BAB II

KAJIAN TEORI

A. Media Sosial

Media sosial merupakan media berbasis daring yang memungkinkan penggunanya untuk berpartisipasi secara aktif, berbagi informasi, serta menciptakan berbagai bentuk konten, seperti blog, jejaring sosial, *wiki*, forum, dan dunia virtual. Di antara berbagai jenis media sosial tersebut, blog, jejaring sosial, dan *wiki* merupakan platform yang paling banyak dimanfaatkan oleh masyarakat di berbagai belahan dunia. Menurut Andreas Kaplan dan Michael Haenlein (2010), media sosial adalah sekelompok aplikasi berbasis internet yang dibangun berdasarkan ideologi dan teknologi *Web 2.0* sehingga memungkinkan pengguna untuk menciptakan serta saling bertukar konten yang dihasilkan oleh pengguna (*user-generated content*). Kehadiran teknologi *Web 2.0* memberikan kontribusi yang signifikan terhadap perkembangan media sosial karena mampu mendorong pertumbuhan dan pemanfaatannya secara lebih luas.

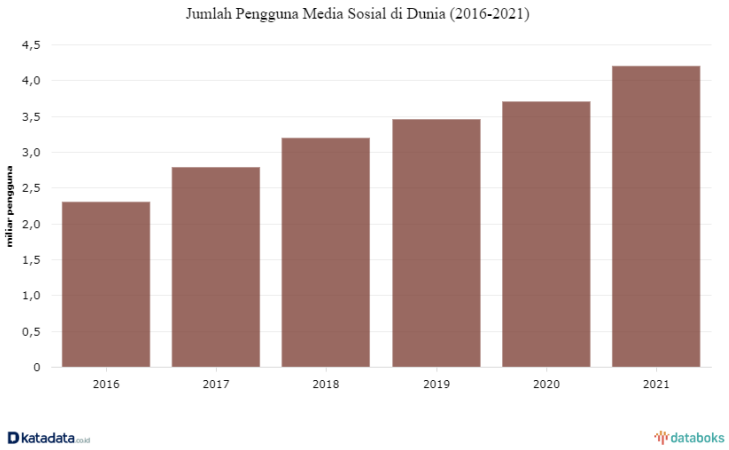
Media sosial merupakan media berbasis internet yang memungkinkan terjadinya interaksi sosial antarpengguna melalui pemanfaatan teknologi berbasis web yang mengubah pola komunikasi dari komunikasi satu arah menjadi komunikasi yang bersifat interaktif. Van Dijk (2013) dalam Nasrullah (2017) mendefinisikan media sosial sebagai platform digital yang berorientasi pada keberadaan pengguna serta memfasilitasi berbagai aktivitas dan kolaborasi di antara mereka. Dengan demikian, media sosial tidak hanya berfungsi sebagai sarana komunikasi, tetapi juga sebagai media yang memperkuat hubungan sosial antarindividu dalam lingkungan digital. Sementara itu, Shirky (2008) dalam Nasrullah (2017) menyatakan bahwa media sosial beserta perangkat lunak sosial merupakan sarana yang memungkinkan pengguna untuk berbagi informasi (*to share*), bekerja sama (*to cooperate*), dan melakukan berbagai tindakan secara kolektif di luar lingkup institusi maupun organisasi formal. Oleh karena itu, media sosial dapat dipahami sebagai ruang digital yang memberikan kesempatan kepada setiap individu untuk mengekspresikan diri, bertukar gagasan, menjalin kerja sama, membangun relasi, membentuk komunitas, serta berpartisipasi dalam berbagai aktivitas sosial sesuai dengan identitas dan karakteristik masing-masing pengguna.

Berdasarkan berbagai definisi yang telah dikemukakan, penggunaan media sosial dapat disimpulkan sebagai aktivitas yang dilakukan seseorang melalui platform berbasis internet untuk berbagi informasi, bertukar gagasan, mengembangkan kreativitas, menyampaikan pendapat, berdiskusi, serta membangun hubungan sosial dengan pengguna lainnya. Aktivitas tersebut umumnya dilakukan melalui berbagai aplikasi media sosial yang dapat diakses dengan mudah menggunakan perangkat digital, seperti *smartphone*.

Karjaluoto (2008) memaparkan bahwa sosial media ialah media yang memungkinkan setiap pengguna untuk berpartisipasi secara aktif serta memberikan kontribusi terhadap konten yang tersedia. Salah satu karakteristik utama media sosial adalah adanya keterbukaan dalam proses komunikasi yang memungkinkan terjadinya dialog antarpengguna. Selain itu, media sosial bersifat dinamis karena kontennya dapat diperbarui maupun dikembangkan, baik oleh pembuat platform maupun oleh komunitas pengguna pada media sosial tertentu. Dengan karakteristik tersebut, media sosial menghadirkan pola komunikasi baru yang lebih interaktif dan partisipatif.

Menurut Karjaluoto (2008), salah satu bentuk media sosial adalah jejaring sosial (*social networks*), yaitu komunitas virtual yang memungkinkan pengguna untuk membangun hubungan dan berinteraksi dengan pengguna lainnya. Beberapa platform jejaring sosial dirancang untuk memperluas jaringan pertemanan maupun profesional, seperti Facebook dan LinkedIn. Jejaring sosial merupakan salah satu jenis media sosial yang banyak dimanfaatkan karena mampu menghubungkan individu maupun organisasi berdasarkan kesamaan minat, profesi, atau hubungan sosial. Dengan demikian, jejaring sosial dapat dipahami sebagai suatu struktur sosial yang menghubungkan individu atau kelompok melalui berbagai bentuk relasi, mulai dari hubungan pertemanan, rekan kerja, hingga hubungan kekeluargaan.

