

BAB 2

TINJAUAN PUSTAKA

2.1 Landasan Teori

Penjelasan yang komprehensif mengenai dasar-dasar teori perlu disampaikan untuk mempermudah pemahaman terkait dengan permasalahan penelitian. Dalam konteks ini, dijelaskan secara rinci mengenai teori-teori yang digunakan dan diterapkan dalam penelitian ini.

2.2.1 Konsep Pemahaman

Pemahaman dapat diartikan sebagai penyerapan dari suatu pengajaran atau materi (Suryani, 2019). Pemahaman dalam Bahasa Indonesia berasal dari kata dasar paham, paham memiliki makna sebagai pengetahuan yang luas mengenai suatu hal sedangkan pemahaman merujuk pada proses memahami suatu masalah atau situasi. (Radiusman, 2020). Pemahaman adalah kemampuan untuk menghubungkan atau mengaitkan setiap informasi yang dipelajari sehingga membentuk gambaran yang lengkap dan jelas di dalam pikiran (Widiasworo, 2017). Adapun pemahaman menurut Sudaryono (2009) merupakan kemampuan seseorang untuk memahami makna atau arti dari materi yang dipelajari, yang dapat tercermin dalam kemampuan merangkum inti dari sebuah bacaan atau mengubah informasi dari satu format ke format lain.

Tingkat pemahaman seseorang terhadap suatu masalah sangat terkait dengan pemikiran pribadi setiap individu (Radiusman, 2020). Pemahaman adalah proses dimana seseorang menghubungkan informasi baru dengan pengetahuan lama yang dimiliki melalui koneksi antara fakta-fakta (Faye, 2014). Menurut

Taksonomi Bloom pemahaman termasuk kategori ranah kognitif level 2 setelah pengetahuan (Nafiati, 2021). Pernyataan tersebut memiliki arti bahwa pemahaman tidak hanya sebatas mengetahui, melainkan juga kemampuan seseorang untuk menggunakan atau menerapkan apa yang telah dipahami. Dari penjelasan tersebut, dapat disimpulkan bahwa pemahaman mengacu pada kapasitas seseorang untuk mengerti suatu konsep atau topik. Seseorang dikatakan paham ketika dapat menjelaskan informasi yang diperoleh dan dapat mengaplikasikan atau menggunakan apa yang telah dipahami.

Tingkatan pemahaman seseorang menurut Andreson dan Karthwol (Suryani, 2019) adalah sebagai berikut:

1. Menafsirkan (*interpreting*)

Penafsiran merupakan kemampuan seseorang untuk mengubah informasi yang didapat dari bentuk satu ke bentuk yang lainnya. Misalnya dari kata ke angka maupun sebaliknya.

2. Memberikan contoh (*exemplifying*)

Exemplifying adalah kemampuan seseorang untuk dapat memberikan contoh yang berkaitan dengan konsep secara umum.

3. Mengklasifikasikan (*classifying*)

Classifying merupakan kemampuan seseorang untuk mengetahui bahwa sesuatu merupakan bagian dari suatu kategori. *Classifying* juga dapat diartikan bahwa seseorang dapat mengetahui sesuatu merupakan bagian dari suatu kategori.

4. Meringkas (*summarizing*)

Seseorang dapat dikatakan paham apabila dapat memberikan pernyataan tunggal yang dapat menyatakan informasi yang disampaikan secara umum.

5. Menarik inferensi (*inferring*)

Inferring diartikan sebagai mencari pola dari beberapa contoh kasus.

Seseorang dapat dikatakan paham apabila dapat membayangkan konsep atau prinsip dengan cara mengkode karakteristik suatu konsep.

6. Membandingkan (*comparing*)

Seseorang dapat dikatakan paham apabila mampu mencari hubungan antara dua ide, objek atau hal lain yang serupa.

7. Menjelaskan (*explaining*)

Seseorang dapat dikatakan paham apabila mampu mengkontruksi ulang atau menjelaskan ulang sebab dan akibat dari suatu konsep.

