

BAB II KAJIAN TEORI

A. Hakikat Informasi

Hakikat informasi adalah pondasi yang tak terpisahkan dalam kemajuan komunikasi dan pengetahuan manusia. Secara luas, informasi merupakan representasi dari data yang telah diatur, diproses, dan diinterpretasikan sehingga memiliki relevansi dan nilai bagi individu atau kelompok yang menerimanya. Namun, untuk memahami sepenuhnya esensi informasi, diperlukan penelusuran mendalam terhadap beragam aspek, seperti sumber, kualitas, serta konteksnya. Hanya dengan pemahaman yang komprehensif tentang sifat dan fungsi informasi, kita dapat mengenali peran serta implikasinya dalam berbagai situasi dan lingkungan yang berbeda (Aldhafferi et al., 2013a).

Informasi, sebagai elemen vital dalam komunikasi manusia, tidak hanya memungkinkan pertukaran gagasan dan pengetahuan, tetapi juga menjadi landasan bagi pengembangan hubungan interpersonal yang berkualitas. Dengan adanya informasi yang tersedia, individu dapat memperluas cakrawala pemahaman mereka tentang lingkungan sekitar, menggali berbagai perspektif, dan memperdalam pemahaman mereka tentang isu-isu kompleks. Selain itu, informasi juga memberikan kemampuan kepada individu untuk mengambil keputusan yang lebih tepat dan terinformasi, baik dalam ranah pribadi maupun profesional. Sebagai hasilnya, informasi tidak hanya menjadi alat penting untuk membangun hubungan sosial yang kuat, tetapi juga menjadi pendorong utama dalam kemajuan dan perkembangan masyarakat secara keseluruhan.

Informasi tidaklah sekadar kumpulan data mentah; ia melibatkan proses kompleks penyaringan, interpretasi, dan kontekstualisasi. Ini berarti bahwa informasi tidak hanya terdiri dari fakta belaka, tetapi juga mencakup pemahaman tentang bagaimana fakta-fakta tersebut saling terkait dan relevan dengan situasi atau permasalahan yang sedang dihadapi. Proses ini menambahkan dimensi yang lebih dalam pada informasi, memungkinkan individu untuk melihat lebih dari sekadar informasi dasar dan menggali makna yang lebih mendalam dari setiap data yang mereka terima. Dengan demikian, informasi menjadi lebih bermakna dan berguna dalam konteks pengambilan keputusan dan pemecahan masalah.

Sumber informasi memegang peranan sentral dalam menentukan kualitas dan keandalan informasi yang disampaikan. Sumber-sumber yang dianggap kredibel dan terpercaya sering kali menjadi penjaga integritas informasi dengan menghasilkan konten yang berkualitas tinggi dan akurat. Mereka cenderung didukung oleh riset yang mendalam, sumber daya yang kuat, dan reputasi yang terjaga, sehingga memberikan keyakinan kepada pembaca atau pengguna informasi. Di sisi lain, sumber-sumber yang tidak kredibel atau dipertanyakan dapat menyebarkan informasi yang salah atau menyesatkan. Hal ini dapat menciptakan lingkungan di mana kebenaran menjadi samar, dan kepercayaan publik terhadap informasi itu sendiri bisa terkikis. Oleh karena itu, penting bagi individu untuk melakukan evaluasi kritis terhadap sumber informasi yang mereka konsumsi, dengan mempertimbangkan reputasi, metodologi, dan niat dari sumber tersebut (Aldhafferi et al., 2013a).

Penting untuk diingat bahwa informasi juga selalu terkait dengan konteks dan motivasi di balik penyampaiannya. Sebagian informasi dapat disampaikan dengan niat baik untuk mengedukasi, memberdayakan, atau memberikan pemahaman yang lebih baik tentang suatu topik kepada pembaca. Namun, di sisi lain, terdapat informasi yang disampaikan dengan motif yang lebih tersembunyi, seperti memengaruhi atau bahkan memanipulasi pendapat orang lain sesuai dengan agenda tertentu. Kesadaran akan tujuan di balik informasi dapat membantu individu untuk mengembangkan sikap kritis terhadap informasi yang diterima, memungkinkan mereka untuk membedakan antara informasi yang objektif dan yang memiliki kepentingan tersembunyi.

Selain sebagai alat komunikasi dan pertukaran pengetahuan, informasi juga memainkan peran penting dalam pembentukan dimensi sosial masyarakat. Informasi menjadi fondasi untuk membangun identitas sosial, mengukuhkan nilai-nilai budaya, dan meneguhkan norma-norma yang mengatur interaksi sosial. Melalui informasi, individu dan kelompok dapat memahami dan merespons dinamika sosial, memperkuat solidaritas, serta mengembangkan kesadaran akan perbedaan dan persamaan di dalam masyarakat. Dengan demikian, informasi bukan sekadar data yang bersifat statis, tetapi sebuah kekuatan yang dinamis yang membentuk dan memengaruhi jalinan sosial dalam masyarakat.