B. Penggunaan Sosial Media



Gambar 2.1 Jumlah Pengguna Media Sosial Dunia

Sumber: https://databoks.katadata.co.id/

Berdasarkan data yang dipublikasikan oleh Databoks, YouTube menjadi platform media sosial yang paling banyak digunakan oleh masyarakat Indonesia dengan tingkat penggunaan mencapai 88%. Posisi berikutnya ditempati oleh WhatsApp dengan persentase penggunaan sebesar 84%, sedangkan Instagram dan Facebook masing-masing memiliki tingkat penggunaan sebesar 79%. Tingginya persentase penggunaan berbagai platform tersebut menunjukkan bahwa media sosial telah dimanfaatkan secara luas oleh masyarakat Indonesia dari berbagai kelompok usia, yaitu mulai dari 16 hingga 64 tahun, sehingga menjadikannya sebagai salah satu sarana utama dalam memperoleh informasi, berkomunikasi, dan berinteraksi di lingkungan digital..

C. Informasi

Menurut Susanto (2017), informasi merupakan hasil pengolahan data yang telah memiliki makna sehingga nantinya bermanfaat bagi pihak yang menerima. Sementara itu, Romney (2017) mendefinisikan informasi sebagai data yang telah diproses dan diolah sehingga memiliki arti serta dapat mendukung proses pengambilan keputusan. Agar dapat memberikan manfaat secara optimal, informasi harus memenuhi beberapa karakteristik sebagai berikut:

1. Relevan

   Informasi dikatakan relevan apabila mampu mengurangi tingkat ketidakpastian serta memberikan nilai tambah dalam proses pengambilan keputusan.

2. Reliabel

   Informasi yang reliabel merupakan informasi yang bebas dari kesalahan, bias, maupun distorsi sehingga mampu menggambarkan kondisi yang sebenarnya. Selain itu, informasi harus disusun berdasarkan data yang jujur, objektif, dan dapat dipercaya. Dalam konteks informasi keuangan, tingkat keandalannya umumnya dibuktikan melalui proses pemeriksaan atau verifikasi oleh pihak yang berwenang.

3. Lengkap

   Informasi disajikan haruslah mencakup seluruh aspek penting yang berkaitan dengan suatu peristiwa atau aktivitas sehingga mampu memenuhi kebutuhan pengguna. Penyajian informasi yang lengkap akan memudahkan pengguna dalam memahami isi informasi tanpa menimbulkan keraguan maupun kesalahpahaman.

4. Tepat waktu

   Informasi perlu tersedia pada waktu yang tepat sesuai dengan kebutuhan pengguna, terutama dalam proses pengambilan keputusan. Ketepatan waktu menjadi faktor yang sangat penting karena keterlambatan penyampaian informasi dapat menghambat proses pengambilan keputusan serta berpotensi menimbulkan kerugian.

5. Dapat dipahami

   Informasi disajikan dalam bentuk yang jelas, sistematis, dan mudah dipahami oleh para pengguna. Karakteristik ini mengharuskan informasi dapat dimengerti oleh individu yang memiliki pengetahuan yang memadai mengenai bidang terkait serta memiliki kemauan untuk mempelajari informasi tersebut secara waja.

6. Dapat diverifikasi

   Informasi yang berkualitas haruslah dapat dibuktikan kebenarannya melalui proses verifikasi. Suatu informasi dikatakan dapat diverifikasi apabila pihak-pihak yang memiliki kompetensi dan melakukan pemeriksaan secara independen memperoleh hasil yang sama, sehingga informasi tersebut dapat dipertanggungjawabkan.

7. Dapat diakses

   Informasi harus tersedia dan dapat diakses oleh pengguna pada saat dibutuhkan serta disajikan dalam format yang mudah digunakan. Kemudahan akses terhadap informasi akan mendukung efektivitas pemanfaatannya, khususnya dalam proses pengambilan keputusan.

D. Kesadaran

Zeman (2001) menjelaskan bahwa istilah *consciousness* berasal dari bahasa Latin, yaitu *conscio*, yang merupakan gabungan dari kata *cum* yang berarti *with* (dengan) dan *scio* yang berarti *know* (mengetahui). Secara etimologis, ungkapan *to be conscious of something* diartikan sebagai berbagi pengetahuan mengenai suatu hal dengan orang lain maupun dengan diri sendiri. Istilah *conscious* (sadar) dan *consciousness* (kesadaran) mulai digunakan dalam bahasa Inggris pada awal abad ke-17. Berdasarkan *Oxford English Dictionary* (OED), konsep kesadaran memiliki enam makna, yaitu:

1. pengetahuan yang dimiliki atau dipahami secara bersama;
2. pengetahuan atau keyakinan yang bersifat internal;
3. kondisi mental yang menunjukkan adanya kesadaran terhadap suatu objek atau keadaan (*awareness*);
4. kemampuan individu untuk menyadari tindakan maupun perasaannya sendiri (*direct awareness*);
5. kesatuan pribadi yang mencakup keseluruhan kesan, pikiran, dan perasaan yang membentuk pengalaman sadar; serta
6. keadaan individu yang berada dalam kondisi bangun atau terjaga secara normal.

