BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi telah mendorong munculnya berbagai inovasi, salah satunya adalah perkembangan media sosial sebagai sarana komunikasi digital. Kehadiran media sosial memberikan beragam kemudahan bagi penggunanya, terutama dalam proses penyebaran dan pencarian informasi yang dapat dilakukan secara cepat, mudah, dan tanpa batas ruang maupun waktu. Peningkatan jumlah pengguna media sosial di Indonesia juga dipengaruhi oleh semakin memadainya infrastruktur dan fasilitas akses internet yang tersedia bagi masyarakat.

Di sisi lain, penggunaan media sosial tidak terlepas dari berbagai risiko yang berkaitan dengan keamanan informasi. Pengguna sering kali belum mengetahui secara pasti tingkat keamanan aplikasi media sosial yang digunakan, mengingat pertukaran data melalui internet berpotensi menimbulkan ancaman terhadap kerahasiaan, integritas, maupun keamanan informasi pribadi. Oleh karena itu, setiap pengguna perlu meningkatkan kewaspadaan serta menerapkan langkah tepat dalam melindungi keamanan informasi selama beraktivitas di media sosial. Seiring dengan pesatnya perkembangan teknologi informasi, khususnya pada saluran komunikasi berbasis internet, masyarakat kini semakin dimudahkan dalam melakukan komunikasi secara efektif dan efisien..

Data yang dipublikasikan oleh *We Are Social* bersama APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) menunjukkan bahwa jumlah pengguna internet di Indonesia pada Januari 2022 mencapai 204,7 juta orang. Jumlah tersebut mengalami pertumbuhan sebesar 1,03% dibanding tahun sebelumnya yaitu 202,6 juta orang pengguna internet di Januari 2021. Dalam lima tahun terakhir, penggunaan internet di Indonesia terus mengalami peningkatan yang signifikan. Bahkan, jika dibandingkan dengan tahun 2018, jumlah pengguna internet telah bertambah sebesar 54,25%.

Meningkatnya jumlah pengguna internet turut tercermin dari tingkat penetrasi internet yang mencapai 73,7% dari total populasi Indonesia pada awal tahun 2022. Pada periode tersebut, jumlah penduduk Indonesia tercatat sebanyak

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

277,7 juta jiwa. Kondisi ini menunjukkan bahwa sebagian besar masyarakat telah memiliki akses terhadap internet sehingga pemanfaatannya semakin meluas dalam berbagai aspek kehidupan.

Tingginya akses internet berbanding lurus dengan meningkatnya aktivitas penggunaan media sosial. Rata-rata masyarakat Indonesia menghabiskan waktu sekitar 3 jam 26 menit setiap hari untuk mengakses media sosial melalui berbagai jenis perangkat digital. Selain itu, kelompok usia 18–34 tahun merupakan segmen yang paling dominan dalam penggunaan media sosial di Indonesia.

Sementara itu, laporan *Digital 2022: Indonesia* yang diterbitkan oleh *DataReportal* mencatat bahwa jumlah pengguna media sosial di Indonesia pada Januari 2022 mencapai 191,4 juta orang. Angka tersebut meningkat sebanyak 21 juta pengguna atau sekitar 12,6% dibandingkan tahun 2021. Jika dibandingkan dengan jumlah penduduk Indonesia yang mencapai 277,7 juta jiwa, maka pengguna media sosial telah mencakup sekitar 68,9% dari total populasi. Data tersebut menunjukkan bahwa media sosial telah menjadi salah satu platform digital yang digunakan secara luas oleh masyarakat Indonesia dalam mendukung aktivitas komunikasi, pertukaran informasi, maupun interaksi sosial.