Tidak hanya itu, dengan berkembangnya teknologi informasi dan komunikasi, hakikat informasi juga mengalami transformasi yang signifikan. Internet dan media sosial telah mengubah cara informasi diproduksi, disebarluaskan, dan dikonsumsi oleh masyarakat secara keseluruhan. Namun, perlu diingat bahwa informasi tidak selalu netral atau obyektif. Informasi seringkali dipengaruhi oleh kepentingan politik, ekonomi, dan sosial tertentu, serta bias individu atau kelompok. Oleh karena itu, menjadi penting untuk secara kritis mengevaluasi dan memilah informasi yang diterima agar dapat membuat keputusan yang tepat dan bertanggung jawab.

B. Keamanan Informasi

Keamanan Informasi menurut merupakan langkah pencegahan terhadap tindakan penipuan pada sistem yang berbasis informasi berbentuk non-fisik (Aldhafferi et al., 2013b). Keamanan informasi adalah tindakan pencegahan dari serangan pengguna computer atau pengakses jaringan yang tidak bertanggung jawab (Revilia, n.d.). Keamanan informasi adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak di kenali dalam sistem komputer (Ahlan et al., 2015b). Dari beberapa pendapat para ahli dapat disimpulkan bahwa keamanan sistem informasi pada komputer merupakan suatu upaya pencegahan kerusakan dan gangguan sistem informasi dari serangan yang terdeteksi pada ancaman yang tidak memiliki arti fisik. Pada CIA triad terdapat 3 aspek dasar yang harus selalu diperhatikan dalam menjaga keamanan informasi. Aspek tersebut adalah *Confidentiality*, *Integrity* dan *Availability*. Tiga aspek keamanan informasi tersebut ialah (Al-Omari et al., 2012):



Gambar 2.2 Tiga Aspek Keamanan Informasi

Sumber: *Cia Triad*

1. *Confidentiality* (Kerahasiaan)

Data-data yang menghasilkan sebuah informasi harus dijaga kerahasiaannya

dari pihak yang tidak berhak mengakses. Usaha untuk memastikan informasi diakses oleh orang yang berwenang atau bagi orang yang memiliki otoritas ini dilakukan dengan menerapkan enkripsi agar penyebaran informasi jelas dan terarah sehingga tidak menimbulkan kerugian bagi pihak yang membutuhkan.

2. *Integrity* (Integritas)

Informasi yang dimiliki tidak boleh diubah oleh orang yang tidak berhak. Hal ini dilakukan untuk memastikan bahwa informasi yang dimiliki dan diakses adalah benar, akurat, dan lengkap. Integritas informasi biasanya dilakukan dengan menerapkan akses kontrol atau pembatasan hak akses untuk mengedit, sehingga yang lain hanya mampu melihat atau membaca informasi yang dihasilkan.

3. *Availability* (Ketersediaan)

Informasi yang dibutuhkan harus dipastikan ketersediaannya, agar aspek ketersediaan ini tercapai biasanya dalam organisasi menerapkan *back-up* data atau cadangan tempat bagi data-data yang akan menghasilkan informasi. Hal tersebut dilakukan agar informasi tetap tersedia walaupun terjadi bencana pada sistem.

Keamanan Informasi pada dasarnya mewakili praktik pencegahan akses, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, perekaman, atau penghancuran informasi yang tidak sah. Ini terdiri dari tiga elemen utama yang disebut sebagai kerahasiaan, integritas, dan aksesibilitas (Puhakainen, 2006). Jika salah satu dari tiga elemen utama ini rusak, kelemahan keamanan terjadi. Informasi adalah aset yang sangat diperlukan dan berharga bagi orang dan organisasi. Dengan demikian, keamanan sangat penting untuk menjaga informasi. Selain itu, teknologi yang terus berkembang dan digunakan untuk pemrosesan informasi menimbulkan risiko (Yel & Nasution, 2022). Sistem informasi juga menjadi global saat ini. Akibatnya, semua individu dan institusi yang memiliki hubungan langsung atau tidak langsung dengan sistem informasi sekarang harus berkontribusi pada keamanan informasi (Revilia, n.d.).

Keamanan informasi menjadi landasan penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data yang disimpan dan dipertukarkan secara elektronik maupun fisik. Penulis memperhatikan bahwa tantangan keamanan informasi semakin kompleks seiring dengan kemajuan teknologi, yang memerlukan

pendekatan yang holistik dan berkelanjutan dalam melindungi informasi dari ancaman seperti peretasan, pencurian identitas, dan serangan malware. Upaya penguatan keamanan informasi melibatkan kebijakan, teknologi, dan pelatihan sumber daya manusia agar dapat mengidentifikasi, mencegah, dan merespons ancaman dengan cepat dan efektif. Dengan memprioritaskan keamanan informasi, organisasi dan individu dapat membangun kepercayaan, melindungi aset penting, dan menjaga ketersediaan layanan bagi penggunaannya yang aman dan produktif.