Kesadaran menurut Freud (dalam Feist, 2010) merupakan segala sesuatu yang diterima melalui pancaindra dan tidak dipersepsikan sebagai ancaman sehingga berada dalam alam sadar (*conscious*). Freud menjelaskan bahwa alam sadar merupakan tingkat kehidupan mental yang dapat disadari dan dialami secara langsung oleh individu. Melalui peran ego, kesadaran memanfaatkan pengalaman-pengalaman pribadi yang tersimpan dalam alam bawah sadar sebagai dasar dalam membentuk serta memperkuat kepribadian seseorang. Sementara itu, Abraham Maslow melalui teori humanistiknya mengemukakan bahwa kesadaran adalah keadaan ketika individu mampu memahami dirinya sendiri, mengenali potensi yang

dimiliki, menyadari nilai-nilai yang dianut, memahami perasaan yang dialami, menentukan langkah yang perlu diambil, serta mengarahkan proses perkembangan dirinya.

Menurut KBBI, kesadaran diartikan sebagai keadaan seseorang yang memahami apa yang dirasakan atau dialaminya, serta memiliki pemahaman yang mendalam yang tercermin dalam pola pikir, sikap, dan perilaku yang mendukung perkembangan lingkungan. Berdasarkan berbagai definisi tersebut, dapat disimpulkan bahwa kesadaran merupakan kondisi ketika seseorang memiliki pemahaman terhadap dirinya maupun lingkungannya yang kemudian diwujudkan melalui sikap dan tindakan dalam kehidupan sehari-hari.

Antonio Gramsci (dalam Femia, 1983) menjelaskan bahwa kesadaran merupakan kemampuan individu dalam memahami situasi, kondisi, serta karakteristik masyarakat tempat ia hidup. Gramsci juga menekankan bahwa perubahan yang terjadi dalam diri seseorang akan memberikan pengaruh yang nyata terhadap perilaku yang ditampilkan.

E. Keamanan Informasi

KBBI sendiri mengistilahkan keamanan ber kata dasar aman, yang berarti keadaan bebas dari berbagai bentuk bahaya atau ancaman. Dalam konteks teknologi informasi, keamanan informasi merupakan serangkaian upaya yang dilakukan untuk melindungi informasi dari berbagai ancaman. (ISO/IEC 17799:2005). Konsep keamanan informasi dikenal dengan CIA Triad, yang terdiri atas tiga prinsip utama yang harus diterapkan dalam pengelolaan informasi, yaitu *Confidentiality* (kerahasiaan), *Integrity* (keutuhan), dan *Availability* (ketersediaan). Ketiga prinsip tersebut menjadi dasar dalam menjaga keamanan informasi agar tetap terlindungi dari berbagai bentuk ancaman maupun penyalahgunaan.

Gambar 2.2 Tiga Aspek Keamanan Informasi

Sumber: Cia Triad

1. *Confidentiality* (Kerahasiaan)

   Prinsip *confidentiality* menekankan bahwa informasi harus terlindungi dari akses oleh pihak yang tidak memiliki hak atau kewenangan. Penerapan prinsip ini bertujuan untuk memastikan bahwa hanya individu yang memiliki otorisasi yang dapat mengakses informasi tertentu. Salah satu upaya yang dapat dilakukan untuk menjaga kerahasiaan informasi adalah dengan menerapkan mekanisme enkripsi, sehingga informasi yang dikirimkan tetap aman dan hanya dapat dibaca oleh pihak yang berwenang.

2. *Integrity* (Integritas)

   Prinsip *integrity* mengharuskan informasi tetap terjaga keutuhan, keakuratan, dan konsistensinya serta tidak mengalami perubahan oleh pihak yang tidak berwenang. Untuk menjaga integritas informasi, organisasi umumnya menerapkan mekanisme pengendalian akses (*access control*) atau pembatasan hak akses, sehingga hanya pengguna tertentu yang memiliki izin untuk mengubah data, sedangkan pengguna lainnya hanya diberikan hak untuk melihat atau membaca informasi tersebut.

3. *Availability* (Ketersediaan)

   Prinsip *availability* memastikan bahwa informasi selalu tersedia dan dapat diakses oleh pengguna yang berhak ketika diperlukan. Untuk mendukung terpenuhinya prinsip ini, organisasi biasanya menerapkan sistem pencadangan (*backup*) data atau menyediakan media penyimpanan cadangan sebagai langkah antisipasi apabila terjadi gangguan maupun bencana pada sistem. Dengan demikian, informasi tetap dapat dipulihkan dan dimanfaatkan tanpa mengganggu kelangsungan operasional organisasi.