Pemahaman sendiri dapat dibedakan menjadi tiga kategori menurut Sudjana (2009), yaitu:

1. Tingkat pemahaman terendah melibatkan interpretasi terjemahan, yang mencakup pemahaman makna teks, interpretasi, dan penerapan prinsip-prinsip tertentu.
2. Tingkat kedua adalah pemahaman penafsiran, di mana seseorang dapat mengaitkan informasi sebelumnya dengan pengetahuan yang sudah dimiliki untuk menghasilkan pemahaman yang lebih mendalam.
3. Tingkat ketiga melibatkan pemahaman ekstrapolasi, yang mengacu pada kemampuan seseorang untuk menafsirkan makna teks dan membuat

kesimpulan yang terkait dengan implikasi dan konsekuensi yang mungkin terjadi.

Dari uraian diatas dapat diketahui bahwa pemahaman merupakan proses menyerap makna dari materi tertentu atau kemampuan seseorang untuk memahami makna dari suatu konsep. Seseorang dianggap memahami ketika mampu memberikan penjelasan atau deskripsi yang komprehensif tentang sesuatu dengan menggunakan bahasa sendiri (Suryani, 2019).

2.2.2 Konsep Privasi Informasi

Privasi adalah hak dasar yang berkaitan dengan upaya untuk menghindari penggunaan kekuasaan yang tidak sah dan tidak diinginkan, dengan cara meminimalkan informasi yang dapat diketahui dan tindakan yang dapat diambil terhadap diri seseorang (Rahmatullah, 2017). Privasi merupakan hal yang sangat signifikan bagi setiap individu karena pada prinsipnya, setiap individu memiliki bagian dari kehidupannya yang ingin dijaga kerahasiaannya dan menginginkan perlindungan terhadap privasi pribadinya. (Anggara, 2015).

Salah satu dimensi privasi menurut Carina B. Paine Schofield dan Adam N. Joinson adalah privasi informasi, privasi informasi dapat dijelaskan sebagai keputusan mengenai seberapa jauh informasi tentang seorang individu akan diungkapkan kepada pihak lain atau organisasi tertentu, istilah ini mencakup berbagai jenis data, seperti informasi keuangan, catatan medis, dan sebagainya. (Rahmatullah, 2017). Privasi informasi menurut Liliana (2021) berkaitan dengan data pribadi yang biasanya disimpan pada sistem komputer, dan sering juga disebut sebagai privasi data. Informasi pribadi meliputi berbagai macam data yang terkait dengan seorang individu, seperti nama, kontak, minat, atribut fisik, status

kesehatan, dan segala hal lain yang dapat digunakan untuk mengidentifikasi individu tersebut (Iman et al., 2020).

Informasi bisa menjadi personal karena informasi tersebut dimiliki oleh seseorang, tentang seseorang dan mengarah kepada seseorang (William, 2012). Selanjutnya William (2012) mengelompokkan informasi pribadi menjadi enam yaitu, informasi milik saya, ditujukan kepada saya, dikirim atau diterbitkan oleh saya, dialami oleh saya, dan relevan bagi saya. Informasi pribadi mencakup fakta yang bersifat sangat pribadi atau sensitif tentang seorang individu, sehingga individu tersebut memiliki keinginan untuk menjaga atau membatasi akses orang lain terhadap pengumpulan, penggunaan, atau penyebaran informasi tersebut (Nurrokhmah, 2016). Kategorisasi informasi pribadi menurut Kwon, et al (2006) dalam matriks sensitivitas privasi dimana terdapat empat kategori informasi pribadi yaitu:

1. Informasi yang pengungkapannya dianggap tidak disetujui, seperti catatan pendidikan dan jejak penelusuran web.
2. Informasi yang pengungkapannya terbuka untuk umum seperti tanggal lahir, tempat lahir, jenis kelamin atau pekerjaan.
3. Informasi yang dapat digunakan dalam pencurian identitas mencakup nomor pengenal pribadi seperti nomor telepon dan nomor jaminan sosial.
4. Informasi yang berpotensi mengarah pada orang tertentu seperti nama lengkap, alamat email, ciri fisik, dan wajah.

Dari pendapat ahli diatas dapat disimpulkan bahwa privasi informasi adalah sesuatu yang berkaitan dengan usaha individu untuk melindungi data maupun informasi yang dimilikinya agar tidak diketahui orang lain. Salah satu dimensi

privasi informasi adalah informasi pribadi, dimana informasi pribadi disini diartikan sebagai semua informasi yang berkaitan dengan seseorang termasuk didalamnya nama, yang dimaksud nama disini terdiri dari nama lengkap maupun nama orang tua, kontak termasuk nomor telepon dan sosial media, hobi, ciri fisik, dan segala hal yang dapat mengidentifikasi seseorang.

2.2.3 Social Media Privacy Concern

Social media privacy concern atau masalah keamanan pada media sosial dapat didefinisikan sebagai kekhawatiran *user* media sosial tentang seberapa aman informasi pribadi *user* terhadap masalah pencurian identitas (informasi pribadi), peniruan atau *phising* sosial, dan pembajakan dengan tanpa sepengetahuan *user* tersebut (Zhang & Gupta, 2016). Penelitian tentang privasi informasi pribadi pertama kali ditemukan oleh Smith, Milberg dan Burke pada tahun 1996 dengan model *Global Information Privacy Concern* (GIPC), penelitian ini masih menjelaskan privasi informasi secara umum. Selanjutnya dikembangkan oleh Stewart dan Seagaras pada tahun 2002 dengan pengembangan *model Concern for Information Privacy* (CFIP) yang memformulasikan dimensi pembentuk atas privasi informasi pribadi dengan *collection, error, unauthorized, secondary used*, dan *improper acces*. Kemudian Malhotra, Kim dan Agarwal pada tahun 2004 mengemukakan model *Internet Users Information Privacy Concern* (IUIPC) yang memperbaharui dimensi terkait *awareness of privacy practice* (Kusyanti et al., 2017).

Hong dan Thong (2013) mengartikan masalah privasi internet sebagai seberapa besar kekhawatiran pengguna internet tentang praktik-praktik situs web yang berkaitan dengan pengumpulan dan penggunaan informasi pribadi. Seseorang

yang memiliki privasi yang tinggi cenderung tidak mempercayai situs web untuk mengelola informasinya dan sebaliknya seseorang dengan privasi yang tinggi lebih cenderung merasa riskan untuk mengungkapkan informasi pribadinya ke situs web. Adapun menurut Dinev dan Hart (2005) *internet privacy concern* merupakan kekhawatiran individu tentang kemungkinan hilangnya privasi karena pengungkapan informasi secara sukarela atau diam-diam ke situs web.

Koohang et al (2018) berpendapat bahwa temuan tentang masalah privasi di internet juga berlaku di situs media sosial maka dari itu dibangun model penelitian *social media privacy concern* diadaptasi dari *Internet privacy Concern* milik Hong dan Thong. Koohang et al (2018) menjelaskan enam dimensi masalah privasi internet untuk menggambarkan secara spesifik tentang privasi pengguna. Enam dimensi tersebut sebagai berikut.

1. Pengumpulan (*collection*)

Pengumpulan yang dimaksud disini adalah pengumpulan informasi yang dikumpulkan oleh *platform* media sosial. Dimensi ini berusaha mendefinisikan pengumpulan informasi oleh *platform* media sosial. Konsep pengumpulan dalam konteks ini merujuk pada seberapa besar kekhawatiran seseorang terhadap berapa banyak informasi pribadi yang dikumpulkan oleh media sosial. Masalah privasi atas konstruksi koleksi kemudian dikaji ke dalam tiga item variabel berikut:

- a. *Platform* media sosial meminta pengguna untuk memberikan informasi.
- b. Pengguna berpikir dua kali untuk memberikan informasi.
- c. *Platform* media sosial mengumpulkan informasi pengguna secara umum.

2. Penggunaan sekunder (*secondary usage*)

Informasi pribadi pengguna yang dikumpulkan oleh situs media sosial untuk satu tujuan, namun digunakan, tanpa izin dari pengguna untuk tujuan lainnya. Dimensi ini berusaha melihat seberapa jauh seseorang khawatir tentang penggunaan informasi yang dimilikinya digunakan secara tidak wajar untuk tujuan selain dari tujuan awal. Masalah penggunaan sekunder ini dikaji dalam tiga item variabel berikut:

- a. *Platform* media sosial menyimpan informasi pengguna untuk tujuannya.
- b. *Platform* media sosial menyimpan informasi pengguna untuk dijual ke pihak lain.
- c. *Platform* media sosial membagikan informasi pengguna tanpa izin pengguna.

3. Kesalahan (*errors*)

Perlindungan yang tidak memadai terhadap kesalahan yang disengaja dan/atau tidak disengaja pada data pribadi pengguna yang dikumpulkan oleh situs media sosial. Dimensi ini berusaha melihat sejauh mana seseorang khawatir tentang kesalahan yang disengaja maupun tidak disengaja yang terjadi pada informasi pribadinya. Dimensi ini kemudian dikaji dalam tiga item variabel sebagai berikut:

- a. *Platform* media sosial memastikan keakuratan informasi pengguna.
- b. *Platform* media sosial memiliki prosedur yang memadai untuk memperbaiki informasi pengguna yang tidak akurat.
- c. *Platform* media sosial menghabiskan waktu dan upaya untuk memverifikasi keakuratan informasi pengguna.

4. Akses yang tidak tepat (*Improper access*)

Informasi pribadi pengguna yang disimpan oleh *platform* media sosial tersedia untuk orang lain atau dapat diakses oleh orang lain. Dimensi ini berusaha melihat sejauh mana seseorang merasa khawatir tentang informasi pribadinya yang bisa saja diakses oleh orang lain. Dimensi ini kemudian dikaji kedalam tiga item variabel, yakni:

- a. *Platform* media sosial berusaha melindungi pengguna dari akses tidak sah yang dapat merugikan pengguna.
- b. *Platform* media sosial mencurahkan waktu dan upaya untuk mencegah aksesn yang tidak tepat ke akun pengguna.
- c. *Platform* media sosial mengambil langkah-langkah untuk mencegah akses yang tidak tepat ke akun pengguna.

5. Kontrol (*control*)

Kontrol yang tidak memadai atas informasi pribadi yang disimpan oleh situs media sosial. Dimensi ini mencoba melihat sejauh mana seseorang mempunyai kendali atas bagaimana informasinya digunakan. Dimensi ini kemudian dikaji dalam tiga variabel berikut ini:

- a. Pengguna memiliki kendali atas informasi apa yang diberikan ke *platform* media sosial.
- b. Pengguna memiliki kendali atas keputusan bagaimana informasi pribadi akan digunakan oleh *platform* media sosial.
- c. Hilang atau berkurangnya kendali pengguna karena informasi digunakan oleh *platform* media sosial untuk tujuan tertentu.

6. Kesadaran (*awareness*)

Kesadaran mengacu pada kombinasi tiga aspek yakni, literasi dalam elemen yang berkaitan dengan privasi informasi, seperti teknologi, peraturan, atau praktik umum yang digunakan oleh media sosial untuk mengumpulkan, menggunakan, dan berbagi informasi pengguna. Selanjutnya, pemahaman bahwa unsur-unsur tersebut ada pada lingkungan saat ini dan menyadari dampaknya di masa depan. Dimensi ini mencoba melihat sejauh mana informasinya di ekspos. Dimensi ini dikaji menggunakan tiga item variabel berikut:

- a. Pengguna tidak mengetahui kebijakan yang ditetapkan oleh *platform* media sosial.
- b. Pengguna tidak menyadari bagaimana informasi pribadi digunakan oleh *platform* media sosial.
- c. Pengguna tidak menyadari bagaimana informasi pribadi dikumpulkan, diproses, dan digunakan oleh *platform* media sosial.

2.2.4 Privasi Informasi dan Media Sosial

Privasi informasi dan media sosial merupakan dua hal yang saling terikat namun seringkali bertentangan. Media sosial merupakan sarana individu untuk berkomunikasi dengan individu lainnya secara tidak langsung melalui suatu *platform* (Islamy, et al., 2018). Media sosial memungkinkan individu untuk terhubung, berbagi, dan berinteraksi secara luas dengan orang lain secara *online*, namun pada saat yang sama hal ini juga menghadirkan tantangan besar terkait ancaman privasi informasi (Cahyono, 2017). Pengguna media sosial seringkali tidak sadar atau terpaksa memberikan informasi pribadi mereka kepada *platform*

media sosial, baik melalui profil pribadi, aktivitas *online* maupun interaksi dengan konten (Rahmawati, et al., 2023). Hal ini dapat meningkatkan risiko privasi, karena informasi yang dibagikan dapat diakses oleh pihak ketiga, termasuk oknum yang tidak bertanggung jawab. Konsep privasi informasi di media sosial juga kompleks karena sifatnya yang dinamis dan berubah-ubah, di mana pengguna harus terus mempertimbangkan antara kenyamanan dalam berbagi informasi dan perlindungan terhadap potensi penyalahgunaan.

Social Media Privacy Concern mengacu pada kekhawatiran pengguna media sosial terkait dengan cara suatu organisasi atau instansi mengelola kebijakan yang dapat berdampak keamanan dari informasi data pribadi pengguna (Mohamed & Ahmad, 2012). Kekhawatiran ini disebabkan karena aktivitas seperti pencurian informasi pribadi, *cyber stalking*, *blackmail*, dan *spam* yang melibatkan informasi pribadi seseorang (D., 2019). Pelanggaran keamanan data pribadi dapat mengakibatkan dampak tidak hanya dari sisi finansial pengguna, hal ini juga berpotensi merusak reputasi mereka di mata masyarakat (Rahmawati, et al., 2023). Oleh karena itu, diperlukan pemahaman terhadap masalah privasi informasi terutama di media sosial agar pengguna dapat membuat keputusan yang lebih bijaksana dalam berbagi informasi pribadi mereka. Dengan pemahaman yang lebih baik tentang risiko dan konsekuensi dari pembagian informasi, pengguna dapat mengambil langkah-langkah untuk melindungi privasi mereka sendiri, seperti mengatur pengaturan privasi yang lebih ketat atau mengurangi jumlah informasi pribadi yang dibagikan secara online.

2.3 Penelitian Sejenis Sebelumnya

Penelitian sebelumnya dapat digunakan sebagai referensi untuk membantu membentuk gambaran tentang bagaimana merancang penelitian yang akan dilakukan selanjutnya. Beberapa penelitian sebelumnya digunakan sebagai pendukung penelitian.

Penelitian pertama berjudul “Pengukuran Kesadaran Keamanan Informasi dan Privasi dalam Sosial Media” yang diteliti oleh Hendro Gunawan (2020). Penelitian ini menggunakan pendekatan analisis kuantitatif, dengan data yang dikumpulkan melalui penyebaran kuesioner kepada mahasiswa jurusan Sistem Informasi di Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta. Sampel dipilih secara acak dan melibatkan sebanyak 143 mahasiswa dengan pengisian kuesioner menggunakan jawaban ya dan tidak. Temuan dari studi ini menunjukkan bahwa pemahaman mahasiswa terhadap pentingnya keamanan informasi tinggi tetapi tidak mencerminkan perilaku terhadap keamanan informasi. Perilaku yang mencerminkan keamanan informasi pada penelitian ini yaitu penggantian *password* secara berkala dan pengaksesan media sosial di tempat umum tanpa memperhatikan tingkat keamanan sistemnya. Secara privasi, temuan menunjukkan bahwa mahasiswa masih mengungkapkan informasi pribadi di media sosial, memiliki akun yang dapat diakses oleh publik, dan tidak mengikuti peraturan privasi.

Penelitian yang dilakukan peneliti memiliki kesamaan dengan penelitian Gunawan (2020) yaitu mengkaji tentang privasi informasi mahasiswa di media sosial. Penelitian ini menjelaskan tingkat kesadaran privasi informasi berbanding terbalik dengan perilaku yang mencerminkan keamanan informasi. Perbedaan

penelitian yang dilakukan oleh peneliti dengan penelitian Gunawan (2020) adalah penelitian Gunawan (2020) menggunakan teori konsep keamanan informasi yang dipaparkan oleh Chan dan Mubarak (2011) adapun pada penelitian yang dilakukan oleh peneliti menggunakan teori yang dikembangkan Koohang et al (2018).

Penelitian kedua berjudul “Pengukuran Kesadaran Keamanan Informasi dan Privasi Pengguna Android di Kota Bandung” yang diteliti oleh Arvand A. Pratama, I. M. Ghufon, J. Ma’ruf, S. Hanafi, dan A. H. Anas (2022). Penelitian ini menggunakan metode pengumpulan data kuantitatif dengan pengisian kuesioner terhadap pengguna android di Kota Bandung. Penelitian ini menggunakan teori Whitman dan Mattord tentang *security awarenses* dan menggunakan teori psikologi Kurger dan Kerney yang membagi tiga komponen untuk mengukur objek yaitu *knowledge*, *attitude* dan *behaviour*. Hasil dari penelitian ini adalah pengguna android di Kota Bandung memiliki tingkat kesadaran yang baik dalam hal menjaga keamanan informasi.

Penelitian yang dilakukan oleh peneliti memiliki kesamaan dengan penelitian yang dilakukan oleh Arvand A. Pratama, I. M. Ghufon, J. Ma’ruf, S. Hanafi, dan A. H. Anas (2022) yaitu mengkaji tentang privasi informasi. Penelitian ini dapat dijadikan referensi bagi peneliti untuk mengkaji lebih jauh tentang privasi informasi. Perbedaan penelitian yang dilakukan oleh peneliti dengan penelitian sebelumnya adalah penelitian Arvand A. Pratama, I. M. Ghufon, J. Ma’ruf, S. Hanafi, dan A. H. Anas (2022) menggunakan teori Whitman dan Mattord tentang *security awareness* sementara penelitian yang dilakukan oleh peneliti menggunakan teori Koohang et al (2018) tentang *social media privacy concern*. Penelitian yang dilakukan oleh Arvand A. Pratama, I. M. Ghufon, J. Ma’ruf, S.

Hanafi, dan A. H. Anas (2022) menggunakan pengguna android sebagai objek penelitian sementara penelitian yang dilakukan oleh peneliti menggunakan *user* Instagram sebagai objek penelitian.

Penelitian ketiga berjudul “Memahami Pengelolaan Pengungkapan Informasi Pribadi di Media Sosial di Kalangan Dewasa Dini” yang diteliti oleh A. S. Ayu Pertiwi dan R. Manalau (2018). Penelitian ini mengadopsi pendekatan campuran di mana pendekatan kuantitatif eksploratif digunakan dalam tahap awal, dan dilanjutkan dengan pendekatan deskriptif kualitatif menggunakan metode fenomenologi dalam tahap berikutnya. Temuan dari studi ini menunjukkan bahwa sebagian besar pengguna media sosial yang menjadi subjek penelitian cenderung mengelola privasi secara kurang protektif. Ini tercermin dari tingginya jumlah informasi yang dibagikan oleh mayoritas pengguna, serta sedikitnya pengguna yang mengatur pengaturan privasi di akun mereka. Mayoritas dari 250 pengguna media sosial yang diselidiki dalam penelitian ini aktif membagikan informasi pribadi mereka di platform media sosial dan melakukannya dengan frekuensi yang signifikan. Persamaan penelitian yang dilakukan oleh peneliti dengan penelitian Pertiwi dan Manalau (2018) adalah sama-sama mengkaji tentang privasi informasi pribadi yang dibagikan di media sosial. Perbedaan penelitian yang dilakukan oleh peneliti dengan penelitian Pertiwi dan Manalau (2018) adalah penelitian sebelumnya memiliki fokus kepada pengelolaan informasi pribadi di media sosial sementara penelitian ini berfokus kepada pemahaman privasi informasi pribadi di media sosial.

Penelitian keempat berjudul “*Users’ Awareness of Personal Information on Social Media: Case on Undergraduate Students of Universitas Indonesia*” yang

diteliti oleh R. Nur Iman, T. Asmiyanto, dan M. Hanif. Inamullah (2020). Penelitian ini bertujuan untuk mengetahui kesadaran pengguna terkait informasi data pribadi dan ragam informasi pribadi yang tercantum di media sosial. Penelitian ini merupakan penelitian kualitatif, pengumpulan data menggunakan metode wawancara dengan pertanyaan terbuka kepada delapan mahasiswa. Hasil dari penelitian ini menunjukkan bahwa tahap kesadaran muncul ketika pengguna berpikir kritis dalam mengambil keputusan yang berkaitan dengan informasi pribadi.

