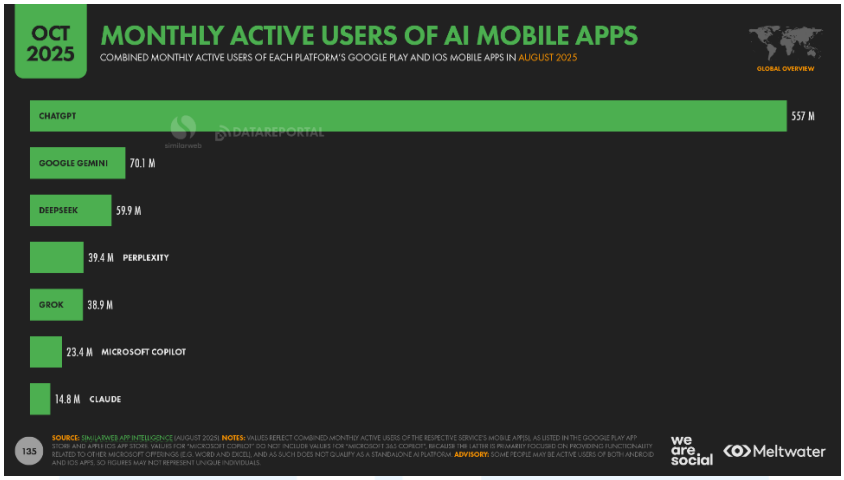
BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Transformasi digital adalah proses perubahan fundamental dalam organisasi maupun cara kerja suatu entitas (bisnis, pemerintah, masyarakat) melalui pemanfaatan teknologi digital untuk menciptakan nilai baru, mengubah proses dan meningkatkan pengalaman pemangku kepentingan (Lamarre et al., 2023). Di tengah percepatan transformasi digital, kita dihadapkan pada sebuah terobosan berupa kecerdasan buatan yang mampu menghasilkan keluaran baru. Penggunaan AI di perusahaan paling banyak umumnya dimanfaatkan untuk menyusun strategi pemasaran dan pembuatan konten sebesar 27%, manajemen pengetahuan 19%, personalisasi layanan 19%, pengembangan desain 14% dan produk serta pembuatan kode 13% seperti temuat dalam laporan AI Index Report 2025 yang disusun oleh Yolanda Gil and Raymond Perrault (2025). Hal ini umum kita kenal sebagai *generative AI* atau gen AI. Beberapa produk yang merupakan bagian dari *generative AI* antara lain seperti ChatGPT, Gemini, Deepseek, Copilot, Claude dan lain sebagainya. Penggunaan kecerdasan buatan kini telah memasuki fase adopsi massal secara global. Analisis Global Overview Report Digital 2026 yang disusun oleh Simon Kemp (2025) menunjukkan bahwa lebih dari 1 miliar pengguna aktif mengakses platform AI generatif dan LLM setiap bulannya. Bahkan, ChatGPT sendiri diperkirakan mencapai 800 juta pengguna mingguan, dengan estimasi 1 miliar pengguna bulanan, sementara platform lain seperti Gemini, DeepSeek, Perplexity, dan Claude menambah ratusan juta pengguna tambahan. Jika digabungkan dengan 250 juta pengguna AI agent di Tiongkok, maka jumlah pengguna AI global jelas berada jauh di atas angka satu miliar. Lonjakan ini didorong oleh ketersediaan aplikasi AI mobile yang sangat popular ChatGPT (557 juta MAU), Google Gemini (70,1 juta MAU), DeepSeek (59,9 juta MAU) yang mencerminkan penetrasi AI yang semakin melekat dalam aktivitas digital sehari-hari seperti pada Gambar 1,1 dibawah ini.



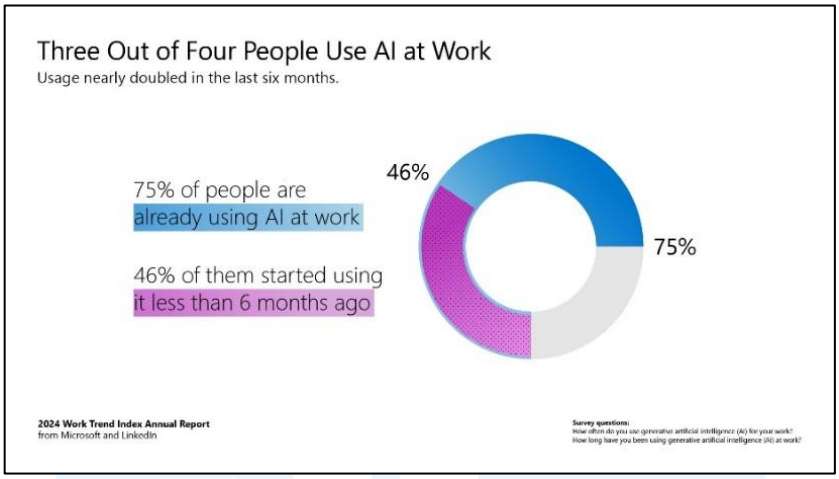
Gambar 1.1 *Monthly Active User of AI*

Sumber : Global Overview Report Digital 2026. Simon Kemp, (2025)

Penggunaan Gen AI akhir-akhir ini sudah tidak terpisahkan dengan rutinitas kerja. Laporan *Work Trend Index 2024* yang disusun oleh Microsoft and Linkedin (2024) mencatat bahwa 75% pekerja berbasis pengetahuan *(knowledge worker)* kini menggunakan Gen AI dalam pekerjaan sehari-hari, dengan 78% di antaranya membawa alat AI pribadi ketempat kerja *(Bring Your Own AI/BYOI)* tanpa sepengetahuan atau persetujuan departemen TI (Microsoft and Linkedin, 2024). Sementara data dari Cyberhaven labs Q2 *AI Adoption and Risk Report* (2024) menyatakan 73,8% penggunaan ChatGPT di tempat kerja dilakukan melalui akun pribadi *(non-corporate)* bahkan persentase lebih tinggi untuk Gemini sebesar 94,4% dan Bard 95,9%. Fenomena ini dikenal dengan istilah *Shadow AI* dimana pengguna teknologi AI secara informal, tanpa pelatihan dan di luar kendali kebijakan keamanan perusahaan (CyberHub, 2025; Puthal et al., 2025). Dalam penelitian ini, *Shadow AI Security Behaviour* didefinisikan sebagai perilaku aktual karyawan dalam menggunakan alat *Generative AI* publik (seperti ChatGPT, Gemini, Copilot) melalui akun pribadi tanpa otorisasi organisasi, yang berpotensi menimbulkan risiko keamanan siber seperti kebocoran data sensitif atau pelanggaran kebijakan perusahaan (Cyberhaven labs, 2024; Puthal et al., 2025).