Keamanan informasi pada dasarnya merupakan serangkaian upaya untuk

mencegah terjadinya akses, penggunaan, pengungkapan, gangguan, perubahan, pemeriksaan, pencatatan, maupun penghancuran informasi oleh pihak yang tidak memiliki kewenangan. Menurut Puhakainen (2006), keamanan informasi dibangun atas tiga elemen utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Apabila salah satu dari ketiga elemen tersebut tidak terpenuhi, maka akan muncul kerentanan yang dapat mengancam keamanan informasi. Informasi merupakan aset yang memiliki nilai penting bagi individu maupun organisasi, sehingga keberadaannya perlu dilindungi melalui penerapan sistem keamanan yang memadai. Di sisi lain, perkembangan teknologi yang semakin pesat serta meningkatnya pemanfaatan teknologi dalam pengolahan informasi turut menimbulkan berbagai risiko keamanan. Selain itu, sistem informasi yang saat ini telah terintegrasi secara global menyebabkan setiap individu maupun organisasi yang berinteraksi, baik secara langsung maupun tidak langsung, dengan sistem informasi memiliki tanggung jawab untuk berperan aktif dalam menjaga keamanan informasi (Vardal, 2009)..

F. Kesadaran Keamanan Informasi

McLeod (2008), keamanan informasi bertujuan untuk menjamin terpenuhinya tiga prinsip utama, yaitu kerahasiaan (*confidentiality*), ketersediaan (*availability*), dan integritas (*integrity*) informasi. Sementara itu, Whitman dan Mattord (2011) mendefinisikan keamanan informasi sebagai serangkaian upaya yang dilakukan untuk melindungi informasi beserta seluruh elemen pendukungnya, termasuk sistem dan perangkat keras yang digunakan dalam proses penyimpanan, pengolahan, maupun penyebaran informasi.

Kruger (2006) menjelaskan bahwa kesadaran keamanan informasi merupakan pemahaman pengguna mengenai pentingnya menjaga keamanan informasi, kesadaran terhadap tanggung jawab pribadi, serta kemampuan untuk bertindak sesuai dengan kebijakan dan prosedur yang telah ditetapkan oleh organisasi. Selaras dengan pendapat tersebut, Furnell dan Clarke (2012) menyatakan bahwa aspek teknologi saja tidak cukup untuk menjamin terciptanya keamanan informasi yang optimal. Oleh karena itu, pengguna akhir (*end user*) memiliki peran yang sangat penting dalam mendukung penerapan keamanan informasi melalui perilaku yang sadar dan bertanggung jawab dalam menggunakan sistem informasi.

Secara keseluruhan, konsep kesadaran keamanan informasi dapat diringkas sebagai satu set pengetahuan, keterampilan, dan perilaku yang memberi pengguna tingkat TI yang sesuai dan pengetahuan keamanan informasi, keterampilan yang membangunnya dan memastikan penerapannya, dan perilaku yang sesuai yang muncul sebagai kebutuhan internal dan mengenali pentingnya keamanan informasi. (Legard, 2021).

Menurut Whitman dan Mattord (2011), *security awareness* merupakan serangkaian kebijakan atau mekanisme pengendalian yang dirancang untuk mengurangi terjadinya pelanggaran keamanan informasi, baik yang disebabkan oleh kelalaian maupun tindakan yang dilakukan secara sengaja. Sementara itu, Kruger (2006) mengembangkan konsep pengukuran kesadaran keamanan informasi berdasarkan teori psikologi sosial yang terdiri atas tiga komponen utama, yaitu *cognition*, *affection*, dan *behaviour*. Ketiga komponen tersebut selanjutnya dikembangkan menjadi tiga dimensi pengukuran, yaitu *knowledge* (pengetahuan), *attitude* (sikap), dan *behaviour* (perilaku).

1. *Knowledge* (pengetahuan)

   Dimensi *knowledge* mengacu pada tingkat pengetahuan individu mengenai keamanan informasi. Pengetahuan merupakan segala sesuatu yang diketahui atau dipahami oleh seseorang. Sementara itu, Notoatmodjo (2012) menjelaskan bahwa pengetahuan adalah hasil dari proses mengetahui yang diperoleh melalui proses pengindraan terhadap suatu objek tertentu. Pengetahuan memiliki peran penting dalam membentuk kemampuan individu untuk memahami dan menerapkan keamanan informasi dalam kehidupan sehari-hari. Menurut Notoatmodjo (2012), tingkat pengetahuan terdiri atas enam tingkatan, yaitu:

   a. Tahu

      Tingkat *tahu* menunjukkan kemampuan seseorang untuk mengingat kembali informasi atau materi yang telah dipelajari. Kemampuan ini berkaitan dengan proses mengenali dan mengingat fakta, konsep, maupun informasi yang pernah diterima sebelumnya.

   b. Memahami

      Kemampuan individu untuk menjelaskan kembali suatu konsep atau objek dengan benar serta mampu menginterpretasikan informasi yang diperoleh

secara tepat, termasuk memberikan contoh yang sesuai.

c. Aplikasi

Aplikasi adalah kemampuan untuk menerapkan pengetahuan, konsep, metode, maupun prinsip yang telah dipelajari ke dalam situasi atau kondisi nyata sehingga dapat dimanfaatkan dalam penyelesaian suatu permasalahan.

d. Analisis

Analisis merupakan kemampuan untuk menguraikan suatu materi atau objek ke dalam bagian-bagian yang lebih kecil serta mengidentifikasi hubungan antarbagian tersebut. Kemampuan ini tercermin dari kemampuan seseorang dalam membedakan, mengelompokkan, membandingkan, maupun menjelaskan suatu informasi secara lebih rinci.

e. Sintesis

Kemampuan untuk menggabungkan berbagai unsur atau informasi menjadi suatu konsep atau bentuk baru yang utuh. Kemampuan ini mencakup aktivitas menyusun, merancang, merumuskan, maupun mengembangkan suatu gagasan berdasarkan informasi yang telah dimiliki.

f. Evaluasi

Kemampuan dalam menilai suatu objek, konsep, atau informasi berdasarkan kriteria tertentu, baik yang ditetapkan sendiri maupun yang telah ditentukan sebelumnya. Penilaian tersebut dilakukan sebagai dasar dalam menentukan kualitas, ketepatan, maupun efektivitas suatu objek atau tindakan.