Keamanan informasi sendiri memiliki 3 aspek yang penting. *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan. *Integrity* (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (*authorized*), harus terjaga keakuratan dan keutuhan informasi serta *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait bilamana diperlukan.

C. Teknik keamanan Informasi

Pengamanan informasi perlu dilakukan untuk menjaga informasi yang dimiliki oleh individu maupun organisasi. Ada beberapa teknik yang dapat digunakan dalam pengamanan informasi meliputi:

1. Pembatasan akses dengan *password* dan *username* atau biometrik
2. *Cryptography* (penyandian) dan *steganography* (pengkodean).

Menurut Romney dan Steinbart (Fata, 2021), *password* yang baik terdiri dari berbagai faktor, yaitu :

1. *Length*

Kata sandi yang kuat berkaitan dengan panjangnya. Lebih panjang kata sandi yang dibuat akan lebih baik.

2. *Multiple character types*

Password yang baik akan menggunakan campuran huruf besar dan huruf kecil, angka, dan karakter khusus untuk meningkatkan kekuatan dari kata sandi.

3. *Randomness*

Password harus tidak mudah untuk ditebak dan diusahakan tidak dapat ditemukan di kamus.

4. *Changed frequently*

Password harus diganti secara berkala. Kebanyakan pengguna mengganti kata sandinya paling tidak setiap 90 hari sekali dan pengguna yang memiliki akses ke informasi yang sensitif biasanya mengganti kata sandinya lebih sering yaitu setiap 30 hari sekali.

5. *Keep secret*

Password harus terjaga kerahasiannya dari orang-orang yang tidak memiliki kepentingan khusus.

D. Kesadaran Keamanan Informasi

Menurut McLeod dan Schell (2008) keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu kerahasiaan, ketersediaan dan integritas. Menurut Whitman dan Mattord (2011), keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi

Kruger dan Kearney (Andrea et al., 2016) menggambarkan kesadaran keamanan sistem sebagai pemahamannya kepentingan melalui pengguna, memahami tanggung jawab pribadi, dan melakukan tindakan yang sesuai dengan prosedur institusi. Menurut Furnell dan Clarke, dimensi teknologi tidak menjamin lingkunganyang terpelihara untuk keamanan informasi. Oleh karena itu, pengguna akhir menjalankan peran kunci dalam konsep keamanan informasi (Aldhafferi et al., 2013b)

Menurut Kruger & Kerney menggunakan teori psikologi sosial membagi tiga komponen untuk mengukur objek yakni *cognition*, *affection* dan *behaviour*. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *Knowledge* (pengetahuan seseorang), *Attitude* (sikap seseorang) dan *Behaviour* (perilaku seseorang).

1. *Knowledge* (pengetahuan)

Menurut Notoatmodjo, “pengetahuan merupakan hasil dari tahu dan ini terjadi setelah orang melakukan pengindraan terhadap suatu objek tertentu”. Pengetahuan menjadi salah satu bagian penting bagi individu dalam kehidupan kesehariannya. Pengetahuan menurut Notoatmodjo (2012) mempunyai 6

tingkatan yaitu:

a. Tahu

Tahu diartikan sebagai keadaan individu dalam mengingat materi yang telah dipelajari. Tingkatan tahu ini berhubungan dengan aktifitas mengingat kembali terhadap sesuatu yang spesifik dari seluruh bahan yang dipelajari atau rangsang yang diterima (Fata, 2021).

b. Memahami

Memahami merupakan kemampuan untuk menjelaskan secara benar mengenai suatu objek dan menginterpretasikan materi yang ada secara benar dan menjelaskan serta menyebutkan contoh.

c. Aplikasi

Aplikasi adalah kemampuan untuk menggunakan materi yang telah didapatkan pada situasi kondisi yang sebenarnya terjadi. Contohnya adalah menggunakan rumus, metode, prinsip, dan lainnya.

d. Analisis

Analisis merupakan kemampuan menjabarkan materi atau objek ke dalam komponen-komponen yang masih berkaitan satu dengan yang lain. Keberhasilan analisis seseorang dapat terlihat dari penggunaan kata kerja dapat menggambarkan, mengelompokkan, membedakan, memisahkan, dan sebagainya.

e. Sintesis

Sintesis mengarah kepada kemampuan untuk meletakkan atau menghubungkan bagian-bagian dalam suatu bentuk keseluruhan yang baru. Sintesis juga merupakan kemampuan untuk menyusun, merencanakan, meringkas, menyesuaikan teori atau rumusan yang telah ada.

f. Evaluasi

Evaluasi merupakan kemampuan untuk melakukan penilaian terhadap suatu materi atau objek penilaian berdasarkan kriteria yang ditentukan sendiri atau menggunakan kriteria yang sudah ada.