Meskipun jumlah pengguna aktif media sosial di Indonesia terus mengalami peningkatan, kondisi tersebut belum diikuti oleh tingkat literasi digital masyarakat yang memadai. Fenomena ini tercermin dalam hasil survei Litbang Kompas yang dilaksanakan pada akhir Januari 2022. Berdasarkan survei yang melibatkan 1.014 responden yang tersebar di 34 provinsi, diperoleh temuan bahwa hampir separuh responden belum memiliki kesadaran mengenai pentingnya perlindungan data pribadi dalam menjalankan aktivitas di ruang digital.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Hasil survei tersebut menunjukkan bahwa sebanyak 46,5% responden belum memahami maupun menyadari bahwa berbagai aktivitas yang dilakukan secara daring, seperti menjelajahi internet (*browsing*), berbelanja secara online, serta menggunakan media sosial, menghasilkan data yang bernilai dan perlu dijaga keamanannya. Temuan ini mengindikasikan bahwa peningkatan penggunaan media digital belum sepenuhnya diimbangi dengan pemahaman masyarakat mengenai pentingnya keamanan informasi dan perlindungan data pribadi.

Berdasarkan data yang dipublikasikan oleh Databoks, YouTube merupakan platform media sosial yang paling banyak digunakan oleh masyarakat Indonesia dengan tingkat penggunaan mencapai 88%. Posisi berikutnya ditempati oleh WhatsApp dengan persentase pengguna sebesar 84%, sedangkan Instagram dan Facebook masing-masing memiliki tingkat penggunaan sebesar 79%. Data tersebut menunjukkan bahwa berbagai platform media sosial memiliki tingkat pemanfaatan yang tinggi di kalangan masyarakat Indonesia.

Tingginya tingkat penggunaan media sosial tersebut mengindikasikan bahwa internet telah menjadi bagian penting dalam kehidupan sehari-hari masyarakat. Selain jumlah penggunanya yang terus meningkat, karakteristik pengguna media sosial di Indonesia juga sangat beragam, mencakup kelompok usia mulai dari 16 hingga 64 tahun. Kondisi ini menunjukkan bahwa media sosial telah dimanfaatkan oleh berbagai lapisan masyarakat sebagai sarana untuk berkomunikasi, memperoleh informasi, maupun memenuhi kebutuhan sosial dan aktivitas lainnya..

Media sosial telah berkembang menjadi salah satu sarana komunikasi digital yang memiliki pengaruh besar dalam kehidupan masyarakat. Platform ini memberikan kemudahan bagi pengguna untuk membuat, mengakses, serta menyebarluaskan berbagai bentuk konten secara cepat dan luas. Seiring dengan pesatnya perkembangan media sosial, isu mengenai keamanan informasi dan perlindungan privasi semakin menjadi perhatian karena tingginya intensitas pertukaran data yang terjadi melalui platform tersebut.

Dalam perkembangannya, media sosial juga kerap menjadi salah satu media yang berpotensi menyebabkan kebocoran informasi yang bersifat rahasia. Kemajuan internet dan media sosial memberikan berbagai manfaat bagi masyarakat, seperti mempermudah komunikasi dan penyebaran informasi. Namun, di balik manfaat tersebut terdapat berbagai risiko yang perlu diwaspadai, terutama yang berkaitan dengan keamanan informasi dan penyalahgunaan data pribadi.

Sebagai bagian dari *World Wide Web*, media sosial memiliki berbagai kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Salah satu permasalahan yang sering muncul adalah penyebaran informasi pribadi oleh pengguna lain ke ruang publik tanpa persetujuan pemilik data. Menurut Kontaxis

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

(2011), pelanggaran privasi di media sosial dapat didorong oleh berbagai motif, seperti penyebaran gosip, pencemaran nama baik, maupun tindakan membagikan berita, foto, dan video secara tidak bertanggung jawab. Oleh karena itu, pengguna media sosial perlu memiliki kesadaran yang tinggi terhadap pentingnya menjaga keamanan informasi serta melindungi privasi dalam setiap aktivitas digital yang dilakukan. Hal ini sebagaimana disampaikan dalam QS Al-Hujurat: 49 ayat 6yaitu:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْٓا اِنْ جَاۤءَكُمْ فَاسِقٌۢ بِنَبَاٍ فَتَبَيَّنُوْٓا اَنْ تُصِيْبُوْا قَوْمًاۢ بِجَهَالَةٍ فَتُصْبِحُوْا عَلٰى مَا فَعَلْتُمْ نٰدِمِيْنَ ٢

"Wahai orang-orang yang beriman! Jika seseorang yang fasik datang kepadamu membawa suatu berita, maka telitilah kebenarannya, agar kamu tidak mencelakakan suatu kaum karena kebodohan (kecerobohan), yang akhirnya kamu menyesali perbuatanmu itu."(QS Al-Hujurat: 49/6).