2. *Attitude* (sikap)

Attitude atau sikap merupakan kecenderungan individu dalam merespons maupun bertindak ketika berinteraksi dan berkomunikasi dengan orang lain. Sukardi (dalam Munandar, 2016), sikap diartikan sebagai kesiapan individu untuk memberikan respons terhadap situasi atau objek tertentu. Sejalan dengan pendapat tersebut, Notoatmodjo (2012) menyatakan bahwa sikap ialah bentuk kesiapan atau kesediaan individu untuk melakukan sesuatu, namun belum diwujudkan dalam tindakan nyata. Menurut Azwar (2015), sikap terdiri atas tiga komponen utama, yaitu:

a. *Kognitif*

Komponen kognitif berkaitan dengan pengetahuan, pemahaman, serta

informasi yang dimiliki individu mengenai suatu objek. Informasi tersebut kemudian diproses sehingga menjadi dasar dalam membentuk cara berpikir dan menentukan keputusan atau respons terhadap objek yang dihadapi.

b. *Afektif*

Komponen afektif berhubungan dengan aspek emosional, yaitu perasaan atau penilaian subjektif individu terhadap suatu objek. Dalam kajian psikologi, aspek afektif mencerminkan bagaimana seseorang menyukai, tidak menyukai, menerima, atau menolak suatu objek berdasarkan perasaan yang dimilikinya.

c. *Konatif*

Komponen konatif menggambarkan kecenderungan individu untuk bertindak atau berperilaku terhadap suatu objek. Komponen ini menunjukkan adanya niat atau dorongan yang memengaruhi tindakan seseorang sebagai respons terhadap situasi yang dihadapinya.

Berdasarkan berbagai pendapat tersebut, dapat disimpulkan bahwa sikap merupakan kecenderungan respons individu terhadap suatu objek yang berpotensi memengaruhi perilakunya. Sikap tidak bersifat bawaan, melainkan dapat berkembang dan berubah melalui proses belajar serta pengalaman yang diperoleh dari lingkungan sekitar.

3. *Behaviour* (perilaku)

Menurut Walgito (2010), perilaku merupakan respons yang muncul sebagai akibat adanya suatu stimulus, di mana setiap individu memiliki kemampuan untuk menentukan bentuk respons atau tindakan yang akan dilakukan. Selanjutnya, Skinner (dalam Walgito, 2010) mengelompokkan perilaku ke dalam dua jenis, yaitu:

a. Perilaku Alami

Perilaku alami (*innate behaviour*) adalah perilaku yang telah dimiliki individu sejak lahir dan muncul secara alami tanpa melalui proses pembelajaran. Bentuk perilaku ini umumnya berupa refleks maupun insting yang terjadi secara otomatis sebagai respons terhadap stimulus tertentu.

b. Perilaku Operan

Perilaku operan ialah perilaku yang terbentuk melalui proses belajar dan pengalaman yang diperoleh individu selama menjalani kehidupan. Perilaku ini berkembang sebagai hasil interaksi dengan lingkungan, sehingga dapat mengalami perubahan sesuai dengan pengalaman, pembiasaan, maupun proses pembelajaran yang diterima.

Penelitian oleh Mattord dan Whitman (2012) menunjukkan bahwa salah satu program yang paling jarang diterapkan, namun memiliki manfaat yang sangat besar, adalah program kesadaran keamanan (*security awareness program*). Program ini ditujukan guna meningkatkan dan mempertahankan kesadaran pengguna terhadap pentingnya keamanan informasi dalam setiap aktivitas yang dilakukan. Penerapan program kesadaran keamanan tidak harus bersifat kompleks maupun memerlukan biaya yang besar. Program tersebut dapat diwujudkan melalui berbagai media, seperti buletin, poster, video edukasi, papan informasi, pamflet, maupun berbagai media promosi lainnya. Selain itu, penggunaan media pendukung, seperti alas tetikus (*mouse pad*), cangkir, kaus, pena, atau perlengkapan kerja lainnya yang memuat slogan keamanan informasi juga dapat dimanfaatkan sebagai sarana untuk mengingatkan pengguna akan pentingnya menjaga keamanan informasi. Agar program tersebut berjalan secara efektif, diperlukan individu atau tim yang memiliki komitmen untuk mengelola, mengembangkan, serta mempromosikan program secara berkelanjutan, termasuk menyediakan dukungan sumber daya yang diperlukan. Penyebaran informasi mengenai keamanan kepada karyawan melalui media cetak, *e-mail*, maupun *intranet* merupakan salah satu cara yang relatif efisien dalam meningkatkan kesadaran keamanan informasi. Tujuan utama dari program ini adalah menanamkan pentingnya keamanan informasi dalam pola pikir pengguna sehingga mereka terdorong untuk lebih peduli terhadap berbagai risiko keamanan. Sebaliknya, apabila program kesadaran keamanan tidak dijalankan secara konsisten, pengguna cenderung mengabaikan aspek keamanan informasi yang pada akhirnya dapat meningkatkan risiko terjadinya kesalahan, kecelakaan, maupun pelanggaran keamanan dalam organisasi.