2. *Attitude* (sikap)

Attitude adalah sikap seseorang dalam berinteraksi ataupun berkomunikasi dengan sesama manusia. Menurut Sukardi (dalam Gunawan, 2021), sikap adalah

suatu kesiapan seseorang untuk bertindak terhadap hal-hal tertentu. Komponen-komponen sikap menurut (Gunawan, 2021) adalah:

a. *Kognitif*

Kognitif adalah komponen yang terbentuk dari pengetahuan dan informasi yang diterima oleh individu dalam kehidupannya yang selanjutnya diproses untuk menghasilkan suatu keputusan untuk bertindak.

b. *Afektif*

Afektif menyangkut masalah emosional subyektif sosial terhadap suatu objek, dimana secara umum dalam psikologi komponen afektif disamakan dengan perasaan yang dimiliki terhadap suatu objek.

c. *Konatif*

Konatif menunjukkan bagaimana kecenderungan berperilaku yang ada dalam diri seseorang berkaitan dengan cara menyikapi objek yang sedang dihadapinya. Berdasarkan penjelasan yang telah disampaikan di atas, dapat disimpulkan bahwa sikap merupakan suatu bentuk reaksi yang timbul atas objek tertentu yang nantinya berhubungan dengan perilaku. Sikap dapat dibentuk atau dipelajari sepanjang individu terus berkembang dalam kehidupan kesehariannya. Sikap merupakan hasil interaksi individu dengan lingkungan sekitarnya.

3. *Behaviour* (perilaku)

Perilaku menunjukkan tindakan yang dilakukan oleh individu terhadap keamanan informasi. Menurut Walgito (2010), perilaku merupakan respon dari stimulus yang mana setiap individu memiliki kemampuan untuk menentukan perilaku yang akan diambalnya. Skinner membagi perilaku menjadi 2 jenis, yaitu:

a. Perilaku Alami

Perilaku alami atau dalam psikologi dikenal dengan *innate behaviour* merupakan perilaku yang dibawa sejak lahir. Perilaku ini biasanya berupa refleks-refleks tertentu atau insting.

b. Perilaku Operan

Perilaku operan atau biasa dikenal dengan nama *operant behaviour* merupakan perilaku yang dibentuk melalui proses belajar.

Penelitian yang dilakukan Mattord dan Whittman memaparkan, salahsatu program yang paling jarang diterapkan, tetapi paling bermanfaat, adalah program kesadaran keamanan. Program kesadaran keamanan dirancang untuk menjaga keamanan informasi di depan pikiran pengguna. Program-program ini tidak harus rumit atau mahal. Program yang baik dapat mencakup buletin, poster keamanan, video, papan buletin, pamflet, dan pernak-pernik. Pernak-pernik dapat mencakup slogan keamanan yang tercetak di alas mouse, cangkir kopi, T-shirt, pena, atau benda apa pun yang sering digunakan selama hari kerja yang mengingatkan karyawan akan keamanan (Munthe & Purnama, 2019). Selain itu, program kesadaran keamanan yang baik membutuhkan individu yang berdedikasi yang bersedia menginvestasikan waktu dan upaya untuk mempromosikan program, bersediameberikan dukungan keuangan yang dibutuhkan. Keamanan informasi adalah metode yang paling hemat biaya untuk menyebarkan informasi dan berita keamanan kepada karyawan. Informasi dapat didistribusikan melalui hard copy, e-mail, atau intranet. Tujuannya adalah untuk menjaga gagasan keamanan informasi di benak pengguna dan untuk merangsang pengguna agar peduli dengan keamanan (Poepjes & Lane, 2012). Jika program kesadaran keamanan tidak diterapkan secara aktif, karyawan mungkin mulai mengabaikan masalah keamanan dan risiko kecelakaan dan kegagalan karyawan akan meningkat.

Kruger melakukan pengukuran pada ketiga dimensi ini di 7 area yang termasuk memiliki resiko yang kritis yaitu:

1. Selalu taat pada aturan perusahaan (*policies-A1*)
2. Menjaga kerahasiaan password dan *Personal Identity Number* (PIN) (*password-A2*)
3. Menggunakan e-mail dan internet dengan bijaksana (*email & internet-A3*)
4. Berhati-hati menggunakan perangkat seluler (*mobile equipment-A4*)
5. Melaporkan insiden keamanan informasi (*incidents-A5*)
6. Menyadari konsekuensi setiap tindakan (*consequences-A6*)
7. Melakukan Back-up Data (*Back-up data A7*)

E. Media Sosial

Media sosial dapat dipahami sebagai suatu platform digital yang menyediakan fasilitas untuk melakukan aktivitas sosial bagi setiap penggunanya.

