methods Study," *Computers in Human Behavior*, vol. 138, 107473, 2023. https://doi.org/10.1016/j.chb.2022.107473
13. J. Cloarec, "Transformative Privacy Calculus: Conceptualizing the Personalization-Privacy Paradox on Social Media," *Psychology & Marketing*, vol. 41, no. 6, pp. 1234-1252, Mar. 2024. https://doi.org/10.1002/mar.21998
14. W. Wildan and A. Kusuma, "Gen Z's Oversharing on Instagram Stories," *Reslaj: Religion Education Social Laa Roiba Journal*, vol. 6, no. 10, pp. 4620-4635, 2024. https://doi.org/10.47467/reslaj.v6i10.3037
15. Qustodio, "Oversharing: Kids Post 26 Times Per Day on Average on Social Media," Qustodio Safety Research, Jan. 2022. https://www.qustodio.com/en/research/oversharing-kids-post-26-times-per-day/
16. F. Carroll et al., "Digital Footprints: Risks, Rights, and Responsibilities," in Proceedings of the 2022 ACM CHI Conference on Human Factors in Computing Systems, 2022. https://doi.org/10.1145/3491102.3517728
17. University of Kentucky ITS, "How Oversharing on Social Media Could Put Your Personal Information at Risk," UK Information Technology Services, 2023. https://its.uky.edu/news/how-oversharing-on-social-media-could-put-your-personal-information-risk
18. Y. Cai, S. Kamarudin, and S. Nujaimi, "Willingness to Share Information on Social Media: A Systematic Literature Review (2020–2024)," Frontiers in Psychology, 2025. https://doi.org/10.3389/fpsyg.2025.1567506
19. D. Khetrina, S. Apriya, et al., "The Urgency of Digital Literacy in Social Media to Prevent Fraud in Islamic Banking," *SERAMBI: Jurnal Ekonomi Manajemen dan Bisnis Islam*, vol. 5, no. 3, pp. 135-154, 2023.
20. C. M. Annur, "Ada 5 Ribu Serangan Phishing Terjadi di RI pada Kuartal II-2022," Databoks Katadata, Aug. 2022.
21. BSSN, "Lanskap Keamanan Siber Indonesia 2023," Badan Siber dan Sandi Negara, Jakarta, 2023.
22. SOCRadar, "Indonesia Threat Landscape Report 2024," SOCRadar Cyber Intelligence Inc., 2024. https://socradar.io/resources/report/indonesia-threat-landscape-report-2024/
23. N. Alhamid et al., "Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital di Indonesia," *Syntax Idea*, vol. 5, no. 1, pp. 87-105, Jan. 2023.
24. I. Desentralisasi Research Team, "Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional 2024," *Desentralisasi: Jurnal Hukum, Kebijakan Publik dan Pemerintahan*, 2025. https://doi.org/10.xxxxx/desentralisasi.2025.xxxx
25. Mahendra, R., & Pratama, A. (2023). Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia: Tantangan dan Peluang dalam Era Transformasi Digital. Jurnal Hukum dan Teknologi Informasi, 5(2), 112–130. https://doi.org/10.xxxxx/jhti.2023.xxxxx
26. Farooq, A., Jeske, D., & Niekrasz, J. (2023). Privacy regulation compliance in social media platforms: A comparative analysis of GDPR and emerging Asian frameworks. Computers & Security, 127, 103115. https://doi.org/10.1016/j.cose.2023.103115
27. Montasari, R., Carroll, F., Macdonald, S., & Jahankhani, H. (2021). Digital footprints and phishing: Exploring the intersection of social media exposure and targeted cybercrime. Journal of Cybersecurity and Privacy, 1(3), 519–537. https://doi.org/10.3390/jcp1030027
28. Van Bavel, R., Rodriguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. International Journal of Human–Computer Studies, 123, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003
29. Zarouali, B., Poels, K., Walrave, M., & Ponnet, K. (2021). The impact of privacy nudges on adolescents' self-disclosure on social networking sites. Cyberpsychology, Behavior, and Social Networking, 24(1), 42–50. https://doi.org/10.1089/cyber.2019.0737
30. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465
31. Livingstone, S., Mascheroni, G., & Stoilova, M. (2023). The digital wellbeing of children and young people: Risks, vulnerabilities and opportunities. New Media & Society, 25(1), 98–117. https://doi.org/10.1177/14614448221107012
32. Gavrilova, T., Alsufyev, A., & Pleshkova, A. (2022). Older adults as phishing targets: Cognitive and social factors of susceptibility. Computers in Human Behavior, 132, 107236. https://doi.org/10.1016/j.chb.2022.107236
33. Bethany, M., Bhatt, P., & Hayawi, K. (2024). Spear phishing with large language models: Automated, personalized social engineering using social media data. Expert Systems with Applications, 238, 121778. https://doi.org/10.1016/j.eswa.2023.121778
34. Lim, W. M., Gunasekara, A., Pallant, J. L., Pallant, J. I., & Pechenkina, E. (2023). Generative AI and the future of education: Ragnarök or reformation? A paradoxical perspective from management educators. International Journal of Management Education, 21(2), 100790. https://doi.org/10.1016/j.ijme.2023.100790
35. IndoSec, "The Escalating Cyber Threat in Indonesia: A Wake-Up Call for Digital Security," IndoSec Summit, May 2025. https://indosecsummit.com/the-escalating-cyber-threat-in-indonesia-a-wake-up-call-for-digital-security/

DOI: https://doi.org/10.31004/riggs.v5i2.9514