Media sosial mempermudah masyarakat untuk menjangkau audiens yang lebih luas serta memfasilitasi berbagai aktivitas, seperti memperoleh informasi, membangun interaksi sosial, dan menyampaikan pengaruh kepada pengguna lainnya. Namun, di balik berbagai manfaat tersebut, media sosial juga membuka peluang terjadinya pelanggaran privasi serta ancaman terhadap keamanan data pribadi akibat tingginya intensitas pertukaran informasi di ruang digital.

Generasi Z merupakan kelompok yang sangat akrab dengan teknologi digital dan memiliki karakteristik sebagai generasi yang senantiasa terhubung (*always connected*) dengan internet. Intensitas penggunaan berbagai platform digital serta kebiasaan berbagi informasi melalui beragam perangkat yang saling terintegrasi menjadikan kelompok ini lebih rentan terhadap berbagai ancaman keamanan siber. Aktivitas tersebut dapat meningkatkan risiko penyalahgunaan data pribadi apabila tidak disertai dengan kesadaran dan penerapan praktik keamanan informasi yang memadai.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Oleh karena itu, tingkat kerentanan keamanan siber yang dihadapi Generasi Z serta pemahaman mereka mengenai berbagai bentuk ancaman keamanan informasi menjadi isu yang penting untuk dikaji. Penelitian mengenai aspek tersebut diperlukan untuk mengetahui sejauh mana kesadaran keamanan informasi telah dimiliki oleh Generasi Z, sehingga dapat menjadi dasar dalam upaya meningkatkan perlindungan terhadap data pribadi dan keamanan aktivitas digital..

Perkembangan teknologi informasi dan komunikasi (TIK) telah menjadikan berbagai aktivitas manusia semakin bergantung pada pemanfaatan sistem digital. Ketergantungan tersebut tidak hanya dirasakan oleh individu, tetapi juga oleh organisasi maupun pemerintah dalam menjalankan aktivitas dan memberikan layanan. Di sisi lain, kondisi tersebut turut meningkatkan risiko terhadap berbagai ancaman keamanan siber, seperti peretasan (*hacking*), kejahatan siber (*cybercrime*), terorisme siber (*cyberterrorism*), serta berbagai bentuk serangan lainnya yang menargetkan sistem informasi.

Meskipun ancaman keamanan informasi terus berkembang, masih banyak individu maupun organisasi yang belum memiliki kesiapan yang memadai dalam mengantisipasi maupun menghadapi berbagai bentuk serangan tersebut. Oleh sebab itu, pemerintah memiliki peran strategis dalam mewujudkan keamanan informasi melalui pengembangan infrastruktur teknologi informasi dan komunikasi serta penyelenggaraan sistem perlindungan yang mampu mengurangi risiko ancaman terhadap aset informasi.

Semakin meningkatnya nilai informasi sebagai aset yang penting menyebabkan tingginya upaya berbagai pihak untuk memperoleh maupun menguasai informasi, termasuk melalui cara-cara yang melanggar hukum. Kondisi tersebut mendorong individu maupun organisasi untuk menerapkan berbagai langkah pengamanan guna mencegah terjadinya akses ilegal, penyalahgunaan informasi, serta meminimalkan dampak yang ditimbulkan apabila terjadi insiden keamanan. Upaya-upaya tersebut merupakan bagian dari penerapan keamanan informasi (*information security*).

Penerapan keamanan informasi bertujuan untuk memastikan bahwa prinsip-prinsip utama keamanan informasi, yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*), tetap terpelihara. Terjaganya ketiga aspek tersebut sangat penting agar proses operasional organisasi dapat berlangsung secara efektif tanpa mengalami gangguan. Sebaliknya, kegagalan dalam menerapkan pengamanan informasi dapat menimbulkan berbagai konsekuensi, seperti hilangnya kepercayaan masyarakat atau pelanggan, terganggunya aktivitas organisasi, hingga menimbulkan kerugian yang berdampak serius terhadap keberlangsungan suatu institusi.