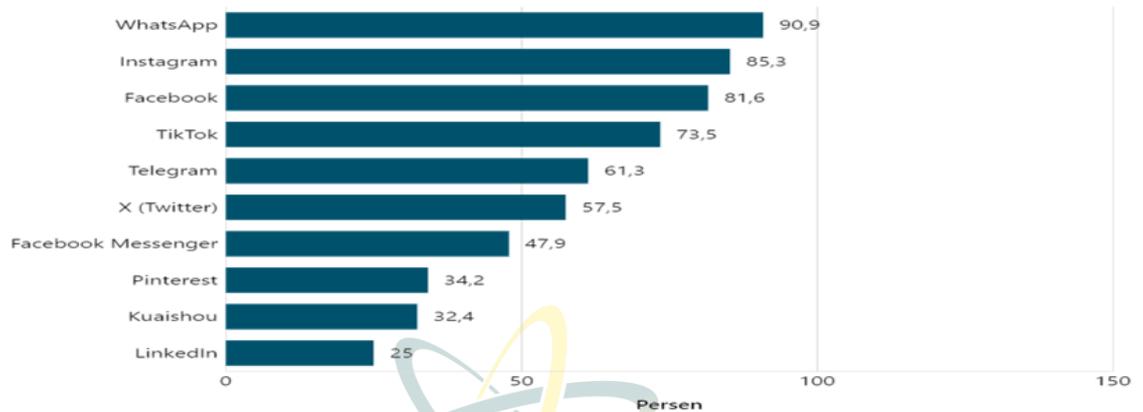
Beberapa aktivitas yang dapat dilakukan di media sosial, misalnya yaitu melakukan komunikasi atau interaksi hingga memberikan informasi atau konten berupa tulisan, foto dan video. Berbagai informasi dalam konten yang dibagikan tersebut dapat terbuka untuk semua pengguna selama 24 jam penuh. Media sosial sendiri pada dasarnya adalah bagian dari pengembangan internet. Kehadiran beberapa dekade lalu telah membuat media sosial dapat berkembang dan bertumbuh secara luas dan cepat seperti sekarang. Hal inilah yang menjadikan semua pengguna yang tersambung dengan koneksi internet dapat melakukan proses penyebaran informasi atau konten kapan pun dan di mana pun (Amin, 2014).

Media sosial adalah sebuah media online, dengan para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, jejaring sosial, wiki, forum dan dunia virtual. Menurut Nasrullah (2015) media sosial adalah medium di internet yang memungkinkan pengguna merepresentasikan dirinya maupun berinteraksi, bekerja sama, berbagi, berkomunikasi dengan pengguna lain membentuk ikatan sosial secara virtual. Menurut B.K. Lewis (2010) dalam karyanya yang berjudul *Social Media and Strategic Communication Attitudes and Perceptions among College Students* yang terbit pada tahun 2010 menyatakan, bahwa media sosial merupakan suatu label yang merujuk pada teknologi digital yang berpotensi membuat semua orang untuk saling terhubung dan melakukan interaksi, produksi dan berbagi pesan. Menurut Chris Brogan (2010) dalam bukunya yang berjudul *Social Media Tactics and Tips to Develop Your Business*, menyebutkan bahwa media sosial adalah suatu perangkat alat komunikasi yang memuat berbagai kemungkinan untuk terciptanya bentuk interaksi gaya baru. Menurut Dave Kerpen (2011) dalam bukunya yang bertajuk *Likeable Social Media* yang terbit pada tahun 2011 mengemukakan bahwa media sosial memiliki definisi sebagai suatu tempat kumpulan gambar, video, tulisan hingga hubungan interaksi dalam jaringan, baik itu antar individu maupun antar kelompok seperti organisasi. Media sosial adalah mengenai menjadi manusia biasa. Manusia biasa yang saling membagi ide, bekerjasama, dan berkolaborasi untuk menciptakan kreasi, berpikir, berdebat, menemukan orang yang bisa menjadi teman baik, menemukan pasangan, dan membangun sebuah komunitas. Intinya, menggunakan media sosial menjadikan kita sebagai diri sendiri (Nurul et al., 2022).

F. Pengguna Media Sosial

10 Aplikasi Media Sosial yang Paling Banyak Dipakai Pengguna Internet* di Indonesia (Januari 2024)

 databoks



Sumber:
We Are Social

Informasi Lain:
pengguna internet usia 16-64 tahun yang menggunakan media sosial setiap bulan