Penelitian yang diteliti peneliti memiliki kesamaan dengan penelitian Iman, Asmiyanto, dan Inamullah (2020) yang mengkaji tentang privasi informasi pribadi di media sosial dengan objek penelitian mahasiswa. Penelitian tersebut dapat dijadikan referensi untuk penelitian selanjutnya mengenai gambaran kesadaran privasi informasi namun dengan teknik pengumpulan data yang berbeda. Perbedaan penelitian yang diteliti oleh peneliti dengan Iman, Asmiyanto, dan Inamullah (2020) adalah teknik pengumpulan data yang digunakan berbeda, pada penelitian sebelumnya menggunakan pendekatan kualitatif sementara penelitian ini menggunakan pendekatan kuantitatif.

Penelitian kelima berjudul *“Research on Influencing Factors of Personal Information Disclosure Intention of Social Media in China”* yang diteliti oleh Anrong Fan, Qiao Wu, Xiaofei Yan, Xiaotong Lu, Yue Ma, dan Xue Xiao pada tahun 2021. Penelitian ini merupakan penelitian kuantitatif dengan pengambilan sampel menggunakan metode *convenience sampling* dan *snowball sampling* dengan jumlah responden sebanyak 580 pengguna media sosial. Artikel ini menyelidiki faktor-faktor yang mempengaruhi pengungkapan informasi pengguna media sosial. Hasil dari penelitian menunjukkan bahwa persepsi risiko di media sosial mempunyai

pengaruh terhadap pengungkapan informasi pribadi. Penelitian ini menunjukkan bahwa pengguna media sosial harus memberikan informasi pribadi tertentu kepada *platform* untuk menggunakan media sosial dan pengguna media mau tidak mau harus menerima ketentuan tersebut.

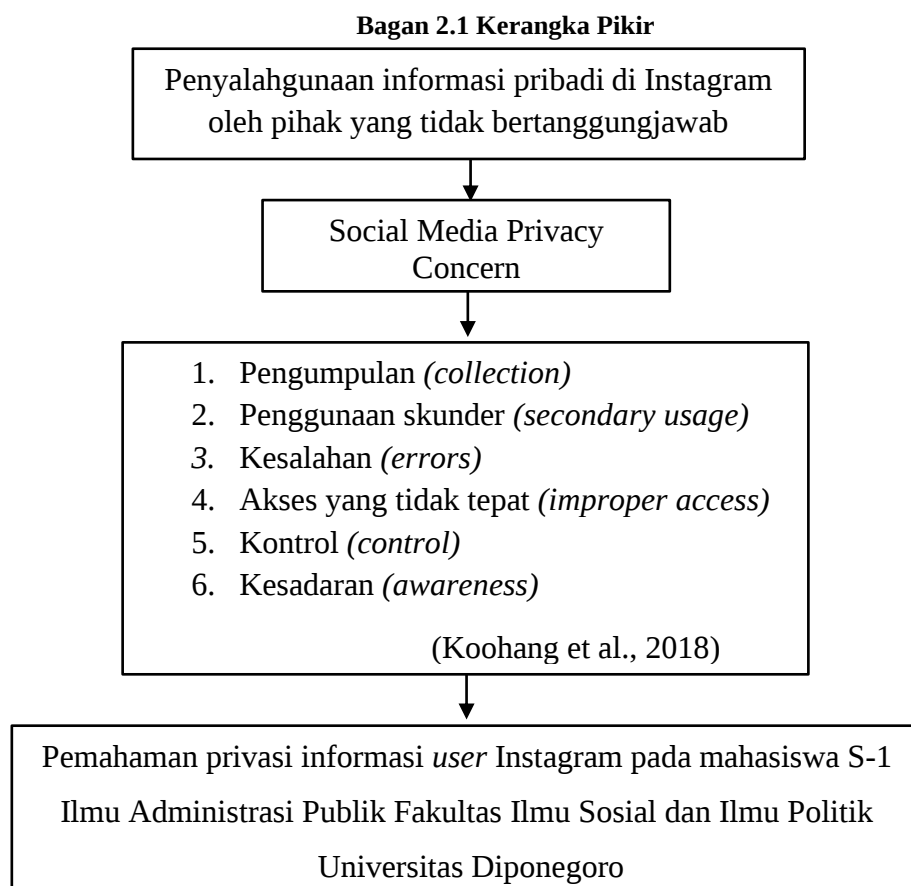
Persamaan penelitian yang diteliti oleh peneliti dengan penelitian yang dilakukan oleh Fan, et al. (2020) adalah sama-sama meneliti tentang privasi informasi di media sosial. Perbedaan penelitian Fan, et al.(2020) dan penelitian yang dilakukan oleh peneliti adalah penelitian Fan, et al. (2020) menggunakan teori kalkulus privasi yang digagas oleh Korzan dan Boswel pada tahun 2008 dan *theory of planned behavior* oleh Ajzen (1991) sementara penelitian yang dilakukan oleh peneliti menggunakan teori *social media privacy concern* oleh Koohang et al (2018).