Generasi Z merupakan kelompok yang lahir pada rentang tahun 1981–2000 dan dikenal sebagai generasi yang tumbuh bersamaan dengan perkembangan teknologi digital. Tingginya intensitas penggunaan internet serta kebiasaan memanfaatkan berbagai perangkat yang saling terhubung menyebabkan generasi ini lebih rentan terhadap ancaman keamanan siber. Karakteristik tersebut, terutama dalam aktivitas berbagi data melalui berbagai platform digital, berpotensi meningkatkan risiko penyalahgunaan informasi pribadi. Oleh karena itu, tingkat pemahaman Generasi Z terhadap kerentanan keamanan siber serta kesadaran mereka mengenai berbagai bentuk ancaman digital menjadi topik yang penting untuk dikaji.

Persepsi seseorang terhadap keamanan informasi juga dipengaruhi oleh pengalaman yang pernah dialami dalam menggunakan teknologi digital. Zhang dan Gupta (2016) menjelaskan bahwa pengguna yang pernah menjadi korban pencurian identitas (*identity theft*) maupun *cyberbullying* cenderung memiliki tingkat kesadaran, persepsi keamanan, dan kepercayaan yang berbeda dibandingkan dengan pengguna yang belum pernah mengalami kejadian serupa. Hal tersebut menunjukkan bahwa pengalaman terhadap insiden keamanan siber dapat memengaruhi perilaku pengguna dalam melindungi informasi pribadinya.

Dalam kehidupan sehari-hari, ancaman keamanan informasi dapat terjadi melalui berbagai bentuk aktivitas digital. Sebagai contoh, seorang mahasiswa dapat mengalami kehilangan atau kerusakan data akademik akibat infeksi *malware* maupun virus yang berasal dari penggunaan media penyimpanan eksternal, seperti *flashdisk*, tanpa terlebih dahulu dilakukan pemindaian menggunakan perangkat lunak antivirus. Kondisi tersebut dapat mengakibatkan terganggunya akses terhadap data dan informasi yang berkaitan dengan kegiatan perkuliahan.

Selain itu, praktik *phishing* juga menjadi salah satu ancaman yang banyak dijumpai di lingkungan digital. *Phishing* merupakan upaya memperoleh informasi rahasia atau mencuri identitas dengan memanfaatkan situs web maupun surat elektronik palsu yang dibuat menyerupai layanan resmi. Salah satu modus yang sering ditemukan adalah pengiriman tautan yang menawarkan hadiah atau promosi atas nama suatu merek tertentu. Ketika tautan tersebut diakses oleh pengguna, korban akan diarahkan ke halaman yang menyerupai situs asli sehingga pelaku

dapat memperoleh data pribadi, seperti nama pengguna, kata sandi, maupun informasi penting lainnya.

Meningkatnya penggunaan akses internet melalui jaringan nirkabel, baik yang bersifat berbayar maupun layanan *Wi-Fi* publik yang tersedia di berbagai fasilitas umum, seperti bandara, stasiun kereta api, dan pusat perbelanjaan, juga berpotensi meningkatkan risiko kebocoran informasi apabila pengguna tidak menerapkan langkah-langkah keamanan yang memadai. Di samping itu, surat elektronik (*email*) masih menjadi salah satu media yang sering dimanfaatkan oleh pelaku kejahatan siber untuk menyebarkan *malware*, mengirimkan lampiran yang mengandung virus, maupun melakukan pencurian kredensial pengguna melalui berbagai teknik rekayasa sosial (*social engineering*). Kondisi tersebut menunjukkan bahwa peningkatan penggunaan teknologi digital harus diimbangi dengan kesadaran dan pemahaman yang baik mengenai keamanan informasi agar berbagai risiko yang mungkin terjadi dapat diminimalkan.