Menurut laporan terbaru We Are Social, WhatsApp menjadi aplikasi media sosial yang paling banyak digunakan di Indonesia pada Januari 2024. Dari seluruh pengguna internet di Indonesia yang berusia 16—64 tahun, mayoritas atau 90,9% nya tercatat memakai aplikasi tersebut. Instagram menempati posisi kedua dengan proporsi pengguna 85,3%, diikuti Facebook 81,6%, dan TikTok 73,5%. Kemudian yang menggunakan Telegram ada 61,3%, dan X (dahulu Twitter) 57,5%. Ada pula yang menggunakan Facebook Messenger, Pinterest, Kuaishou (Kwai dan Snack Video), serta LinkedIn dengan proporsi lebih kecil seperti terlihat pada grafik. Secara keseluruhan, We Are Social mencatat ada 139 juta identitas pengguna media sosial di Indonesia pada Januari 2024. Jumlahnya setara 49,9% dari total populasi nasional (*We Are Social, 2024*). Penggunaan media sosial di Indonesia meningkat dari tahun ke tahun, dengan penggunaan internet yang lebih banyak digunakan untuk berhubungan dengan teman dan keluarga, mengisi waktu luang, mengetahui apa yang dibicarakan oleh orang lain, dan mencari inspirasi tentang apa yang akan dilakukan (Kruger & Kearney, 2006).

G. Penelitian Terdahulu

Penelitian yang berjudul ”*Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Sosial Media*” ini berfokus pada kesadaran keamanan informasi dan privasi dalam penggunaan media sosial, khususnya di kalangan mahasiswa Program Studi Sistem Informasi, Fakultas Teknologi Industri, Universitas Atma

Jaya Yogyakarta. Penelitian ini membahas terkait teknologi informasi dan internet yang telah mengubah cara manusia berkomunikasi, dengan media sosial yang menjadi salah satu platform utama untuk memperoleh dan membagikan berita acara secara online. Peneliti juga berpendapat bahwa media sosial telah menyediakan kemudahan dan kecepatan dalam pembuatan dan distribusi konten, namun juga membawa masalah terkait keamanan informasi dan privasi (Gunawan, 2021). Dari hasil penelitian tersebut, meskipun ada 85% mahasiswa memahami pentingnya keamanan informasi, perilaku mereka tidak mencerminkan kesadaran tersebut. Sebanyak 75% dari mereka tidak mengganti kata sandi secara berkala dan sering mengakses media sosial di tempat umum yang tidak diketahui Tingkat keamanannya. Jika dilihat dalam hal privasi, ada 40,6% mahasiswa masih mencantumkan informasi pribadi di media sosial yang terbuka untuk umum dan 54,9% tidak menerapkan pengaturan privasi yang memadai. Penelitian ini menggunakan metode penelitian lapangan (field research) dengan pendekatan kuantitatif, yang melibatkan pengumpulan data melalui kuisinoner yang disebarkan kepada 143 mahasiswa. Data yang valid dan dapat dianalisis berjumlah 133 sampel. Data primer diperoleh langsung dari responden melalui kuesioner, sementara data sekunder dikumpulkan dari buku, brosur dan artikel terkait. Hasil kuesioner menunjukkan adanya kesenjangan antara pemahaman dan praktik keamanan informasi di kalangan mahasiswa. Sebagian besar responden masih menunjukkan perilaku yang berisiko terhadap keamanan dan pprivasi informasi mereka di media sosial. Adapun perbedaan penelitian ini adalah dengan jumlah responden dan sampel yang berbeda. Namun persamaannya terletak pada sama-sama meneliti tentang kesadaran dan keamanan informasi di era digital khususnya para mahasiswa.

Penelitian yang berjudul "*Eksistensi Media Sosial, Youtube, Instagram dan Whatsapp Ditengah Pandemi Covid-19 Dikalangan Masyarakat Virtual Indonesia*" artikel ini membahas terkait perkembangan media sosial dan dampaknya terhadap keamanan informasi serta privasi pengguna. Peneliti menjelaskan terkait media sosial seperti youtube, Instagram, dan Whatsapp mengalami peningkatan signifikan selama pandemi Covid-19 (Ihendra & Laugu, 2020). Indonesia menempati posisi ketiga terbesar di dunia dalam jumlah pengguna media sosial.

Penelitian menunjukkan adanya lonjakan media sosial Youtube skitar 88%, Whatsapp sebesar 84%, dan Instagram sebesar 79%. Media sosial telah menjadi bagian integral dari kehidupan sehari-hari menyediakan kemudahan dan kecepatan dalam berbagi dan mengakses informasi. perkembangan media sosial di indonesia dan global mengalami peningkatan yang sangat signifikan. Metode yang digunakan dalam penelitian ini yaitu studi pustaka. Metode dengan studi kepustakaan merupakan teknik yang digunakan untuk meneliti dalam memecahkan suatu masalah dengan cara penelahan terhadap buku-buku, literatur-literatur, catatancatatan, dan laporan yang ada kaitannya dengan masalah yang diteliti.