Volume data perusahaan yang dimasukkan ke alat AI meningkat sebesar 485% dari Maret 2023 hingga Maret 2024, dimana 96% penggunaan AI di dominasi

oleh *"BigThree"* yaitu OpenAI, Gemini dan Copilot (Cyberhaven labs, 2024). Jenis data sensitif yang dikirimkan ke *Shadow AI*, 27.4% nya merupakan data perusahaan yang bersifat sensitif (naik dari 10.7% dari setahun sebelumnya). Jenis data sensitif teratas adalah *Customers Support* sebesar 16,73%, *Source code* sebesar 12,7%, *R&D material* sebesar 10,8% dan *Legal documents* berdasarkan temuan Cyberhaven labs (2024). Menurut sumber lainnya KPMG *Trust, attitudes and use of artificial intelligence A global study 2025,* 48% pekerja mengunggah data perusahaan termasuk informasi keuangan, pelanggan, dan strategis ke alat AI publik seperti ChatGPT (Gillespie et al., 2025). Kondisi ini semakin mengkhawtirkan karena penggunaan AI publik tanpa tata kelola *(Shadow AI)* telah diidentifikasi sebagai salah satu kontributor utama meningkatnya risiko kebocoran data dan biaya insiden keamanan, dimana laporan *IBM Cost of a Data Breach Report 2024* mencatat bahwa organisasi yang mengalami insiden akibat penggunaan AI atau shadow IT menghadapi biaya pelanggaran data yang lebih tinggi dan waktu deteksi yang lebih lama dibandingkan organisasi dengan tata kelola AI yang matang (IBM, 2024b). Menurut IBM pada *Cost of a Data Breach Report*, satu dari lima organisasi melaporkan pelanggaran keamanan akibat *Shadow AI*, dan hanya 37% yang memiliki kebijakan untuk mengelola AI atau mendeteksi *Shadow AI*. Organisasi yang menggunakan *Shadow AI* tingkat tinggi mengalami biaya pelanggaran keamanan rata-rata $670.000 lebih tinggi dari pada organisasi dengan tingkat *Shadow AI* rendah atau tanpa *Shadow AI*. Insiden keamanan yang melibatkan *Shadow AI* menyebabkan lebih banyak informasi identitas pribadi (65%) dan kekayaan intelektual (40%) yang dikompromikan dibandingkan dengan rata-rata global (masing-masing 53% dan 33%) (IBM, 2025b). Secara sektoral, Industri yang paling rentan adalah Teknologi dengan 23,6% karyawan mengirmkan data perusahaan ke AI, diikuti oleh Media dan Hiburan sebesar 7,5% dan Jasa Profesional sebesar 4,1% sementara Manufaktur dan Ritel memiliki adopsi terendah kurang dari 1%, polanya 98% data dimasukkan ke AI melalui *copy-paste* (bukan unggah file), sehingga sulit di deteksi oleh sistem keamanan berbasis file (Cyberhaven labs, 2024)

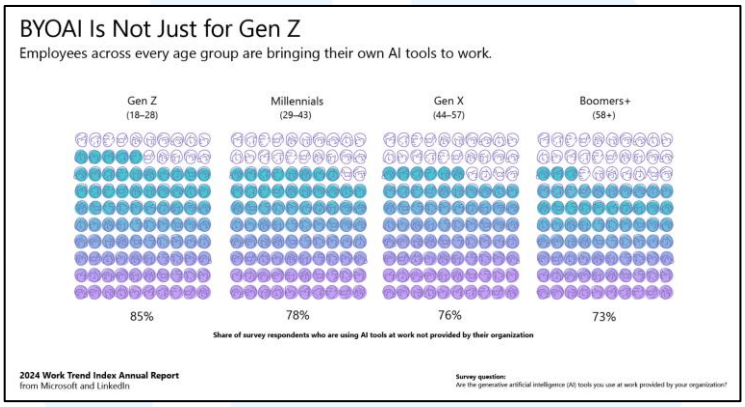


Gambar 1.2 Proporsi pengguna AI di tempat kerja tahun 2024

Sumber : Microsoft and Linkedin (2024)

Gambar 1.2 menunjukkan data dari *Work Trend Index 2024* yang dilaporkan oleh Microsoft and Linkedin (2024) yang mana 3 dari 4 orang karyawan telah menggunakan AI dalam pekerjaannya. Tingginya tingkat adopsi ini menunjukkan bahwa penggunaan AI generatif telah menjadi praktik arus utama *(mainstream)* dalam dunia kerja modern, sejalan dengan temuan (Salesforce, 2025) yang melaporkan bahwa 61% pekerja global telah menggunakan atau berencana menggunakan AI generatif dalam aktivitas professional mereka. Fakta ini memperlihatkan bahwa penggunaan AI bukan lagi bersifat eksperimental, melainkan telah terintegrasi dalam praktik kerja sehari-hari. Lebih lanjut, fenomena tersebut tidak hanya terjadi pada generasi Z, tetapi juga meluas pada seluruh kelompok usia, mulai dari Gen Z hingga Boomers. Gambar 1.3 dari Microsoft and Linkedin (2024) dibawah ini memperlihatkan bagaimana fenomena *Bring Your Own AI* (BYOI) ini telah terjadi di semua segmen usia dalam dunia kerja, dan semakin memperbesar terjadinya *Shadow AI*. 85% Gen Z, 78% Millennials, 76% Gen X, dan bahkan 73% Boomers+ menggunakan alat AI di tempat kerja yang tidak disediakan oleh organisasi mereka. Temuan ini menegaskan bahwa *Shadow AI* bukanlah isu generasi, melainkan fenomena lintas usia yang dipicu oleh dorongan produktivitas dan kemudahan akses terhadap AI publik. Studi Lee et al (2025) juga menunjukkan bahwa pengguna AI tetap memanfaatkan AI publik meskipun

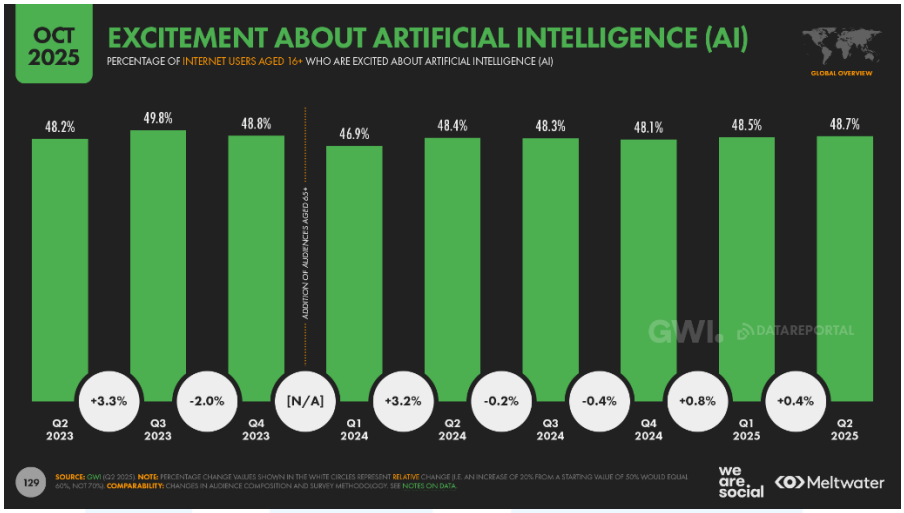
menyadari risiko privasi, selama mereka merasa memiliki strategi adaptif atau kontrol terhadap penggunaannya. Dengan kata lain, preferensi menggunakan akun atau aplikasi AI pribadi terjadi di semua kelompok karyawan, sehingga risiko keamanan siber dari *Shadow AI* menjadi tantangan organisasi secara menyeluruh, bukan hanya dari generasi tertentu saja.



Gambar 1.3 BYOI dalam setiap grup usia tahun 2024

Sumber : Microsoft and Linkedin (2024)

Survei GWI tahun 2025 yang tertuang pada Global Overview Report Digital 2026 yang disusun oleh Simon Kemp (2025) menunjukkan bahwa hampir 50% pengguna internet berusia 16 tahun ke atas merasa *"excited"* terhadap AI yang termuat dalam gambar 1.4, sebuah indikator bahwa adopsi AI kemungkinan akan terus meningkat secara eksponensial. Tren ini mengisyaratkan bahwa penggunaan AI di lingkungan kerja, termasuk praktik *Bring Your Own AI (*BYOI) dan *Shadow AI*, akan semakin meluas karena dorongan eksplorasi dan kenyamanan pengguna terhadap teknologi tersebut.



Gambar 1.4 *Excitement about AI*

Sumber : Global Overview Report Digital 2026. Simon Kemp (2025)

Shadow AI lahir dari kesenjangan antara kebutuhan produktivitas individu dan kesiapan organisasi. Di satu sisi, karyawan menghadapi tekanan kerja yang tinggi, 68% merasa kewalahan oleh volume dan kecepatan pekerjaan dan 46% mengalami kelelahan mental (Microsoft and Linkedin, 2024). Perkembangan *generative AI* dalam beberapa tahun terakhir semakin memperkuat dinamika ini, karena teknologi tersebut mampu membantu pengguna menghasilkan konten, melakukan analisis, serta mengotomasi berbagai tugas pekerjaan secara cepat sehingga menjadi alat yang menarik bagi karyawan untuk meningkatkan produktivitas kerja (Naqbi et al., 2024). Di sisi lain lebih dari 20% pekerja global mengaku nyaris tidak mendapat dukungan atau pelatihan AI dari organisasi mereka (Mayer et al., 2025) dan hanya 39% yang menerima pelatihan AI dari perusahaan (Microsoft and Linkedin, 2024). Literatur tentang adopsi AI di organisasi menunjukkan bahwa kurangnya dukungan organisasi, termasuk pelatihan, kebijakan penggunaan teknologi, serta kesiapan infrastruktur digital, dapat mendorong karyawan untuk mengadopsi teknologi AI secara mandiri di luar kerangka tata kelola organisasi (Bankins et al., 2023). Akibatnya, karyawan mengambil inisiatif sendiri untuk menggunakan alat AI publik/akses pribadi untuk menyelesaikan tugas meskipun menyadari akan risiko yang mungkin dihadapi. Fenomena ini menggambarkan praktik penggunaan AI secara informal atau tidak

terkelola dalam organisasi, yang sering disebut sebagai Shadow AI, yaitu penggunaan teknologi AI oleh individu tanpa pengawasan atau regulasi formal dari organisasi (Combetto, 2026).

Penelitian Salesforce (2025) dalam *Generative AI statistiks* mengungkap bahwa pekerja memiliki dua sisi pandangan terhadap AI generatif. Di satu sisi, mereka melihat manfaat dari AI generatif, tetapi di sisi lain, mereka juga khawatir dalam mengelola risikonya dan mempelajari keterampilan yang dibutuhkan untuk memanfaatkan sepenuhnya teknologi yang berkembang pesat ini. Fenomena ambivalensi ini juga dikonfirmasi oleh laporan *McKinsey, The state of AI in 2023: Generative AI's breakout year* yang menunjukkan bahwa meskipun organisasi mengalami peningkatan produktivitas dan efisiensi melalui AI generatif, mayoritas responden tetap mengindentifikasi risiko signifikan terkait keamanan data, akurasi output serta tata kelola penggunaan AI di lingkungan kerja (McKinsey & Company, 2023). Tiga dari lima pekerja (61%) saat ini menggunakan atau berencana menggunakan AI generatif. Lebih dari dua per tiga pekerja (68%) menyatakan bahwa AI generatif akan membantu mereka melayani pelanggan dengan lebih baik. Dua per tiga pekerja (67%) mengatakan AI generatif akan membantu mereka mendapatkan lebih banyak manfaat dari investasi teknologi lainnya, seperti model AI dan machine learning lainnya (Salesforce, 2025). Namun, banyak pekerja yang belum tahu bagaimana menggunakan AI generatif secara bertanggung jawab. Separuh dari pekerja yang disurvei (54%) menyatakan mereka khawatir hasil output AI generatif tidak akurat, dan 59% khawatir output-nya mengandung bias, hampir tiga perempat responden (73%) meyakini bahwa AI generatif menimbulkan risiko keamanan baru, dari mereka yang menyatakan berencana menggunakan AI generatif, hampir 60% mengaku tidak tahu cara melakukannya dengan menggunakan sumber data tepercaya atau sambil memastikan data sensitif tetap aman (Salesforce, 2025). Kekhwatiran serupa juga tercermin dalam laporan *IBM AI in Action 2024*, yang menegaskan bahwa isu utama dalam adopsi AI di perusahaan bukan lagi sekedar kesiapan teknologi, melainkan governance, keamanan data dan kesiapan keterampilan karyawan dalam mengelola risiko AI secara etis dan tanggung jawab (IBM, 2024a).

Disisi lain, secara umum kondisi ini sepertinya terjadi juga di Indonesia, karena didukung faktor tingkat literasi dan keterampilan digital masyarakat meningkat, menurut data Goodstat (2025) dari Kementerian Komdigi tentang IMDI (Indeks Masyarakat Digital Indonesia) tahun 2024 mencapai skor 43,34. Angka ini menunjukkan kenaikan sejak 2022 lalu. Dari empat pilar penilaian, pilar keterampilan digital memperoleh skor paling tinggi, yaitu 58,25. Pada 2022, skor IMDI mencapai 37,80. Kemudian, nilainya naik pada 2023, menjadi 43,18. Meskipun demikian, hanya pilar keterampilan digital yang konsisten naik. Dalam konteks perkembangan *generative AI*, peningkatan literasi digital ini juga mempercepat adopsi teknologi AI oleh individu di tempat kerja, bahkan sebelum organisasi memiliki kebijakan dan tata kelola yang matang dalam mengatur penggunaannya (Budhwar et al., 2023).

Indonesia khususnya kawasan Jabodetabek, merupakan pusat ekosistem perusahaan digital terbesar di Asia Tenggara. Pada tahun 2024 ditulis pada salah satu artikel milik Kompas mengutip data dari AWS, lebih dari 5,9 juta bisnis di Indonesia telah mengadopsi teknologi kecerdasan buatan (AI), setara dengan 10 bisnis baru per menit (Kompas, 2025b). Posisi Indonesia sebagai motor utama ekonomi digital Kawasan juga ditegaskan dalam laporan *e-Conomy SEA 2024* yang menyebutkan bahwa nilai GMV ekonomi digital Asia Tenggara mencapai USD 263 miliar pada 2024, dengan Indonesia sebagai kontributor terbesar di kawasan tersebut (Google, Temasek, 2024). Laporan yang sama juga menegaskan bahwa Asia Tenggara mengalami pertumbuhan dua digit secara konsisten dalam GMV dan revenue digital selama tiga tahun terakhir, didorong oleh sector e-commerce, transportasi, online media dan layanan digital lainnya (Google, Temasek, 2024). Kondisi ini menunjukkan bahwa perusahaan di Indonesia khususnya di kawasan Jabodetabek menjadi episentrum pertumbuhan ini karena konsentrasi tinggi perusahaan rintisan *(startup)*, perusahaan teknologi, layanan keuangan digital *(fintech)*, *e-commerce*, *edutech*, transportasi online *(ride hailing)* dan konsultan digital yang beroperasi dalam ekosistem yang sangat dinamis dan kompetitif, dengan intensitas penggunaan teknologi digital dan AI yang tinggi (Statista, 2024a). Dalam konteks organisasi modern, integrasi kecerdasan buatan dan sistem berbasis

data telah menjadi komponen penting dalam transformasi operasional perusahaan digital karena teknologi tersebut memungkinkan otomatisasi proses kerja, analisis data berskala besar, serta pengambilan keputusan berbasis algoritma yang meningkatkan efisiensi organisasi (Bankins et al., 2023). Selain itu, perkembangan *generative AI* berbasis *Large Language Models (LLM)* semakin mempercepat penggunaan AI dalam aktivitas kerja sehari-hari seperti pada pembuatan konten, analisis informasi, pemrograman, serta dukungan pengambilan keputusan, sehingga memperluas adopsi AI di berbagai sektor bisnis digital (Naqbi et al., 2024). Dalam lingkungan kerja yang sangat terdigitalisasi tersebut, peluang untuk terjadinya *Shadow AI* sangatlah besar untuk perusahaan yang mengandalkan jaringan digital untuk sebagian besar atau seluruh proses dan bisnisnya, termasuk interaksi dengan pelanggan, pemasok, dan karyawan, serta operasional internal. Fenomena ini semakin penting karena penerapan AI dalam organisasi tidak hanya menjadikan produktivitas lebih baik, tetapi juga merubah cara karyawan berinteraksi dengan teknologi, yang pada akhirnya dapat mendorong penggunaan AI secara mandiri di luar sistem resmi organisasi. (Budhwar et al., 2023).

Menurut laporan di Indonesia AI Report 2025 oleh Kumparan (2025), penggunaan AI yang ditujukan untuk membantu pekerjaan/tugas di Indonesia adalah sebesar 68% selain pada kebutuhan harian lainnya, yang mana 83% nya didominasi oleh penggunaan Chatbot AI generatif seperti (Copilot, Gemini, ChatGPT, Claude dll). Wilayah Jabodetabek merupakan kawasan dengan penyumbang 50% responden survey yang dilakukan dan di muat dalam Indonesia AI Report 2025 disusul oleh Surabaya 20%, Medan 10% dan beberapa kota lainnya, dimana para responden dominan atau sebesar 45% berstatus karyawan swasta dan paling teratas sebesar 14% bekerja di Teknologi/IT, disusul 13% bekerja di *Retail/Commerce*. Jika dilihat dari industri, setiap industri menunjukkan karakter yang berbeda. Sektor Digital dan Media menunjukkan sikap paling progresif, dengan persentase tertinggi yaitu 55%. Hal ini mengindikasikan karakteristik bidang industri yang sangat kompetitif dan akrab dengan teknologi. Sementara sektor *Commerce & Consumers Services* di angka 37% yang menunjukkan bahwa industri ini masih dalam fase mengevaluasi penerapan teknologi AI untuk kegiatan

perusahaan (Kumparan, 2025). Secara umum, adopsi chatbot AI generatif dalam pekerjaan sudah cukup luas dan cenderung tidak terhindarkan. Hal ini terlihat dari 57% publik yang sudah menggunakan chatbot AI generatif, baik itu ada atau tidaknya dukungan organisasi pada penggunaan AI dalam pekerjaan. Untuk kondisi yang kurang mendapat dukungan organisasi melalui penyediaan alat bantu AI generatif resmi perusahaan ini lah yang berpotensi menimbulkan *Shadow AI* (Kumparan, 2025). Perusahaan digital secara umum dapat didefinisikan sebagai organisasi yang mengintergrasikan teknologi digital ke dalam model bisnis, proses operasional serta penciptaan nilai bagi pelanggan melalui platform, data dan ekosistem berbasis teknologi (OECD, 2023; Verhoef et al., 2021). Transformasi menuju perusahaan digital tidak hanya melibatkan adopsi teknologi informasi, tetapi juga perubahan mendasar dalam struktur organisasi, proses bisnis, serta mekanisme penciptaan nilai perusahaan. *Digitalization* mendorong organisasi untuk mengintegrasikan teknologi digital ke dalam strategi bisnis, operasi, dan model bisnis sehingga mengubah cara perusahaan beroperasi dan bersaing di lingkungan bisnis yang semakin berbasis data dan teknologi (Calderon et al., 2024). Dalam konteks ini, perusahaan digital tidak hanya memanfaatkan internet dan perangkat lunak sebagai alat bantu, akan tetapi juga menjadikan teknologi digital sebagai inti dari proporsi nilai, strategi pertumbuhan serta mekanisme interaksi dengan pelanggan dan mitra bisnis. OECD (2023) dalam *Digital Education Outlook* menegaskan bahwa perusahaan digital beroperasi dalam ekosistem berbasis data dan platform, dimana konektivitas, *cloud computing* serta integrasi AI menjadi pendorong utama produktivitas dan inovasi. Industri digital Indonesia berkembang sangat pesat mulai dari telekomunikasi, *startup, media digital, fintech* hingga *e-commerce*, namun menghadapi tantangan di akses, keamanan, dan pengembangan talenta digital. Laporan *e-Conomy SEA 2024* menunjukkan bahwa Indonesia merupakan kontributor terbesar ekonomi digital Asia Tenggara dengan pertumbuhan yang konsisten dalam sektor e-commence, transportasi digital, dan layanan online berbasis platform (Google, Temasek, 2024).

Ekosistem startup tumbuh pesat berkat pendanaan ventura yang meningkat, dari 3,92 miliar USD di 2016 menjadi 22 miliar USD di 2022. Jakarta menjadi pusat

utama lebih dari 500 startup, namun perkembangan juga terjadi di Bandung, Yogyakarta, dan Denpasar (Statista, 2024b). Saat ini Indonesia memiliki delapan unicorn dan dua decacorn (GoTo Group dan J&T Express). Startup seperti Gojek, Tokopedia, Bukalapak, dan Traveloka menjadi pelopor, didorong oleh kebutuhan layanan digital, pembayaran daring, logistik, dan transportasi online (Statista, 2024b). Dengan tingkat penetrasi internet yang tinggi serta percepatan adopsi AI generatif di sektor korporasi, perusahaan digital Indonesia beroperasi dalam lingkungan yang sangat terdigitalisasi dan berbasis data, sehingga aspek tata kelola keamanan siber menjadi faktor krusial untuk memastikan keberlanjutan pertumbuhan tersebut (Google, Temasek, 2024; OECD, 2023).

Menurut Amazon (2025), 87% perusahaan di Indonesia melaporkan percepatan adopsi AI generatif dalam 12 bulan terakhir, dengan Jabodetabek sebagai wilayah dengan penetrasi tertinggi. Namun, hanya 31% perusahaan yang memiliki kebijakan formal atau kerangka tata kelola AI yang jelas. Kesenjangan antara kecepatan adopsi dan kematangan tata kelola menciptakan lingkungan ideal bagi munculnya *Shadow AI* penggunaan alat AI generatif oleh karyawan tanpa izin, pelatihan, atau pengawasan TI (CyberHub, 2025; IBM, 2025). Berdasarkan dokumen survey *The Ipsos AI Monitor 2024* yang dimuat oleh Ipsos menemukan 54% responden global merasa *"excited"* terhadap produk dan layanan berbasis AI, namun 52% juga merasa *"nervous"* karena AI membuat mereka cemas, di Indonesia persentase yang merasa *"nervous"* lebih tinggi (62%) dibanding rata-rata global, sementara yang merasa *"excited"* juga tinggi (78%) (Carmichael, 2024). Secara ideal, perusahaan digital mengharapkan kepatuhan penuh terhadap kebijakan keamanan TI serta penggunaan AI melalui platform resmi yang aman. Namun, realitas menunjukkan adanya kesenjangan signifikan: mayoritas karyawan menggunakan AI publik melalui akun pribadi, mengunggah data internal secara tidak sadar, serta menyembunyikan penggunaan AI dari organisasi. Gap ini menciptakan risiko kebocoran data, hilangnya kontrol, dan kegagalan tata kelola AI. Temuan ini memperkuat bahwa penggunaan AI generatif di tempat kerja tidak hanya dipengaruhi oleh persepsi manfaat, tetapi juga oleh persepsi ancaman dan

kemampuan individu dalam mengelola risiko, yang secara konseptual sejalan dengan kerangka *Protection Motivation Theory (PMT).*