Berdasarkan laporan Global Cybersecurity Index 2017 yang diterbitkan oleh *International Telecommunication Union* (ITU), Indonesia menempati peringkat ke-70 dari 165 negara dalam indeks keamanan siber global. Posisi tersebut menunjukkan bahwa upaya peningkatan kapasitas keamanan siber di Indonesia masih perlu terus dikembangkan agar mampu menghadapi berbagai ancaman yang semakin kompleks di era digital.

Selain itu, hasil pengukuran Digital Civility Index yang dilakukan oleh Microsoft pada periode April–Mei 2020 juga menggambarkan tantangan yang dihadapi masyarakat Indonesia dalam beraktivitas di ruang digital. Penelitian tersebut melibatkan 16.000 responden dari 32 negara, termasuk Indonesia. Berdasarkan hasil pengukuran tersebut, Indonesia berada pada peringkat ke-29 dengan skor 76. Dalam indeks tersebut, semakin tinggi nilai yang diperoleh, semakin rendah tingkat keberadaban digital masyarakat, sehingga hasil tersebut menunjukkan masih perlunya peningkatan kesadaran dan etika dalam penggunaan teknologi digital.

Data dari Badan Siber dan Sandi Negara (BSSN) turut memperlihatkan tingginya ancaman keamanan siber di Indonesia. Sepanjang periode Januari hingga Agustus 2021, tercatat lebih dari 888,7 juta insiden serangan siber. Jumlah tersebut

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

terus meningkat hingga mencapai sekitar 1,6 miliar serangan pada akhir tahun 2021. Selain itu, BSSN juga melaporkan terdapat 5.574 kasus peretasan yang terjadi sepanjang tahun 2021.

Berbagai data tersebut mengindikasikan bahwa Indonesia masih menghadapi tantangan yang cukup besar dalam aspek keamanan siber. Tingginya jumlah serangan siber serta rendahnya tingkat keberadaban digital menunjukkan bahwa kesadaran masyarakat mengenai pentingnya keamanan informasi dan perlindungan data pribadi masih perlu ditingkatkan. Oleh karena itu, diperlukan berbagai upaya edukasi dan peningkatan literasi keamanan siber agar masyarakat mampu mengenali, mencegah, serta mengurangi risiko yang ditimbulkan oleh berbagai ancaman di ruang digital.

Perkembangan teknologi informasi dan internet turut memengaruhi aktivitas digital mahasiswa Fakultas Ilmu Sosial, termasuk dalam aspek keamanan informasi. Intensitas penggunaan perangkat digital dan berbagai layanan berbasis internet menjadikan mahasiswa sebagai salah satu kelompok yang perlu memiliki pemahaman yang baik mengenai pentingnya melindungi informasi pribadi maupun data yang berkaitan dengan institusi. Oleh karena itu, kesadaran keamanan informasi menjadi aspek yang sangat penting dalam mendukung penggunaan teknologi secara aman dan bertanggung jawab.

Kesadaran keamanan informasi dapat diartikan sebagai tingkat pengetahuan, pemahaman, dan kemampuan seseorang dalam menerapkan praktik-praktik keamanan ketika memanfaatkan internet maupun media digital. Kesadaran tersebut mencakup kemampuan untuk mengenali potensi ancaman, menjaga kerahasiaan data pribadi, serta melindungi informasi yang dimiliki individu maupun organisasi selama beraktivitas di ruang digital.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Salah satu faktor yang berkontribusi terhadap terjadinya pelanggaran keamanan informasi dan privasi adalah rendahnya kesadaran pengguna dalam menerapkan praktik keamanan saat menggunakan perangkat *smartphone*. Meskipun sebagian pengguna telah memiliki pengetahuan mengenai cara penggunaan perangkat yang aman, pengetahuan tersebut sering kali belum diimplementasikan secara konsisten dalam aktivitas sehari-hari. Kondisi ini

menunjukkan adanya ketimpangan antara tingkat pengetahuan dengan perilaku oengguna dalam melindungi keamanan informasinya.