Kruger melakukan pengukuran pada ketiga dimensi ini di 7 area 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*)

Dimensi tersebut merupakan komponen utama yang nantinya akan membentuk sebuah kesadaran individu dalam hal melindungki keamanan informasinya, kemudian mengembangkan pemahaman serta membentuk sikap terhadap pengetahuan yang dimiliki, dan selanjutnya menerapkannya dalam perilaku sehari-hari. Proses tersebut diharapkan mampu meningkatkan kesadaran individu dalam melindungi informasi pribadi sehingga memberikan dampak positif terhadap keamanan aktivitas digital yang dilakukan. Selanjutnya, Kruger dan Kearney (2006) mengelompokkan kesadaran keamanan informasi ke dalam beberapa level of awareness sebagai berikut.

Tabel 2.1 *Level Of Awareness*

Awareness	Measurements (%)
Good	**80 – 100**
Average	**60 – 79**
Poor	**59 and less**

Level of awareness tersebut dibedakan ke dalam tiga kategori, yaitu *good* (baik), *average* (sedang), dan *poor* (buruk). Pertama, kategori *good* menunjukkan tingkat kesadaran keamanan informasi yang baik, yaitu apabila memperoleh nilai ≥80%. Pada tingkat ini, pengetahuan mengenai keamanan informasi (*knowledge*) telah dipahami melalui sikap (*attitude*) dan diterapkan dalam perilaku sehari-hari (*behaviour*). Kedua, kategori *average* menunjukkan tingkat kesadaran keamanan informasi yang berada pada kisaran ≥60% hingga <80%. Tingkat ini mengindikasikan bahwa salah satu dari tiga aspek kesadaran keamanan informasi, yaitu pengetahuan, sikap, atau perilaku, belum terpenuhi secara optimal. Ketiga, kategori *poor* menunjukkan tingkat kesadaran keamanan informasi yang rendah,

yaitu apabila memperoleh nilai <60%. Pada tingkat ini, pengetahuan mengenai keamanan informasi yang diperoleh belum dapat dipahami dengan baik sehingga tidak memengaruhi sikap maupun perilaku individu dalam menerapkan keamanan informasi dalam kehidupan sehari-hari.

G. Konsep Umum Keamanan Informasi

Menurut Chan dan Mubarak (dalam Mukhlis, 2014), terdapat beberapa konsep dasar keamanan informasi yang penting untuk dipahami, yaitu sebagai berikut:

1. *Phishing*

Phishing diartikan sebagai usaha seseorang dalam mencuri informasi rahasia atau identitas seseorang dengan memanfaatkan *e-mail* maupun situs web palsu yang dirancang menyerupai alamat *e-mail* atau situs resmi. Selain menggunakan media digital, *phishing* juga dapat dilakukan melalui teknik nonteknis, seperti *social engineering*, maupun dikombinasikan dengan *spam* sebagai sarana untuk mengelabui korban. Ancaman ini berkaitan erat dengan aspek kerahasiaan (*confidentiality*) dalam keamanan informasi, sehingga setiap individu perlu memahami karakteristik serta risiko yang ditimbulkannya.

2. SPAM

Spam adalah pesan elektronik yang dikirim tanpa persetujuan penerima dan umumnya bersifat komersial atau tidak diinginkan. Keberadaan *spam* tidak hanya mengganggu pengguna, tetapi juga berpotensi membahayakan sistem informasi karena dapat mengandung virus berbahaya. Ancaman tersebut dapat menurunkan kinerja sistem, menghambat akses pengguna, bahkan melanggar aspek ketersediaan (*availability*) informasi. Selain itu, *spam* sering kali menyisipkan tautan yang mengarah ke situs *phishing*. Meskipun organisasi telah menerapkan berbagai mekanisme penyaringan *spam*, perlindungan tersebut tidak selalu mampu mencegah seluruh ancaman. Oleh sebab itu, pemahaman pengguna mengenai *spam* dan dampaknya menjadi bagian penting dalam mendukung keamanan informasi.

3. *Social Engineering*

Social engineering merupakan teknik yang memanfaatkan pendekatan nonteknis untuk memperoleh informasi rahasia atau melakukan pencurian identitas. Dalam praktiknya, pelaku menggunakan manipulasi psikologis, penyamaran identitas, maupun berbagai bentuk rekayasa sosial lainnya agar korban secara sukarela

memberikan informasi yang bersifat rahasia.

4. *Strong Password*

Strong password atau kata sandi yang kuat berfungsi sebagai mekanisme autentikasi pengguna sekaligus mencegah akses oleh pihak yang tidak berwenang. Selain melalui *social engineering* dan *phishing*, kata sandi juga dapat diperoleh secara ilegal menggunakan teknik *password cracking*. Tingkat keamanan sebuah kata sandi ditentukan oleh tingkat kesulitan dan lamanya waktu yang dibutuhkan untuk memecahkannya. Semakin kompleks kombinasi kata sandi yang digunakan, maka semakin kecil peluang keberhasilan serangan. Oleh karena itu, pengguna perlu memiliki kesadaran untuk membuat kata sandi yang kuat dengan memadukan huruf, angka, simbol, serta jumlah karakter yang memadai agar keamanan akun dapat terjaga.

5. *Data or Information Integrity*

Diartikan sebagai aspek yang bertujuan menjaga keutuhan serta keakuratan informasi. Beberapa karakteristik integritas data dan informasi meliputi:

a. Akurasi dan kebenaran, yaitu informasi harus apa adanya yang mana sesuai dengan kondiri rill sehingga data yang tersimpan bebas dari kesalahan.
b. Kepercayaan, yaitu informasi yang terdapat dalam sistem harus dapat dipercaya karena mencerminkan keadaan yang sesungguhnya.
c. Keberlakuan dan ketepatan waktu, yaitu informasi harus tetap relevan, mutakhir, serta disesuaikan dengan perubahan kondisi yang terjadi sehingga nilainya tetap terjaga

6. *Social Networking*

Media sosial atau *social networking* berpotensi menjadi sumber kebocoran informasi apabila pengguna membagikan data pribadi. Makanya, penggunaan media sosial sangat perlu menjadi bagian dari kebijakan keamanan informasi dalam suatu organisasi. Meningkatkan kesadaran pengguna terhadap berbagai risiko yang terdapat pada media sosial merupakan langkah penting untuk mencegah terjadinya penyalahgunaan maupun kebocoran informasi.

H. Teknik Pengamanan Informasi

Pengamanan informasi merupakan langkah penting yang harus dilakukan untuk melindungi aset informasi yang dimiliki oleh seseorang. Menurut Ariyus

(2009), terdapat beberapa teknik yang dapat diterapkan dalam menjaga keamanan informasi, yaitu:

1. Membatasi akses terhadap informasi melalui penggunaan *username* dan *password* maupun autentikasi biometrik; serta (
2. Menerapkan teknik *cryptography* (kriptografi) dan *steganography* (steganografi) sebagai metode untuk melindungi informasi dari akses yang tidak berwenang.

Sementara itu, Romney dan Steinbart (2015) menjelaskan bahwa kata sandi (*password*) yang kuat memiliki beberapa karakteristik, yaitu:

1. *Length,* yaitu kata sandi sebaiknya memiliki jumlah karakter yang cukup panjang karena semakin panjang kata sandi, semakin tinggi tingkat keamanannya.
2. *Multiple character types,* yaitu menggunakan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus untuk meningkatkan kompleksitas kata sandi.
3. *Randomness,* yaitu kata sandi disusun secara acak sehingga tidak mudah ditebak maupun ditemukan dalam kamus.
4. *Changed frequently,* yaitu kata sandi perlu diperbarui secara berkala, umumnya setiap 30 hari - 90 hari.
5. *Keep secret,* yaitu kata sandi harus dijaga kerahasiaannya serta tidak dibagikan kepada pihak yang tidak memiliki kewenangan untuk mengakses informasi tersebut.

I. Penelitian Terdahulu

Penelitian berjudul ***"Pengukuran Kesadaran Keamanan Informasi dan Privasi dalam Bersosial Media"*** yang dilakukan oleh Hendro Gunawan dan diterbitkan dalam *Jurnal Muara Sains, Teknologi, Kedokteran, dan Ilmu Kesehatan* pada tahun 2021 bertujuan untuk menganalisis tingkat kesadaran mahasiswa generasi milenial terhadap keamanan informasi dan privasi dalam penggunaan media sosial. Objek penelitian ini adalah mahasiswa Program Studi Sistem Informasi Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta. Pengumpulan data dilakukan melalui penyebaran kuesioner kepada responden. Hasil penelitian menunjukkan bahwa mahasiswa memiliki tingkat pemahaman yang tinggi mengenai pentingnya keamanan informasi dengan persentase sebesar 85%. Namun,

perilaku mereka belum sepenuhnya mencerminkan praktik keamanan informasi yang baik, seperti tidak melakukan pergantian kata sandi secara berkala (75%) serta masih sering mengakses media sosial menggunakan jaringan publik yang tingkat keamanannya belum dapat dipastikan. Dari aspek privasi, sebagian mahasiswa masih mencantumkan informasi pribadi pada media sosial, memiliki akun yang bersifat terbuka untuk umum (40,6%), serta belum memanfaatkan pengaturan privasi secara optimal (54,9%), sehingga informasi penting yang dimiliki masih berpotensi diakses oleh pihak lain (Hendro, 2021:1–8). Persamaan penelitian yaitu terletak pada fokus kajian, yang sama-sama mengukur tingkat kesadaran mahasiswa terhadap keamanan informasi dalam penggunaan media sosial serta menggunakan pendekatan penelitian kuantitatif. Adapun perbedaannya terletak pada variabel yang diteliti dan karakteristik responden.