Idealnya sebuah perusahaan mengharapkan adanya kepatuhan penuh dari para pekerja terhadap kebijakan keamanan TI, terutama dalam menangani data sensitif. Namun, realitas yang terjadi justru menunjukkan adanya gap kinerja keamanan siber yang cukup signifikan. Transformasi digital dan adopsi teknologi *Artificial Intelligence (AI)* dalam organisasi telah mengubah cara karyawan bekerja, termasuk meningkatnya interaksi antara manusia dan sistem AI dalam menyelesaikan berbagai tugas pekerjaan (Bankins et al., 2023). Perubahan ini di satu sisi meningkatkan efisiensi kerja, namun di sisi lain juga memperluas potensi risiko keamanan informasi apabila penggunaan teknologi tersebut tidak diikuti dengan tata kelola yang memadai (Budhwar et al., 2023). Menurut data pada Laporan Microsoft Work Trend (2024), terdapat 52% pengguna AI enggan mengakui penggunaan AI untuk menyelesaikan tugas penting, karena mereka takut AI dianggap dapat menggantikan manusia ataupun karena hal tersebut melanggar aturan perusahaan. Fenomena ini sejalan dengan literatur yang menunjukkan bahwa penggunaan *generative AI* dalam pekerjaan sering kali terjadi secara informal dan tidak selalu berada di bawah pengawasan organisasi, terutama ketika teknologi tersebut mudah diakses oleh individu melalui berbagai platform publik (Combetto, 2026). Kebocoran data menjadi ancaman utama dimana ketika karyawan tanpa sadar mengunggah dokumen interal ke platform publik, hal ini sangat berpotensi membocorkan laporan keuangan, strategi bisnis atau data pelanggan (Kompas, 2025a ; CyberHub, 2025). Selain itu, kontrol organisasi yang hilang menjadi kondisi realitas selanjutnya, keadaan dimana manajemen tidak tahu sejauh mana, untuk apa, dan dengan risiko apa AI digunakan sehingga sulit mengukur dampak atau merancang strategi mitigasi (Puthal et al., 2025). Gap ini diperparah oleh kebingungan karyawan melalui tahun 2024 oleh Cyberhaven labs (2024) menemukan sekitar 77% karyawan masih bingung bagaimana mengintegrasikan AI ke dalam karier mereka. Bukan karena enggan, melainkan karena tidak tahu apakah penggunaan AI diperbolehkan dan seberapa batasannya. Bukan karena menolak keamanan, tetapi karena tidak ada kejelasan dari pimpinan.

Sejumlah faktor dapat menjelaskan bagaimana pertumbuhan *Shadow AI* yang pesat. Pertama, adanya kebijakan yang bersifat *enabling* serta ketersediaan luas alat *generative AI* untuk publik mendorong adopsi yang cepat di lingkungan kerja. Standarisasi teknologi AI melalui *Open API, model foundation* serta ekosistem *platform cloud* mempercepat integrasi AI ke dalam proses bisnis tanpa memerlukan infrastruktur internal yang kompleks. Laporan McKinsey & Company, (2023) dalam *The State of AI* menegaskan bahwa kemudahan akses terhadap model *generative AI* melalui API dan layanan cloud telah menurunkan hambatan adopsi secara signifikan di berbagai fungsi organisasi. Hal ini diperkuat oleh temuan GoogleCloud (2024) yang menunjukkan bahwa platform AI berbasis *cloud* dan model *pre-trained* memungkinkan implementasi AI dalam hitungan minggu, bukan bulan sehingga mempercepat eksperimen mandiri di tingkat individu maupun tim. Melalui kehadiran *platform low-code* dan *no-code* hambatan teknis untuk mengembangkan solusi AI semakin berkurang, memungkinkan staf non teknis untuk menguji dan menerapkan AI ke dalam alur kerja mereka tanpa harus melalui pengawasan formal departemen TI. Begitu juga layanan AI berbasis *cloud (cloud-based)* dan *framework machine learning open-source* seperti *PyTorch* dan *TensorFlow* memungkinkan siapa pun untuk merancang dan mengimplementasikan solusi AI dengan cepat, tetapi sering kali di luar kerangka tata kelola *(governance)* organisasi. Faktor lain yang mempercepat pertumbuhan *Shadow AI* adalah dorongan inovasi individu *(innovation-driven behaviour)*. Banyak karyawan yang memiliki motivasi kuat untuk meningkatkan kinerja, produktivitas dan efisiensi kerja melalui otomatisasi berbasis AI. Studi oleh Salesforce (2025) menunjukkan bahwa 61% pekerja telah menggunakan atau berencana menggunakan *generative AI* untuk meningkatkan produktivitas kerja. Sementara itu, penelitian oleh (Lee et al., 2025) menemukan bahwa pengguna *generative AI* cenderung terus memanfaatkan teknologi tersebut meskipun menyadari adanya risiko privasi, terutama ketika mereka menilai manfaatnya lebih besar dibanding potensi ancaman. Dorongan inovasi dan peningkatan kinerja ini dapat berkembang menjadi apa yang disebut sebagai *Shadow Volition, Shadow Volition,* yaitu kemauan tersembunyi untuk menggunakan teknologi di luar

kebijakan organisasi demi mencapai efisiensi, yang pada akhirnya berkontribusi pada munculnya *Shadow AI* ketika tidak diimbangi dengan kebijakan dan kontrol keamanan yang memadai (Puthal et al., 2025).

Beberapa contoh kerentanan yang muncul akibat praktik *Shadow AI* dapat dilihat secara sistematis pada gambar 1.5 oleh Puthal et al (2025) yang mengklasifikasikan taksonomi serangan terhadap *Shadow AI* mulai dari *data integrity attacks, privacy attacks* hingga *regulatory and compliance risks.* Salah satu kerentanan utama adalah *unsecured API endpoints,* yaitu penggunaan API untuk mentransfer data tanpa mekanisme autentikasi dan enkripsi yang memadai. *Endpoint* yang tidak diamankan memungkinkan penyerang melakukan injeksi kode berbahaya, eksploitasi, eksploitasi permintaan tidak sah, serta pencurian data sensitif. Risiko ini sejalan dengan laporan OWASP (2023) API Security Top 10, yang menempatkan *broken authentication* dan *broken object level authorization* sebagai ancaman utama dalam sistem berbasis API, termasuk layanan AI berbasis *cloud*. Selain itu, seperti yang dipublikasikan oleh Nist (2023) melalui *Artificial Intelligence Risk Management Framework* menegaskan bahwa integrasi model AI melalui API eksternal tanpa kontrol validasi input dan monitoring berkelanjutan meningkatkan risiko manipulasi data dan *adversarial exploitation*. Kerentanan lain adalah o*verprivileaged access,* yaitu pemberian hak akses berlebihan pada sistem atau akun yang menggunakan AI, yang berpotensi memicu eskalasi hak akses dan kebocoran data. IBM (2024b) menunjukkan bahwa penyalahgunaan kredensial menjadi penyebab utama pelanggaran data global. Selain itu, *insecure third party integrations* pada layanan SaaS meningkatkan risiko kebocoran lintas platform, sebagaimana dicatat dalam The European Union Agency for Cybersecurity (ENISA) (2024), kondisi saat beberapa alat *Shadow AI* memerlukan *interface* (tampilan antarmuka) dengan aplikasi pihak ketiga atau bahkan sistem SaaS. Temuan ini memperkuat bahwa *Shadow AI* tidak hanya berisiko teknis tetapi juga berdampak pada kepatuhan dan tata kelola organisasi (Puthal et al., 2025).

Table 1 Taxonomy of attacks on shadow AI

Category	Attack Type	Impact	Vulnerability
Data Integrity Attacks	Data Poisoning	Model produces incorrect predictions	Lack of data validation in Shadow AI
	Adversarial Attacks	AI misclassifies malicious inputs	Weak adversarial robustness
Privacy Attacks	Model Inversion	Extraction of sensitive training data	Lack of encryption in AI deployment
	Membership Inference	Determining if data was used for training	Shadow AI model lacks privacy safeguards
Evasion Attacks	Input Manipulation	Bypassing AI-based security defenses	Lack of secure input validation
Access Exploits	Unauthorized API Usage	Uncontrolled AI model interactions	Shadow AI models calling unprotected APIs
	Privilege Escalation	Gaining unauthorized access to AI features	Lack of authentication in Shadow AI
Regulatory and Compliance Risks	Data Exfiltration	Leakage of sensitive business data	AI tools transferring data to external servers
	Compliance Violation	Legal consequences and penalties	Shadow AI bypassing security policies

Gambar 1.5 Taksonomi serangan pada *Shadow AI*

Sumber : Puthal et al., (2025)

Di banyak organisasi, karyawan dan departemen berada di bawah tekanan seperti tenggat waktu yang ketat dan persaingan. Jika departemen IT tidak mampu memenuhi ekspektasi ini karena kekurangan sumber daya manusia atau karena politik internal, karyawan tidak memiliki pilihan lain selain mencari alat AI yang tersedia. Dalam kondisi tersebut, ketika departemen IT tidak mampu memenuhi ekspektasi akibat keterbatasan sumber daya atau proses birokrasi internal, karyawan cenderung mengambil inisiatif sendiri dengan memanfaatkan alat AI publik yang mudah diakses. Kondisi tersebut semakin diperkuat oleh ketersediaan berbagai platform *generative AI* yang mudah diakses secara publik dan mampu membantu pengguna dalam menghasilkan konten, melakukan analisis, serta mengotomasi berbagai tugas pekerjaan secara cepat (Naqbi et al., 2024). Namun, tentunya fleksibilitas ini hadir dengan konsekuensi yang harus diterima seperti hilangnya kontrol karena teknologi-teknologi ini sering kali diadopsi tanpa panduan yang memadai, yang mengakibatkan risiko (Puthal et al., 2025). Selain itu, penggunaan AI yang tidak terkelola dengan baik juga dapat memperluas potensi ancaman keamanan siber, termasuk risiko kebocoran data, manipulasi informasi, serta penyalahgunaan teknologi digital yang dihasilkan melalui sistem AI generatif (Schmitt & Koutroumpis, 2025).

Berdasarkan fenomena tersebut, terlihat bahwa perilaku *Shadow AI (Shadow AI Security Behaviour)* dipengaruhi oleh tiga faktor utama. Pertama, tingkat *cybersecurity awareness* yang rendah membuat karyawan tidak memahami batas aman penggunaan AI publik dan implikasi kebocoran data. Hal ini konsisten

dengan temuan (Li et al., 2022) yang menunjukkan bahwa kesadaran keamanan siber berperan signifikan dalam membentuk persepsi ancaman dan respons individu terhadap risiko teknologi. Kedua, dukungan organisasi yang tidak memadai, seperti minimnya pelatihan dan ketiadaan kebijakan AI formal, mendorong karyawan mencari solusi sendiri. Studi terbaru oleh Gillespie et al., (2025) yang tertuang dalam global study KPMG berjudul *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025* menegaskan bahwa kurangnya kerangka tata kelola dan pelatihan AI meningkatkan kemungkinan penggunaan AI di luar kebijakan resmi perusahaan. Penelitian mengenai implementasi AI di organisasi menunjukkan bahwa keberhasilan penggunaan AI sangat dipengaruhi oleh dukungan organisasi, termasuk kesiapan teknologi, kebijakan tata kelola, serta dukungan manajemen dalam memfasilitasi penggunaan teknologi secara bertanggung jawab (Bankins et al., 2023). Ketiga, literasi AI yang belum matang menciptakan ilusi kompetensi yang membuat karyawan merasa aman menggunakan AI publik tanpa mempertimbangkan risiko keamanan secara menyeluruh. Temuan serupa juga diidentifikasi dalam penelitian Tran et al (2025), yang menyatakan bahwa tingkat literasi dan persepsi kemampuan diri memengaruhi cara individu menilai efektivitas dan risiko penggunaan AI. Ketiga faktor ini membentuk dasar penyusunan variabel independen penelitian.

Fenomena kebocoran data yang dipicu oleh praktik *Shadow AI* tidak lagi sekadar bersifat teoretis, melainkan telah terdokumentasi dalam lanskap ancaman siber terkini. Laporan *ENISA Threat Landscape 2025 Part 2* mengonfirmasi bahwa peningkatan penggunaan alat kecerdasan buatan generatif yang tidak terkelola *(unmanaged/unauthorised AI tools)* oleh karyawan secara signifikan memperbesar vektor eksfiltrasi data sensitif. Organisasi di berbagai sektor melaporkan insiden terpaparnya kode sumber, dokumen hukum, dan data pelanggan ke platform AI publik, yang terjadi akibat pemrosesan informasi di luar lingkungan korporat yang terlindungi (The European Union Agency for Cybersecurity (ENISA), 2025). Meskipun ENISA belum mengklasifikasikan *Shadow AI* sebagai kategori ancaman yang berdiri sendiri, laporan tersebut menegaskan bahwa praktik ini secara nyata memperkuat vektor data breach yang sudah ada dengan cara menghindari

mekanisme keamanan tradisional seperti *Data Loss Prevention (DLP)* dan pengawasan TI terpusat. Lebih lanjut, ENISA mencatat bahwa sebagian besar insiden ini tidak bermotif jahat, melainkan muncul dari kebutuhan produktivitas operasional yang tidak diiringi dengan kerangka tata kelola AI yang matang, sehingga menciptakan celah keamanan sistemik. Temuan ini memperkuat urgensi penelitian ini, mengingat kebocoran data akibat *Shadow AI* lebih banyak didorong oleh perilaku adaptif sukarela *(voluntary maladaptive behaviour)* ketimbang serangan siber terstruktur, sehingga memerlukan pendekatan pemahaman mekanisme kognitif karyawan di tingkat individu.

Meskipun fenomena *Shadow AI* ini telah diidentifikasi sebagai risiko keamanan siber utama (Balogun et al., 2025; Puthal et al., 2025) tetapi penelitian empiris yang menjelaskan mengapa karyawan tetap menggunakannya walaupun mereka mengetahui risikonya, penelitian seperti ini masih sangat terbatas. Sebagian besar studi atau penelitian tentang keamanan siber lebih berfokus pada perilaku kepatuhan *(compliance)* dalam konteks *mandatory behaviour,* bukan pada suatu sikap prilaku sukarela yang melanggar kebijakan organisasi seperti pada *Shadow AI* (Li et al., 2022). Menurut Sommestad et al., (2015) dalam jurnal *A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour* menyatakan bahwa *Protection Motivation Theory* (PMT) paling kuat menjelaskan perilaku keamanan ketika perilaku bersifat sukarela dimana *Shadow AI* sukarela dilakukan dan secara tersembunyi, lalu ancaman dan respon yang spesifik dan konkret karena dengan *Shadow AI* dapat menimbulkan kebocoran data spesifik dan yang terakhir ancaman dapat mengenai individu secara langsung pada konteks ini *Shadow AI* dapat berakibat pada risiko PHK, reputasi dan denda pribadi. *Shadow AI* memenuhi ketiga kriteria tersebut namun, belum ada penelitian yang menjelaskan mekanisme kognitif di balik keputusan karyawan untuk tetap menggunakannya meskipun mereka menyadari risiko kebocoran data dan pelanggaran kebijakan. *Protection Motivation Theory (PMT)* yang terbukti kuat belum diterapkan untuk *maladaptive behaviour* seperti *Shadow AI* khususnya di Indonesia. Selain itu, peran faktor kontekstual seperti *cybersecurity awareness*, dukungan organisasi dan *AI literacy* sebagai anteseden persepsi *Protection*

Motivation Theory (PMT) dalam konteks ini masih belum dieksplorasi secara empiris. Penelitian ini bertujuan mengisi kesenjangan tersebut dengan menguji model berbasis PMT yang diperluas untuk memahami bagaimana persepsi kognitif membentuk niat dan perilaku *Shadow AI* di kalangan karyawan perusahaan digital.