Selain itu, masih ditemukan berbagai perilaku yang berpotensi meningkatkan risiko kebocoran data di kalangan mahasiswa, seperti menggunakan jaringan *Wi-Fi* publik tanpa memperhatikan aspek keamanannya serta membagikan kata sandi (*password*) kepada orang lain tanpa pertimbangan yang memadai. Tindakan-tindakan tersebut dapat membuka peluang bagi pihak yang tidak bertanggung jawab untuk memperoleh akses terhadap informasi pribadi maupun data penting. Oleh karena itu, diperlukan peningkatan kesadaran keamanan informasi agar mahasiswa mampu menerapkan perilaku digital yang lebih aman serta meminimalkan risiko terjadinya pelanggaran keamanan informasi.

Perkembangan teknologi informasi pada era digital telah mendorong transformasi berbagai layanan perpustakaan ke dalam lingkungan siber (*cyberspace*). Perubahan tersebut tidak hanya memberikan kemudahan dalam pengelolaan dan penyebaran informasi, tetapi juga menghadirkan tantangan baru terkait keamanan informasi. Dalam konteks ini, perpustakaan dituntut untuk menjaga tiga aspek utama keamanan informasi, yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi agar layanan dan koleksi digital tetap terlindungi.

Seiring dengan meningkatnya pemanfaatan teknologi digital, ancaman terhadap keamanan informasi di perpustakaan juga semakin beragam. Ancaman tersebut dapat berupa infeksi *malware*, pencurian data, akses tidak sah terhadap sistem, hingga berbagai bentuk serangan siber lainnya yang berpotensi mengganggu operasional perpustakaan. Sumber ancaman tidak hanya berasal dari pihak eksternal, tetapi juga dapat muncul dari faktor internal, seperti kesalahan pengguna, lemahnya pengelolaan sistem, maupun kelalaian dalam menerapkan prosedur keamanan informasi.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Berbagai ancaman tersebut pada dasarnya bersifat potensial, namun dapat berkembang menjadi insiden keamanan yang nyata apabila kelemahan pada perangkat keras, perangkat lunak, infrastruktur fisik, maupun proses bisnis tidak segera diidentifikasi dan diperbaiki. Oleh karena itu, penerapan sistem keamanan informasi yang komprehensif menjadi langkah penting untuk meminimalkan risiko

terjadinya gangguan terhadap layanan perpustakaan serta melindungi aset informasi yang dimiliki.

Risiko kejahatan siber juga menjadi perhatian serius karena pelaku sering kali sulit untuk diidentifikasi maupun ditindak, sementara dampak yang ditimbulkan dapat menyebabkan kerugian yang besar bagi institusi. Salah satu contoh serangan siber yang pernah menjadi perhatian dunia adalah penyebaran *ransomware WannaCry*, yaitu jenis *malware* yang mengenkripsi file pada perangkat korban sehingga data tidak dapat diakses kembali tanpa proses pemulihan tertentu. Serangan tersebut telah menyebar secara luas dan menginfeksi berbagai organisasi di puluhan negara, termasuk Indonesia, sehingga menjadi salah satu bukti nyata pentingnya penerapan keamanan informasi dalam melindungi sistem dan aset digital.

Pesatnya perkembangan teknologi informasi dan komunikasi telah memberikan kontribusi yang signifikan terhadap pengelolaan aset informasi di perpustakaan. Pemanfaatan teknologi tersebut diwujudkan melalui berbagai layanan berbasis digital, seperti sistem informasi perpustakaan, sistem pengelolaan koleksi, serta sistem penyebaran informasi kepada pengguna. Melalui penerapan sistem informasi, berbagai aset informasi perpustakaan dapat dikelola secara lebih efektif dan didistribusikan kepada pemustaka dengan memanfaatkan teknologi digital.

Namun, optimalisasi pemanfaatan teknologi informasi perlu diimbangi dengan penerapan keamanan informasi yang memadai. Keamanan informasi tidak dapat terwujud secara otomatis, melainkan memerlukan komitmen dan kesadaran dari seluruh unsur organisasi, khususnya pengelola perpustakaan, dalam melindungi aset informasi dari berbagai ancaman.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

Menurut Franindya (2014:2), keamanan informasi dapat ditinjau berdasarkan tiga prinsip utama, yaitu ketersediaan (*availability*), keutuhan (*integrity*), dan kerahasiaan (*confidentiality*). Prinsip *availability* menekankan bahwa informasi harus dapat diakses oleh pihak yang memiliki hak akses. Prinsip *integrity* mengharuskan informasi tetap utuh, akurat, dan tidak mengalami perubahan oleh pihak yang tidak berwenang. Sementara itu, prinsip *confidentiality*

bertujuan untuk memastikan bahwa aset informasi hanya dapat diakses oleh pihak yang memiliki otorisasi sehingga kerahasiaannya tetap terjaga.