Berdasarkan kelima penelitian sebelumnya diatas menjelaskan bahwa tingkat pemaparan informasi pribadi di media sosial masih tinggi. Faktor yang menyebabkan tingginya pengungkapan informasi pribadi salah satunya adalah karena *user* media sosial kurang sadar akan risiko yang ditimbulkan dan secara tidak langsung terpaksa memberikan informasinya kepada media sosial agar dapat menggunakan media sosial tersebut. *User* media sosial harus memahami terlebih dahulu tentang privasi informasi agar data-data yang dimiliki tidak disalahgunakan oleh oknum yang tidak bertanggung jawab. Penelitian ini memiliki landasan kuat dan relevan dalam menyelidiki pemahaman *user* Instagram dalam memahami privasi informasi. Penelitian ini mencoba mengkaji masalah privasi informasi media sosial menggunakan teori *Social Media Privacy Concern*. Di Indonesia, permasalahan seputar privasi masih belum banyak dieksplorasi secara menyeluruh.

Hal ini disebabkan oleh kurangnya perhatian terhadap isu privasi, baik dari kalangan akademisi maupun pemerintahan. Hal ini tercermin dari belum adanya regulasi khusus yang mengatur perlindungan privasi di dunia maya, terutama pada platform media sosial seperti yang diungkapkan oleh (Widiyaningsih, 2018). Penelitian ini diharapkan dapat memberikan perspektif baru tentang pemahaman *user* media sosial khususnya pada media sosial Instagram dalam memahami privasi informasi.

2.4 Kerangka Pikir

Kerangka pikir penelitian digunakan sebagai acuan dan alur penelitian yang akan dilakukan, selain itu kerangka pikir digunakan untuk menyederhanakan dan mempermudah proses penelitian. Berikut merupakan kerangka pikir yang digunakan dalam merancang penelitian.



Pada era digital ini banyak terjadi penyalahgunaan informasi pribadi secara digital oleh oknum yang tidak bertanggung jawab. Penyalahgunaan ini dapat terjadi di media sosial seperti Instagram, hal ini dapat terjadi karena tidak adanya pemahaman privasi informasi oleh *user* instagram sendiri. Korban dari penyalahgunaan informasi pribadi ini dapat dialami oleh siapa saja, termasuk mahasiswa. Mahasiswa S-1 Ilmu Administrasi Publik yang nantinya akan mengelola banyak informasi masyarakat perlu dikaji tingkat pemahamannya terhadap privasi informasi pribadi terlebih dahulu sebelum terjun ke masyarakat. Penelitian ini mencoba melihat pemahaman privasi informasi *user* instagram pada mahasiswa S-1 Ilmu Administrasi Publik Fakultas Ilmu Sosial dan Ilmu Politik Universitas Diponegoro. Masalah privasi informasi dikaji menggunakan teori yang dicetuskan oleh Hong & Thong (2013) tentang masalah privasi internet atau *internet privacy concern* (IPC). Teori ini dikembangkan dan memvalidasi konseptual masalah privasi internet dengan mengintegrasikan enam dimensi, yakni *collection*, *secondary usage*, *errors*, *improper access*, *control*, dan *awareness*. Penelitian ini mengadaptasi instrumen yang dikembangkan oleh Koohang et al. (2021) berupa pertanyaan yang berkaitan dengan masalah privasi media sosial atau *social media privacy concerns* (SMPC).