Penelitian ini juga menggunakan jenis penelitian deskriptif. Berdasarkan data yang didapatkan menyebutkan bahwa indonesia pengguna internet terbesar no 3 dunia bersama dengan jepang dan india. Pengguna internet di indonesia mengalami lonjakan sekitar 17.3 % juta dari 64% dari total penduduk Indonesia mayoritas pengguna menggunakan posel sebanyak 171 juta atau setara dengan 98% . Menyikapi hal tersebut maka dapat dilihat bahwa Eksistensi dari berbagai media juga mengalami peningkatan dalam suasana pandemi covid-19 ini seperti media sosial youtube adalah salah satu media sosial dengan pengguna terbesar dunia khususnya indonesia dengan jumlah pengguna sekitar 88% dan selanjutnya disusul oleh media sosial Whatsapp dengan jumlah akses sebesar 84 %, instagram dengan 79% dengan hal itu dapat kita lihat perbandingan dari tingkat eksistensi media sosial media yang populer selama masa pandemi Covid-19 yang menempatkan youtube sebagai media pertama yang sangat digemari dengan jumlah pengguna tertinggi didunia. Adapun persamaan penelitian adalah kesamaan yang meneliti terkait kesadaran masyarakat terhadap system keamanan sosial media. Perbedaannya adalah pada letak sampel dan objek yang diteliti. Pada penelitian ini peneliti berfokus pada media sosial seperti Youtube, Instagram dan Whatsapp ditengah pandemi Covid-19.

Penelitian selanjutnya adalah penelitian yang berjudul “*Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising*” Salah satu perkembangan teknologi itu yaitu berupa Perkembangan jejaring media sosial. Banyak kemudahan yang ditawarkan oleh media komunikasi baru ini, pengguna jejaring sosial dapat menyebarkan maupun mencari pesan atau informasi

dengan cepat. Meningkatnya penggunaan jejaring sosial di Indonesia disebabkan oleh semakin lengkapnya fasilitas akses internet. Kita tidak mengetahui apakah aplikasi media sosial ini aman untuk digunakan, karena dunia internet tentu tidak lepas dari masalah keamanan karena di internet data bisa masuk ke mana saja. Oleh karena itu, disarankan kepada setiap user untuk tetap memperhatikan keamanan informasi dalam menggunakan social media (Fata, 2021). Perkembangan teknologi informasi semakin mempengaruhi kehidupan manusia. Segala aspek kehidupan telah mengandung unsur internet dalam memudahkan pekerjaan. Kata teknologi dan internet tak asing lagi di kalangan masyarakat bahkan pada masyarakat awam sekalipun. Hal ini didasari telah menyebar luasnya koneksi internet dan sangat mudah untuk diakses. Perkembangan teknologi sejauh ini sangatlah pesat terutama pada bagian internet yang dapat dimanfaatkan untuk komunikasi tidak hanya bisa digunakan pada perangkat besar seperti personal computer atau laptop yang terhubung lewat jaringan web akan tetapi penggunaan pada bidang komunikasi saat ini bisa diakses lewat perangkat yang lebih ringkas yaitu mobile. Pesatnya perkembangan teknologi pada mobile ini sekarang dapat digunakan tidak sekedar untuk komunikasi tapi kita dapat mengakses berbagai macam aplikasi yang sudah saling terhubung di internet diantaranya ada fintech, game online, aplikasi belanja, akses map, aplikasi bank, streaming video dan music, aplikasi Kesehatan dan bahkan aplikasi kewanitaan semua kini dapat diakses hanya melalui mobile. Terdapat sangat banyak aplikasi yang mendukung kemudahan komunikasi maka terciptalah media sosial. Media sosial itu sendiri pun tergolong dalam beberapa bidang dalam mempublikasikan konten dan komunikasi, ada media sosial chat yang mendukung penuh untuk melakukan chatting dan juga ada media sosial share yang mendukung untuk melakukan publish text, gambar, dan video untuk disebarluaskan dan dapat diakses oleh seluruh pengguna lainnya. Menurut data statistik dari Hootsuite pengguna media sosial di dunia mencapai 3,8 miliar orang dari jumlah populasi dunia yaitu 7,75 miliar. Di Indonesia sendiri pengguna media sosial mencapai 160 juta orang dari jumlah populasi 272 juta orang. Disini terbukti bahwa orang menggunakan media sosial untuk tetap terhubung satu sama lain dan angka tersebut akan bertambah setiap tahunnya. *Phishing* adalah upaya untuk mendapatkan informasi dengan teknik pengelabuan. Data yang di *phishing*

merupakan data pribadi yang di input oleh korban pada laman palsu yang di kloning dari laman tertentu. Kegiatan *phising* memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. metode penelitian yang digunakan melalui studi literature dan percobaan, yang bertujuan mendapat pengetahuan. Studi literature didapatkan melalui jurnal, internet, dan sebagainya. Sedangkan percobaan dilakukan sendiri dengan menggunakan sistem operasi kali linux dan tool setoolkit dan menerapkan teknik *phising*. Hasil penelitian pada jurnal ini adalah dengan menunjukkan hasil percobaan yang membuktikan bahwa semua media sosial rentan terhadap teknik *phising*. Berbagai halaman bisa saja di cloning untuk mengelabui pengguna. Aksi *phising* ini sangat sering terjadi maka dihibau kepada seluruh pengguna media sosial agar berhati-hati dan selalu memperhatikan url saat mengakses laman tertentu. Persamaan penelitian ini adalah sama-sama meneliti tentang bagaimana keamanan informasi yang bisa diusahakan pada setiap individu yang menggunakan media sosial tersebut. Perbedaan penelitian ini adalah penelitian ini menggunakan bagaimana cara Teknik *phising* tersebut bekerja dalam mengganggu keamanan informasi para pengguna media sosial.