Berdasarkan uraian latar belakang tersebut, peneliti tertarik untuk melakukan penelitian dengan judul **"Pengukuran Tingkat Kesadaran terhadap Keamanan Informasi Mahasiswa Ilmu Perpustakaan Universitas Islam Negeri Sumatera Utara dalam Bersosial Media".**

B. Rumusan Masalah

1. Bagaimana tingkat kesadaran informasi mahasiswa FIS UIN Sumatera Utara Dalam Bersosial Media?
2. Bagaimana tingkat keamanan informasi mahasiswa FIS UIN Sumatera Utara Dalam Bersosial Media?
3. Bagaimana pengaruh tingkat keamanan terhadap tingkat kesadaran informasi mahasiswa FIS UIN Sumatera Utara Dalam Bersosial Media?

C. Tujuan Penelitian

1. Untuk mengetahui tingkat kesadaran informasi mahasiswa FIS UIN Sumatera Utara Dalam Bersosial Media
2. Untuk mengetahui tingkat keamanan informasi mahasiswa FIS UIN Sumatera Utara Dalam Bersosial Media
3. Untuk mengetahui pengaruh tingkat keamanan terhadap tingkat kesadaran informasi mahasiswa FIS UIN Sumatera Utara Dalam Bersosial Media?

D. Manfaat Penelitian

1. Bagi Mahasiswa Fakultas Ilmu Sosial penelitian ini diharapkan dapat memberikan konstribusi ilmu pengetahuan bagi kajian akan keamanan informasinya dalam bersosial media
2. Bagi para dosen dan *civitas akademika* penelitian ini diharapkan menjadi referensi dalam menjaga keamanan informasi pada saat mengakses sosial medianya.
3. Bagi peneliti lain harapannya dapat dijadikan referensi dan pembanding untuk penelitian mendatang dengan topik yang sama.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

E. Sistematika Penulisan

BAB I Pendahuluan : Bab ini memuat uraian mengenai latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan. Penyajian pada bab ini bertujuan untuk memberikan gambaran secara ringkas, sistematis, dan jelas mengenai permasalahan yang melatarbelakangi dilaksanakannya penelitian.

BAB II Kajian Teori : Bab ini berisi landasan teori yang menjadi dasar dalam penelitian. Mengenai keamanan informasi, berbagai fenomena yang berkaitan dengan keamanan informasi, serta teori-teori yang menjelaskan tingkat kesadaran terhadap keamanan informasi sebagai acuan dalam menganalisis permasalahan penelitian.

BAB III Metodologi Penelitian : Bab ini menjelaskan metode yang digunakan dalam penelitian, meliputi lokasi dan waktu penelitian, populasi dan sampel, definisi operasional variabel, hipotesis penelitian, teknik pengumpulan data, serta teknik analisis data yang digunakan untuk menjawab rumusan masalah penelitian.

BAB IV Hasil dan Pembahasan : Bab ini menyajikan hasil penelitian yang diperoleh dari proses pengumpulan dan pengolahan data, disertai pembahasan mengenai tingkat kesadaran keamanan informasi pada mahasiswa Fakultas Ilmu Sosial UIN Sumatera Utara berdasarkan hasil analisis yang telah dilakukan.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN

BAB V Penutup : Bab ini memuat kesimpulan yang disusun berdasarkan hasil penelitian serta pembahasan yang telah dilakukan. Selain itu, bab ini juga menyajikan saran-saran yang diharapkan dapat menjadi masukan bagi pihak-pihak terkait maupun sebagai bahan pertimbangan untuk penelitian selanjutnya.