Penelitian yang dilakukan oleh Nahier Aldhafferi, Charles Watson, dan A.S.M. Sajeev pada tahun 2013 dengan judul ***Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices, yang dipublikasikan dalam International Journal of Security, Privacy and Trust Management,*** bertujuan untuk mengukur tingkat kesadaran pengguna terhadap risiko kebocoran informasi pribadi pada media sosial. Dalam penelitian tersebut, responden diberikan beberapa pertanyaan mengenai praktik penggunaan informasi pribadi pada akun media sosial mereka. Hasil penelitian menunjukkan bahwa sekitar 66% responden merasa khawatir terhadap potensi penyalahgunaan informasi pribadi yang mereka bagikan di media sosial. Selain itu, sebanyak 69% responden menyatakan tidak menginginkan informasi pribadi mereka dapat diakses oleh orang yang tidak dikenal. Penelitian ini juga mengungkap bahwa 35% responden mengetahui penyedia layanan media sosial membagikan informasi profil mereka kepada situs web lain. Temuan tersebut menunjukkan perlunya pengembangan mekanisme yang memberikan kendali kepada pengguna untuk menentukan apakah informasi pribadi mereka dapat dibagikan atau tidak kepada pihak lain. Di sisi lain, hasil penelitian memperlihatkan bahwa sebagian besar pengguna telah menunjukkan sikap yang lebih berhati-hati dalam menerima permintaan pertemanan dari orang yang tidak dikenal. Sebanyak 71% responden mengaku pernah menerima permintaan pertemanan dari orang asing, sedangkan

68% di antaranya memilih untuk menolak permintaan tersebut (Nahier dkk., 2013). Adapun persamaannya ialah, kedua penelitian sama-sama mengukur tentang kesadaran responden terhadap keamanan informasi nya dalam menggunakan media online dan metode yang digunakan pada kedua penelitian ini adalah kuantitatif. Adapun perbedaannya ada pada fokus penggunaan media online yang digunakan yaitu pada penelitian sebelumnya berfokus pada media sosial dan situs web, sedangkan pada penelitian saat ini berfokus pada media sosial saja.

Penelitian yang berjudul ***"Analisis Kesadaran Cybersecurity pada Pengguna Media Sosial di Indonesia"*** merupakan skripsi yang disusun oleh Muhammad Rifqi Ramadhani pada tahun 2020. Hasil penelitian menunjukkan adanya perbedaan yang signifikan dalam tingkat kesadaran terhadap *cybersecurity* di kalangan pengguna media sosial di Indonesia. Perbedaan tersebut dipengaruhi oleh karakteristik responden, khususnya usia dan domisili. Selain itu, penelitian ini juga menemukan bahwa dari berbagai platform media sosial yang dianalisis, YouTube memiliki pengaruh paling besar terhadap tingkat kesadaran *cybersecurity*. Temuan tersebut ditunjukkan oleh nilai *p-value* yang lebih kecil dibandingkan platform media sosial lainnya serta nilai koefisien regresi yang bersifat positif. Hal ini mengindikasikan bahwa semakin tinggi intensitas penggunaan YouTube, maka semakin tinggi pula tingkat kesadaran pengguna terhadap keamanan siber (Rifqi, 2020). Persamaan penelitian yang dilakukan penulis adalah sama-sama mengukur tingkat kesadaran mahasiswa akan keamanan informasinya dan juga metode yang digunakan adalah metode kuantitatif. Perbedaanya ada pada fokus media yang digunakan yaitu pada penelitian sebelumnya berfokus pada keamanan informasi dalam penggunaan internet secara menyeluruh sedangkan pada penelitian saat ini berfokus pada keamanan informasi dalam bersosial media. Populasi dan sampel yang digunakan juga berbeda yaitu mahasiswa prodi Akuntansi Sanata Dharma dengan mahasiswa Fakultas Ilmu Sosial UIN Sumatera Utara. Hasil penelitian sebelumnya menunjukkan tingkat kesadaran yang baik sedangkan hasil penelitian saat ini menunjukkan tingkat kesadaran sedang.

Penelitian yang berjudul ***"Keamanan Informasi Data Pribadi pada Media Sosial"*** yang dilakukan oleh Mesra Bety dan Mahyuddin K. M. Nasution serta

dipublikasikan dalam *Jurnal Informatika Kaputama (JIK)* pada tahun 2022 membahas pentingnya perlindungan data pribadi dalam penggunaan media sosial. Penelitian ini menggunakan metode studi kepustakaan (*library research*) dengan mengkaji berbagai literatur yang berkaitan dengan keamanan informasi pada media sosial. Hasil penelitian menunjukkan bahwa terdapat enam aspek utama yang perlu diperhatikan dalam penggunaan sistem aplikasi berbasis daring yang berkaitan dengan privasi data, yaitu keamanan dan perlindungan data, kesadaran pengguna, pengaturan kontrol, manajemen risiko, transparansi, serta etika. Selain itu, penelitian ini menekankan pentingnya membangun kepercayaan pengguna melalui perancangan layanan internet yang berorientasi pada kebutuhan pengguna (*user priority*). Pengguna juga perlu diberikan keleluasaan untuk menentukan mekanisme pengendalian terhadap informasi pribadi yang akan diungkapkan maupun dimanfaatkan oleh pihak lain. (Mesra Betty dkk, 2022). Persamaan pada penelitian sebelumnya dengan penelitian saat ini ialah sama meneliti tentang keamanan informasi data pribadi pada media sosial dengan menggunakan metode yang sama pula yaitu kuantitatif. Perbedaannya yaitu, pada penelitian sebelumnya tidak berfokus pada pengukuran tingkat kesadaran tetapi lebih ke pemahaman tentang keamanan informasi itu sendiri.

J. Hipotesis Penelitian

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

H_0 : Terdapat pengaruh antara tingkat kesadaran dengan keamanan informasi.

H_a : Tidak ada pengaruh antara tingkat kesadaran dengan keamanan informasi