Beberapa penelitian terkini telah meletakkan fondasi penting seperti menujukkan bahwa *organizational support* dan *cybersecurity awareness* memengaruhi persepsi *Protection Motivation Theory (PMT)* yang pada gilirannya membentuk perilaku keamanan siber (Li et al., 2022). Lalu penelitian yang dilakukan oleh Kiran et al., (2025) membuktikan bahwa *coping appraisal (self-efficacy, response efficacy)* lebih kuat memprediksi perilaku keamanan dari pada *threat appraisal.* Sementara menurut Lee et al., (2025) bahwa pengguna Gen AI tidak serta merta berhenti menggunakan AI meski menyadari risiko privasi, selama mereka memiliki strategi yang adaptif seperti melakukan verifikasi output yang dihasilkan. Namun, tidak ada yang secara langsung menghubungkan faktor kontekstual seperti *cybersecurity awareness*, dukungan organisasi dan *AI literacy* terhadap proses kognitif *Protection Motivation Theory (PMT)* membentuk niat dan perilaku penggunaan *Shadow AI*.

Dalam beberapa tahun terakhir, kerangka *Protection Motivation Theory (PMT)* terus divalidasi dan diadaptasi untuk menjawab kompleksitas perilaku keamanan siber di era transformasi digital. Studi meta-analisis terkini mengonfirmasi bahwa PMT tetap menjadi kerangka prediktif yang *robust* dengan *effect size* moderat hingga besar dalam menjelaskan niat dan perilaku protektif pengguna teknologi (Jan et al., 2023). Relevansi teoretis ini semakin diperkuat oleh sejumlah penelitian empiris periode 2023–2025 yang mengintegrasikan PMT ke dalam konteks teknologi spesifik, seperti perilaku keamanan perangkat pintar konsumen (Karayel & Saygılı, 2025), kepatuhan kebijakan keamanan di sektor perbankan sensitif (Alrawhani et al., 2025), serta validasi jalur kognitif *awareness–intention–behaviour* pada ekosistem digital Asia (Tran et al., 2025). Lebih lanjut, penelitian mutakhir memperluas aplikabilitas PMT ke ranah kecerdasan buatan dan tata kelola digital, di mana Kiran et al (2025) membuktikan dominasi *coping*

appraisal dalam pemodelan eksplanatori-prediktif perilaku siber, Alshammari & Al-mamary (2025) mengintegrasikan PMT dengan TPB dan *operant conditioning* untuk memetakan kepatuhan kebijakan organisasi, serta Lee et al., (2025) mengungkap bagaimana pengguna GenAI mengaktifkan mekanisme koping adaptif ketika menghadapi risiko privasi dan ketidakakuratan output. Temuan-temuan terkini ini secara konsisten menegaskan bahwa efektivitas PMT tidak lagi bergantung pada pendekatan berbasis ketakutan *(threat-driven)*, melainkan pada penguatan kapasitas koping, literasi teknologi, dan dukungan kontekstual yang memediasi proses *appraisal* kognitif. Meskipun perkembangan tersebut telah memperkaya pemahaman mengenai kepatuhan teknologi sukarela, belum ada studi yang secara eksplisit menguji mekanisme PMT yang diperluas pada fenomena *voluntary maladaptive behaviour* seperti *Shadow AI*, khususnya dalam konteks kesenjangan tata kelola organisasi dan tekanan produktivitas digital yang masih belum terpetakan secara empiris. Padahal, hubungan inilah yang krusial untuk merancang intervensi keamanan yang efektif dalam suatu organisasi. Analisis Kesenjangan Penelitian *(Research Gap Analysis)* tertuang pada Tabel 1.1 berikut ini.

Tabel 1.1 Analisis Kesenjangan Penelitian *(Research Gap Analysis)*

Studi (Tahun)	**Konteks/Contoh**	**Fokus Utama**	**Temuan Kunci**	**Kesenjangan (Gap) yang Diidentifikasi**
Puthal et al. (2025)	Shadow AI dalam lanskap keamanan siber organisasi	Ancaman teknis & organisasional Shadow AI	Memetakan risiko sistemik (data leakage, model poisoning) & kesenjangan governance organisasional	Berhenti pada level makro/teknis; belum menguraikan mekanisme psikologis individu yang mendorong adopsi sukarela
Balogun et al. (2025)	Sensitive industries (Healthcare, Finance, Education)	Implikasi etis & regulasi di sektor sensitif	Mengonfirmasi dampak privasi, bias algoritma, & risiko kepatuhan pada level institusional	Fokus pada aspek regulasi makro; mengabaikan proses kognitif mikro di balik keputusan

Studi (Tahun)	Konteks/Contoh	Fokus Utama	Temuan Kunci	Kesenjangan (Gap) yang Diidentifikasi
				pelanggaran kebijakan oleh karyawan
Sommestad et al. (2015)	Meta-analisis 28 studi PMT pada information security behaviour	Meta-analisis PMT & perilaku keamanan informasi	PMT menjelaskan ~40% varians niat; coping appraisal lebih prediktif untuk perilaku sukarela (voluntary)	Memvalidasi PMT untuk voluntary behaviour, namun penerapannya pada voluntary maladaptive behaviour (seperti Shadow AI) belum teruji secara empiris
Lee et al. (2025)	Pengguna GenAI umum yang menghadapi risiko privasi dan halusinasi	Adaptasi pengguna terhadap risiko GenAI	Risiko tidak selalu menghambat penggunaan; justru memicu mekanisme koping adaptif & verifikasi informasi	Menjelaskan respons risiko individu, tetapi belum mengintegrasikan dinamika pelanggaran kebijakan organisasional serta peran organizational support
Bankins et al (2023)	Tinjauan multilevel AI di organisasi (68 artikel empiris)	Tinjauan multilevel adopsi AI di organisasi	Literatur masih didominasi perspektif makro; secara eksplisit menyerukan riset mekanisme psikologis individu	Mengidentifikasi blind spot penelitian AI pada level individu, khususnya terkait kepatuhan, kognisi, & respons perilaku karyawan
Li et al. (2022)	Karyawan lintas sektor	Jalur mediasi kesadaran & perilaku protektif siber	Memvalidasi alur awareness → intention → behavior dengan niat sebagai mediator signifikan	Menyediakan kerangka mediasi yang kuat, namun belum mengintegrasikan cognitive appraisal PMT

Studi (Tahun)	Konteks/Contoh	Fokus Utama	Temuan Kunci	Kesenjangan (Gap) yang Diidentifikasi
				maupun spesifikasi konteks *Generative AI*
Kiran et al. (2025)	Pengguna cybersecurity & profesional	Pemodelan eksplanatori-prediktif perilaku siber	PMT terbukti robust; coping appraisal > threat appraisal; validasi metodologis PLS-SEM	Fokus pada kepatuhan siber umum & prediksi algoritmik, belum menguji voluntary AI violation di konteks ekonomi digital berkembang
Penelitian Ini	Karyawan perusahaan digital (startup, fintech, edutech, dll.) di Jabodetabek	Mekanisme kognitif PMT untuk Shadow AI Security Behaviour	Mengintegrasikan faktor kontekstual (Cybersecurity Awareness, AI Literacy, Organizational Support) → Threat/Coping Appraisal → Intention → Behaviour	Mengisi kesenjangan multidimensi dengan menjembatani perspektif makro-teknis dan mikro-behavioral melalui model PMT yang diperluas, diuji secara rigor dengan explanatory-predictive PLS-SEM pada perusahaan digital Jabodetabek

Berdasarkan fenomena, business gap dan research gap tersebut munculah pertanyaan-pertanyaan kritis seperti "Mengapa karyawan di perusahaan digital *(startup, e-commerce, fintech, edutech, ride hailing,* konsultan digital*)* tetap menggunakan *Shadow AI* meskipun menyadari risiko kebocoran data dan serang siber?" atau "Bagaimana persepsi kognitif berbasis *Protection Motivation Theory (PMT)* yang dipengaruhi *cybersecurity awareness*, dukungan organisasi dan literasi AI dapat membentuk niat dan perilaku penggunaan *Shadow AI*?". Studi terkini

menunjukkan bahwa faktor kontekstual organisasi seperti dukungan manajemen dan tingkat awareness keamanan siber secara signifikan memengaruhi appraisal kognitif individu dalam konteks perilaku keamanan informasi (Li et al., 2022). Selain itu, penelitian terbaru dalam konteks penggunaan *generative AI* menemukan bahwa literasi AI dan persepsi efektivitas respons menjadi determinan penting dalam membentuk niat penggunaan teknologi, bahkan ketika risiko privasi dan keamanan telah disadari (Lee et al., 2025; Tran et al., 2025). Dengan demikian, penelitian ini bertujuan menjawab pertanyaan tersebut dengan menguji model berbasis *Protection Motivation Theory (PMT)* yang diperluas dengan factor kontekstual, tujuannya untuk memberikan pemahaman teoritis yang lebih mendalam sekaligus memberikan rekomendasi manajerial yang konkret dalam mengelola risiko *Shadow AI*.

1.2 Rumusan Masalah

Perkembangan pesat *generative AI* mendorong meningkatnya *Shadow AI*, yaitu penggunaan alat AI publik oleh karyawan tanpa izin organisasi. Praktik ini menimbulkan risiko kebocoran data sensitive, pelanggaran regulasi dan ancaman keamanan siber, sementara dukungan organisasi seperti pelatihan, kebijakan AI yang jelas dan solusi AI resmi masih sangat terbatas. Kondisi ini menciptakan dilema bagi karyawan antara mengejar produktivitas atau mematuhi kebijakan keamanan siber, sehingga memicu perilaku *maladaptive* seperti *Shadow AI Security Behaviour*.

Meskipun *Protection Motivation Theory* (PMT) terbukti kuat menjelaskan perilaku keamanan siber, penelitian sebelumnya lebih banyak berfokus pada perilaku kepatuhan dan perilaku adaptif. Belum banyak penelitian yang mengintegrasikan faktor kontekstual seperti *cybersecurity awareness*, *organizational support*, dan *AI literacy* dengan mekanisme kognitif PMT *(threat appraisal dan coping appraisal)* untuk menjelaskan niat dan perilaku *Shadow AI*. Dengan demikian, masih terdapat kesenjangan pengetahuan knowledge gap mengenai bagaimana faktor kontekstual dan proses kognitif membentuk *Shadow AI Security Behaviour* pada karyawan perusahaan digital.

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mengisi kesenjangan pengetahuan *(knowledge gap)* dalam literatur keamanan siber dan perilaku penggunaan teknologi AI, khususnya terkait *Shadow AI* sebagai bentuk *maladaptive behaviour* secara sukarela di kalangan karyawan perusahaan digital *(startup, e-commerce, ride hailing, fintech, edutech* dan konsultan digital). Secara spesifik, penelitian ini bertujuan untuk.

1. Mengembangkan dan menguji model teoretis berbasis *Protection Motivation Theory* (PMT) yang diperluas dengan faktor kontekstual *(Cybersecurity Awareness, AI Literacy, Organizational Support)* untuk menjelaskan mekanisme kognitif yang mempengaruhi niat penggunaan *Shadow AI* di kalangan karyawan perusahaan digital.
2. Menguji pengaruh faktor *antecedant* yaitu *Cybersecurity Awareness, AI literacy,* dan *Organizational Support* terhadap proses kognitif *Protection Motivation Theory* (PMT) seperti *(Threat Appraisal)* dan *(Coping Appraisal)* dalam membentuk niat dan perilaku *Shadow AI*.
3. Menganalisa peran mediasi dari *Threat Appraisal (Perceived Severity)* dan *Coping Appraisal (Self Effjcacy, Response Self Efficacy & Response Cost)* terhadap *Intention to use Shadow AI* sebagaimana diusulkan oleh Tran et al (2025)
4. Mengindetifikasi dampak niat *Intention to use Shadow AI* dalam hubungan antara proses kognitif *Protection Motivation Theory* (PMT) dan perilaku nyata *Shadow AI Security Behaviour,* sebagaimana diuji oleh Kiran et al (2025)
5. Memberikan rekomendasi manajerial praktis bagi perusahaan digital untuk merancang intervensi keamanan siber yang efektif, dengan mempertimbangkan tekanan kerja, dukungan organisasi, dan litetasi AI karyawan.

Oleh karena itu, penelitian ini tertarik untuk menjawab beberapa pertanyaan sebagai berikut :

1. Bagaimana faktor kontekstual organisasi *(Cybersecurity Awareness, AI Literacy, Organizational Support)* memengaruhi persepsi kognitif *(Perceived Severity, Self Efficacy, Response Self Efficacy, Response Cost)* karyawan terkait penggunaan *Shadow AI*?
2. Bagaimana persepsi kognitif *(Perceived Severity, Self Efficacy, Response Self Efficacy, Response Cost)* berbasis *Protection Motivation Theory* membentuk niat penggunaan *Shadow AI*?
3. Apakah niat penggunaan *Shadow AI* memediasi hubungan antara persepsi kognitif *(Perceived Severity, Self Efficacy, Response Self Efficacy, Response Cost)* dan *Shadow AI Security Behaviour*?

1.4 Manfaat Penelitian

Bagian ini memaparkan kontribusi atau manfaat penelitian yang mengungkapkan secara spesifik kegunaan yang hendak dicapai, dilihat dari sisi:

a. Kontribusi Akademis. Penelitian ini memperluas *Protection Motivation Theory* (PMT) ke dalam konteks *maladaptive behaviour* khususnya *Shadow AI* yang belum pernah diuji sebelumnya. Selama ini, PMT hanya digunakan untuk menjelaskan perilaku patuh *(compliance)*, bukan pelanggaran sukarela demi efisiensi. Penelitian ini juga mengintegrasikan faktor kontekstual *(Cybersecurity Awareness, AI Literacy, Organizational Support)* sebagai anteseden proses kognitif *Protection Motivation Theory (PMT)*, memperkaya model yang selama ini bersifat individualistik.

b. Kontribusi Manajerial. Temuan penelitian memberikan dasar bagi perusahaan digital untuk:
   - Merancang kebijakan AI yang realistis (tidak hanya melarang, tapi menyediakan alternatif resmi),
   - Meningkatkan pelatihan literasi AI dan keamanan siber,

- Mengomunikasikan risiko dengan fokus pada dampak pribadi (bukan hanya organisasi), sesuai prinsip *Protection Motivation Theory* (PMT).

Dengan demikian, penelitian ini membantu perusahaan mengurangi risiko kebocoran data sekaligus mendukung produktivitas berbasis AI yang aman.