Penelitian selanjutnya berjudul “*Literasi Media Sosial: Kesadaran Keamanan Dan Privasi Dalam Perspektif Generasi Milenial*”. Situs media sosial memberi masyarakat analog kemampuan menjangkau audiens global, dan berjasa dalam sarana konektivitas untuk mencari informasi, bersosialisasi, dan mempengaruhi, sayangnya juga memberikan celah terjadinya pelanggaran privasi dan keamanan terhadap data pribadi pengguna. Hasil survei CSIS pada Agustus 2017 menyebutkan 54,3 persen generasi milenial menggunakan media online setiap harinya, sebanyak 81,7 persen generasi milenial menggunakan Facebook, 70,3 persen menggunakan Whatsapp dan 54,7 persen menggunakan Instagram. Ini menjadikan peran media sosial sangat krusial untuk mempersuasi dan sekaligus juga memberikan kerentanan pada generasi millennial . Generasi milenial adalah generasi yang lahir antara tahun 1981-2000, atau yang saat ini berusia 19 tahun hingga 38 tahun, begitu mudahnya terpapar ancaman keamanan di dunia digital, karakteristik mereka berbagi data pribadi dengan berbagai perangkat online yang disebabkan oleh konvergensi media menambah resiko ancaman digital, bagaimana mereka menangkap situasi kerentanan keamanan cyber ini serta sejauh mana

pemahaman mereka tentang ancaman tersebut menjadi masalah yang menarik untuk diteliti. Perilaku tersebut tergantung pada realisasi aktual dan pengalaman mereka di media sosial. Sebagai contoh, pengguna yang menjadi korban pencurian identitas atau cyber bullying akan memiliki perspektif keamanan dan kepercayaan yang sangat berbeda dari mereka yang tidak. Penelitian ini dilakukan bertujuan untuk mengetahui bagaimana kondisi literasi digital terhadap penggunaan media sosial di kalangan generasi milenial yang merupakan pengguna aktif dari media sosial. Generasi milenial sebagai generasi yang "selalu terhubung" menjadi target dari kurangnya kesadaran akan pentingnya prosedur keamanan dan privasi ini.

Salah satu karakteristik mereka yaitu berbagi data dengan berbagai perangkat online dan konvergensi media menambah resiko ancaman digital, bagaimana kondisi kerentanan keamanan cyber serta sejauh mana pemahaman tentang ancaman tersebut menjadi masalah menarik untuk diteliti. Penelitian bertujuan untuk mengetahui kondisi literasi digital penggunaan media sosial di kalangan generasi millennial (Revilia, n.d.). Metode yang digunakan dalam penelitian ini adalah survey, wawancara dan observasi, analisis data kondisi literasi digital pada generasi milenial dilakukan menggunakan Technology Acceptance Model (TAM). Hasil penelitian ditemukan bahwa pengguna yang lebih lama menggunakan media sosial tidak mempengaruhi tingkat literasi media sosial. Pengguna yang pernah mengalami ancaman lebih menunjukkan kesadaran dengan meningkatkan level keamanan akun media sosial, dan lebih waspada sebelum mengizinkan akses ke perangkat pribadi. Individu yang lebih sadar akan pengaturan kata sandi umumnya memiliki tingkat kesadaran lebih tinggi tercermin dari niat mereka untuk berperilaku aman saat menggunakan media sosial. Persamaan penelitian ini adalah memiliki topik utama yang sama dengan focus pada kesadaran keamanan informasi dan privasi dalam konteks media sosial. Penelitian ini juga membahas tentang mahasiswa dan generasi milenial yang umumnya termasuk dalam rentang usia yang sama. Perbedaannya terletak dengan focus pada aspek praktis dalam lingkungan Pendidikan dan bagaimana mahasiswa tertentu mengelola keamanan informasi mereka di media sosial. Sedangkan penelitian yang saya lakukan lebih mengedepankan teori dan perspektif luas tentang bagaimana generasi milenial memahami dan menangani masalah keamanan dan privasi di media sosial

H. Hipotesis Penelitian

Hipotesis adalah dugaan sementara dalam penelitian. Adapun hipotesis dalam penelitian ini adalah:

H₀ : Terdapat pengaruh yang signifikan terhadap kesadaran dengan keamanan informasi

H_a : Tidak terdapat pengaruh terhadap tingkat kesadaran dengan keamanan informasi.



UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN