BAB 2

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 *Information Privacy Concern* dan Perilaku Perlindungan Privasi

Privasi adalah proses kontrol seorang individu dalam mengatur kapan, bagaimana, dan sejauh mana informasi miliknya dikomunikasikan kepada orang lain (Van De Garde-Perik et al., 2008). Privasi juga merupakan konstruksi yang dinamis, didorong oleh konteks (Belanger & Crossler, 2011; Crossler, 2010; Hong & Thong, 2013; Raschke et al., 2014; Xu et al., 2008), dan multidimensi. Altman (1975) mengemukakan bahwa privasi mencakup aspek interpersonal dan sosial, dan bervariasi sesuai dengan pengalaman hidup.

Privasi informasi menurut (Clark & Westin, 1968) adalah klaim individu, kelompok, atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain. Privasi informasi juga dapat didefinisikan sebagai proses pengendalian informasi dimana individu mengatur jenis, mode, dan luas informasi pribadi yang disampaikan kepada orang lain (Lanier Jr & Saini, 2008; Van De Garde-Perik et al., 2008). Dalam kehidupan nyata, informasi privasi memiliki patasan praktis dalam berbagai faktor, contohnya sektor industri, budaya, dan peraturan perundang-undangan (Malhotra et al., 2004).

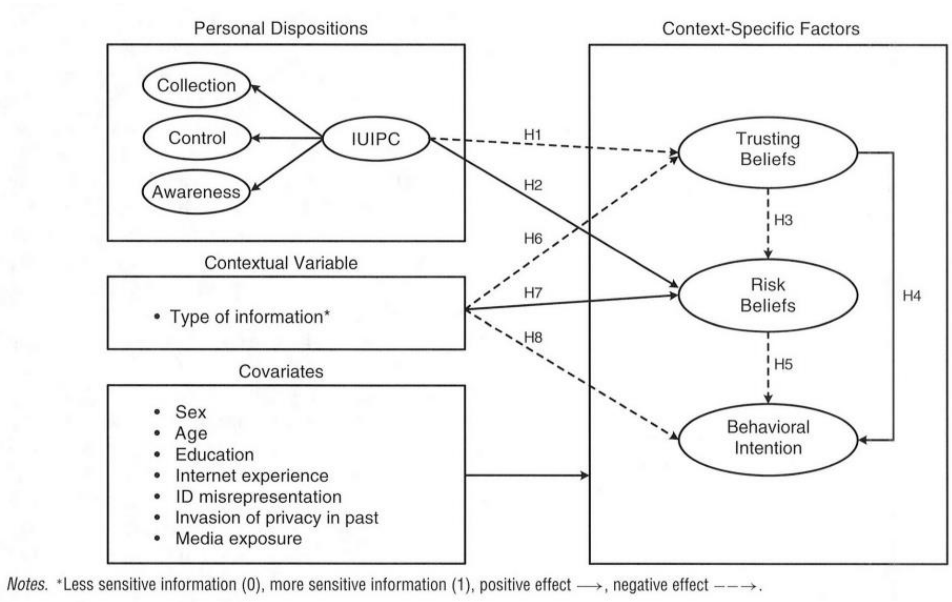
Information privacy concerns mengacu pada pandangan subjektif individu mengenai keadilan dalam konteks privasi informasi (Campbell, 1997). Para pengguna khawatir akan praktik yang dilakukan suatu organisasi yang mengumpulkan dan menggunakan informasi pribadi mereka yang merupakan *information privacy concerns* (Smith et al., 1996). *Information privacy concerns* setiap orang tidak sama. Hal ini dikarenakan masing-masing orang memiliki opini yang berbeda akan konsep adil dan tidak adil. Opini tersebut dipengaruhi oleh beragam faktor eksternal, karakteristik pribadi, dan pengalaman (Malhotra et al., 2004).

Privasi informasi saat ini telah menjadi isu yang serius di lingkungan *online* (Son & Kim, 2008), terutama di jejaring sosial. Tidak dapat dipungkiri jika jejaring sosial menawarkan fitur-fitur yang menarik minat penggunanya, namun di jejaring sosial rentan akan ancaman keamanan, kontrol akses lemah (Acquisti & Gross, 2006). Oleh karena itu, orang-orang berusaha melindungi privasi mereka dengan berbagai cara (Boerman et al., 2018). Usaha untuk melindungi privasi inilah yang disebut dengan perilaku perlindungan privasi. Milne et al. (2009) mendefinisikan perilaku perlindungan sebagai tindakan khusus berbasis komputer yang dilakukan seseorang untuk menjaga keamanan informasi. Meskipun jejaring sosial telah dilengkapi dengan langkah-langkah keamanan, hal itu bergantung pada pengguna untuk mengaktifkannya (Adhikari & Panda, 2018).

Hubungan antara *information privacy concerns* dan perilaku perlindungan privasi pada awalnya dieksplorasi oleh Altman (1975). Ia menyatakan bahwa orang-orang mencoba untuk menerapkan tingkat privasi yang diinginkan dengan

mekanisme perilaku. Kemudian, Malhotra, Kim, dan Agarwal (2004) membentuk model *information privacy concerns* dengan nama *Users' Information Privacy Concerns* (IUPC) dan merupakan pengembangan dari model *Concern For Information Privacy* (CFIP) milik Stewart dan Segars. Di dalam model tersebut *information privacy concerns* disebut sebagai anteseden kuat dari *trust beliefs, risk beliefs,* dan *behavioral intention* yang dalam konteks ini adalah perilaku perlindungan privasi. Korzaan dan Boswell (2008) turut menemukan hal yang serupa, yaitu *information privacy concerns* sebagai faktor yang secara positif mempengaruhi niat seseorang untuk melindungi privasinya.

Bagan 2.1 Model *Users' Information Privacy Concerns* (IUPC)



(Sumber: Malhotra et al., 2004)

2.1.2 *Motivation Protection Theory* sebagai Anteseden *Information Privacy Concerns*

Protection Motivation Theory atau PMT adalah teori milik Ronald W. Rogers yang dikemukakan pada tahun 1975 melalui artikel "*A Protection Motivation Theory of*

Fear Appeals and Attitude Change" dan merupakan kelanjutan dari *Health Belief Model* (HBM). Dasar dari teori ini adalah buku milik Richard Lazarus pada tahun 1966 berjudul "*Stress, Appraisal and Coping"*, yang meneliti perilaku seseorang dalam situasi stress dan cara mengatasinya. PMT digunakan untuk memahami banding rasa takut dan bagaimana orang mengatasinya (Rogers, 1975).

Dalam PMT, ketika seseorang merasa terancam oleh situasi yang berisiko, motivasinya untuk melindungi diri meningkat. Pada model awal dari PMT, motivasi seseorang untuk melindungi dirinya dari risiko muncul dari tiga komponen utama: *perceived vulnerability*, *perceived severity,* dan *response efficacy*. Namun, model ini belum memberikan penjelasan yang cukup untuk kegagalan seorang individu mengadopsi perilaku protektif. Sehingga pada 1983, James E. Maddux dan Ronald W. Rogers merevisi model PMT dengan menambahkan tiga penilaian kognitif: *self-efficacy, rewards,* dan *response costs* (Adhikari & Panda, 2018).

1. *Perceived Vulnerability*

   Seperti yang digambarkan oleh Lee, Larose, and Rifon (2008), *perceived vulnerability* atau kerentaan yang dirasakan adalah sejauh mana seseorang percaya bahwa dirinya akan mendapat ancaman. Pada tahun 2004, penelitian milik Dinev dan Hart menemukan bahwa *perceived vulnerability* mempengaruhi *online privacy concerns*. Beberapa penelitian setelahnya pun memiliki hasil yang sama dengan penelitian milik Dinev dan Hart. Seperti penelitian Lee, Larose, and Rifon, *perceived vulnerability* seseorang akan membuatnya melakukan perilaku perlindungan terhadap ancaman dari virus internet. Penelitian lain milik Crossler (2010) juga menunjukkan bahwa

perceived vulnerability yang dalam konteks penelitian ini adalah pandangan pengguna mengenai konsekuensi menggunakan internet seperti kebocoran informasi, penipuan, dan pencurian identitas, berhubungan dengan *online privacy concerns*.

2. *Perceived Severity*

   Perceived severity atau keparahan yang dirasakan menurut LaRose et al. (dalam Adhikari and Panda 2018) merujuk pada keparahan yang dihasilkan dari peristiwa yang mengancam. Seorang individu yang merasakan akibat dari kehilangan informasi di situs jejaring sosial akan cenderung lebih peduli dengan privasi informasinya (Mohamed & Ahmad, 2012). Dengan demikian, *perceived severity* yang tinggi akan memaksa seseorang untuk mengadopsi tindakan perlindungan (T. Wang et al., 2016). Penelitian terdahulu pun telah menyatakan bahwa *perceived severity* secara signifikan mempengaruhi niat pengguna jaringan nirkabel rumahan untuk menggunakan fitur keamanan seperti *anti-spyware software* (Chenoweth et al., 2009; Crossler, 2010). Sementara itu, penelitian milik Zhang dan McDowell (2009) menemukan hasil yang menarik, bahwa *perceived severity* tidak memiliki pengaruh dan tidak memotivasi pengguna internet untuk menggunakan kata sandi yang kuat.

3. *Response Efficacy*

   Woon, Tan, dan Low mendeskripsikan *response efficacy* atau efikasi respon sebagai keyakinan seorang individu bahwa koping respon dapat melindungi individu itu sendiri maupun orang lain dari suatu ancaman. (Adhikari & Panda, 2018; Mohamed & Ahmad, 2012). Dari penelitian-penelitian sebelumnya,

diketahui bahwa *response efficacy* merupakan *predictor* signifikan dari langkah-langkah keamanan individu (Woon, Tan, dan Low dalam Adhikari & Panda, 2018; Mohamed & Ahmad, 2012). Selain itu, *response efficacy* juga menjelaskan tentang penggunaan *anti-spyware* untuk melindungi privasi informasi, mempengaruhi maksud seseorang dalam menggunakan kata sandi yang kuat, dan menyimpan cadangan data (Chenoweth et al., 2009; Crossler, 2010; Zhang & McDowell, 2009). Namun, *response efficacy* tidak berpengaruh terhadap kepatuhan akan kebijakan keamanan informasi (Zhang & McDowell, 2009). Oleh karena itu pengguna yang percaya bahwa risiko hilangnya informasi dapat ditangani dengan tindakan perlindungan akan lebih memperhatikan privasi informasi mereka (Adhikari & Panda, 2018).

4. *Self-Efficacy*

   Self-efficacy diadopsi dari teori kognitif sosial. Teori kognitif sosial didefinisikan sebagai interaksi timbal balik antara faktor pribadi, individu, dan lingkungan dan bersifat dinamis (Bandura, 1989). Dalam teori kognitif sosial, pengendalian diri adalah prediktor perilaku seseorang. Dengan demikian, *self-efficacy* yang merupakan keyakinan seseorang akan kemampuannya untuk melakukan suatu perilaku dapat disebut sebagai dasar perubahan sosial (Bandura, 1995; Compeau et al., 1999). Penelitian mengenai *self-efficacy* dan pengaruhnya dalam penggunaan komputer maupun system informasi lain telah banyak dilakukan, termasuk penelitian yang membahas hubungan *self-efficacy* dan *online privacy concerns*. *Self-efficacy* dalam penelitian Korzaan & Boswell (2008) mempengaruhi *information privacy concerns* seorang individu. Pada

penelitian lain diketahui bahwa *self-efficacy* memiliki hubungan yang positif dengan motivasi untuk melindungi informasi *online* (Chai et al., 2009) dan menjadi predictor pada intensi untuk mengadopsi perilaku perlindungan seperti perlindungan dari virus di internet (Lee et al., 2008; Milne et al., 2009). Tidak semua penelitian menunjukkan hasil yang positif terkait dengan hubungan *self-efficacy* dan *information privacy concerns*. Seperti pada penelitian LaRose & Rifon (2007), *self-efficacy* tidak memiliki hubungan dengan *information disclosure*. Selain itu, penelitian Youn (dalam Mohamed & Ahmad, 2012) juga memaparkan bahwa *self-efficacy* tidak berhubungan dengan *information privacy concerns*.

5. *Rewards*

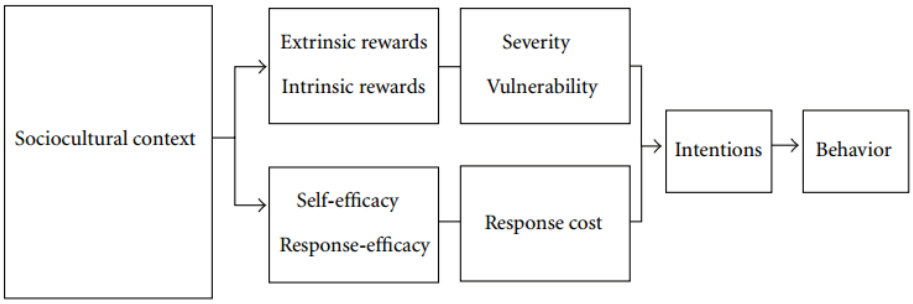
   Rewards atau imbalan berkaitan dengan manfaat yang diharapkan setelah melakukan suatu perilaku (Lee et al., 2008; Mohamed & Ahmad, 2012). Dalam PMT, disebutkan bahwa *rewards* dari perilaku berisiko melemahkan niat seoraang individu untuk melindungi diri dari risiko. (Maddux & Rogers, 1983; Rogers, 1975). Dalam jejaring sosial, pengguna akan lebih memperhatikan keuntungan yang ia rasakan daripada risiko penyebaran informasi pribadinya (Adhikari & Panda, 2018). Seperti yang disebutkan Youn (dalam Adhikari & Panda, 2018; Mohamed & Ahmad, 2012) melalui penelitiannya, remaja yang berusia antara 14 sampai 18 tahun akan dengan suka rela memberikan informasi pribadinya demi sebuah *rewards* yang ditawarkan situs jejaring sosial. *Rewards* tersebut berupa permainan *online*, kuis, dan lain sebagainya. Seseorang yang tidak memberikan informasi mengenai dirinya akan dapat

terhindar isu privasi informasi seperti serangan virus internet dan pencurian identitas. Namun, dengan memberikan informasi pribadi di situs jejaring sosial akan lebih diterima oleh pengguna lain situs tersebut (Baren et al. dalam (Adhikari & Panda, 2018).

6. *Response Costs*

   Response costs mengukur biaya yang harus dibayar seseorang (misalnya waktu, uang, dan usaha) ketika melakukan perilaku perlindungan (Zhang & McDowell, 2009). Jika biaya yang harus dilakukan seorang individu untuk melakukan perilaku yang direkomendasikan tinggi, maka kemungkinan individu tersebut akan melakukannya menjadi rendah. Tidak banyak penelitian yang mengkaji mengenai hubungan antara *response costs* dan *information privacy concerns*. Salah satu penelitian yang turut memasukkan *response costs* sebagai anteseden *information privacy concerns* adalah penelitian milik Terlizzi et al. (2020). Terlizzi et al. berpendapat jika seorang individu menganggap *response costs* untuk melindungi informasinya berada di luar kemampuan dan sumber dayanya, maka mereka akan lebih peduli pada kemungkinan kehilangan data pribadi dan data keuangan di *m-banking* dan perangkat seluler miliknya. Sebagai contoh, upaya yang diperlukan untuk melindungi posel dengan kata sandi dapat meningkatkan *information privacy concerns*.

Bagan 2.2 Model *Protection Motivation Theory* (PMT)



(Sumber: Pham et al., 2012)

2.2 Penelitian Sejenis Sebelumnya

Maksud dari tinjauan penelitian sejenis sebelumnya adalah untuk menambah wawasan penulis dan menunjukkan orisinalitas penelitian yang akan dilakukan. Maka dari itu, penulis akan meninjau beberapa penelitian mengenai *information privacy concern* dan perilaku perlindungan privasi yang telah dilakukan sebelumnya.

Penelitian pertama adalah penelitian milik Mohamed dan Ahmad dengan judul "*Information Privacy Concerns, Antecedents and Privacy measure Use in Social Networking Sites Evidence from Malaysia*". Pada 2012, Mohamed dan Ahmad mempublikasikan penelitian ini di jurnal *Computers in Human Behavior*. Partisipan dalam penelitian Mohamed dan Ahmad ini adalah mahasiswa di salah satu perguruan tinggi Malaysia. Tujuan penelitiannya adalah untuk mengetahui *information privacy concern*, variable eksogen dari *information privacy concern*, dan penggunaan ukuran privasi di situs jejaring social.

Guna mendapatkan hasil dan mencapai tujuan penelitian, Mohamed dan Ahmad menggunakan metode penelitian kuantitatif. Kuesioner digunakan untuk mengumpulkan data. Dalam membuat pertanyaan pada kuesioner, sekaligus menentukan variable eksogen dari *information privacy concern*, Mohamed dan Ahmad menggunakan *social cognitive theory* yaitu *self-efficacy*; *protection motivation theory* yaitu *perceived severity, perceived vulnerability, response efficacy,* dan *rewards*; dan faktor gender. Sebanyak 413 kuesioner dibagikan ke mahasiswa salah satu universitas di Malaysia dengan berdasarkan desain survei *cross-sectional* dan teknik *cluster sampling*.

Dari 413 kuesioner yang dibagikan sebanyak 345 kuesioner diisi oleh responden, dan hanya 340 kuesioner yang dapat dianalisis. Kriteria dari kuesioner yang dipakai adalah jika responden memiliki paling tidak satu akun jejaring social dan menggunakannya, juga mengisi paling tidak 90% pertanyaan pada kuesioner. Hasil dari analisis menunjukkan bahwa dalam urutan kepentingan hanya *perceived severity, self-efficacy, perceived vulnerability*, dan gender yang merupakan variable eksogen dari *information privacy concern* di social media. Selain itu, hasil juga menunjukkan bahwa *information privacy concern* menjelaskan penggunaan ukuran privasi di situs jejaring social.

Persamaan penelitian penulis dan penelitian milik Mohamed dan Ahmad adalah topik yang dibahas, penggunaan PMT sebagai anteseden *information privacy concerns*, pemilihan metode penelitian kuantitatif dan teknik analisis data yang menggunakan *structural equation modelin* (SEM). Selanjutnya perbedaan pada kedua penelitian adalah responden yang digunakan dimana kriteria responden

penulis adalah pengguna Twitter sementara responden Mohamed dan Ahmad adalah mahasiswa salah satu perguruan tinggi di Malaysia. Selain itu, jika penelitian milik penulis menggunakan seluruh aspek PMT sebagai anteseden *information privacy concerns*, maka penelitian Mohamed dan Ahmad hanya menggunakan *perceived severity, perceived vulnerability, response efficacy, rewards,* dan *self-efficacy* ditambah dengan faktor individu berupa gender.

Penelitian sejenis sebelumnya yang kedua adalah penelitian milik Adhikari dan Panda pada tahun 2018 dengan judul "*Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks"*. Tujuan dari penelitian Adhikari dan Panda adalah untuk memvalidasi variabel eksogen dari *users' information privacy concerns* (UIPC) dan menguji bagaimana UIPC mempengaruhi perilaku perlindungan privasi. Untuk variable eksogen, Adhikari dan Panda menggunakan *protection motivation theory* yaitu *perceived vulnerability, perceived severity, rewards, and response efficacy* dan *social cognitive theory* yaitu *self-efficacy*.

Penelitian milik Adhikari dan Panda ini mengambil sampel dari mahasiswa sebuah universitas di India. Populasi dari mahasiswa di universitas tersebut mencapai hampir 5000 mahasiswa dan berasal dari budaya yang beragam. Berdadarkan teknik *simple random sampling*, responden dipilih secara acak dari daftar penerimaan mahasiswa baru. Namun, terdapat juga dua pertimbangan utama untuk sampel yaitu rentang usia antara, 18 sampai 24 tahun dan memiliki akun jejaring sosial. Penentuan ukutan sampel dilakukan dengan menggunakan kalkulator ukuran sampel apriori untuk pemodelan persamaan strukturan atau

structural equation modeling (SEM). Berdasarkan perhitungan ukuran efek dan kekuatan statistik, jumlah sampel minimum adalah 210 responden. Oleh karena itu, kuesioner yang dibagikan adalah sebanyak 410 atau dua kali sampel minimum. Kuesioner dibagikan pada bulan September 2016. Dari 410 kuesioner yang dibagikan, 337 kuesioner diisi oleh responden. Setelah mengeliminasi 31 kuesioner yang tidak valid dan tidak lengkap, 306 kuisoner dianalisis. Analisis data tersebut menggunakan model persamaan struktural (*structural equation modeling*/SEM).

Hasil dari penelitian Adhikari dan Panda menunjukkan bahwa *perceived vulnerability*, *perceived severity*, dan *self-efficacy* mempengaruhi *users' information privacy concerns* secara signifikan. *Perceived vulnerability* memiliki kontribusi maksimal akan pengaruhnya terhadap *information privacy concerns*. Hal ini ditunjukkan dengan pengguna yang percaya akan risiko keamaan di jejaring sosial, sangat memperhatikan privasi informasinya. Maka dari itu, mereka menunjukkan perilaku perlindungan privasi untuk melindungi diri dari potensi risiko keamanan informasi. *Perceived severity* mempengaruhi *information privacy concerns* yang berkonotasi dengan persepsi pengguna tentang konsekuensi negatif dari risiko privasi informasi di jejaring sosial (misalnya, pencurian identitas), yang kemudian membuat mereka melindungi privasi sebagai tindakan pencegahan. Pengaruh *self-efficacy* terhadap *information privacy concerns* ditunjukkan dengan pengguna yang memiliki kepercayaan diri dan kemampuan untuk melindungi dirinya dari ancaman privasi memiliki pemahaman terhadap *information privacy concerns* yang mendorongnya untuk memiliki perilaku perlindungan privasi di jejaring sosial. Sementara itu *rewards and response efficacy* tidak secara signifikan

mempengaruhi *users' information privacy concerns*. Selain itu, diketahui juga bahwa *users information privacy concers* dan perilaku perlindungan privasi saling berhubungan.

Sama dengan penelitian sejenis yang pertama, persamaan penelitian penulis dan penelitian milik Mohamed dan Ahmad terletak pada topik yang dibahas, penggunaan PMT sebagai anteseden *information privacy concerns,* pemilihan metode penelitian kuantitatif dan teknik analisis data yang menggunakan *structural equation modeling* (SEM). Kemudian perbedaan pada kedua penelitian adalah responden yang digunakan dimana kriteria responden penulis adalah pengguna Twitter. Adapun responden Mohamed dan Ahmad adalah mahasiswa salah satu perguruan tinggi di Malaysia. Selain itu, jika penelitian milik penulis menggunakan seluruh aspek PMT sebagai anteseden *information privacy concerns*, maka penelitian Mohamed dan Ahmad hanya menggunakan *perceived severity, perceived vulnerability, response efficacy, rewards,* dan *self-efficacy* ditambah dengan faktor individu berupa gender.

Selanjutnya terdapat penelitian milik Chen, Beaudoin, dan Hong (2017) dengan judul "*Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors*". Penelitian oleh Chen, Beaudoin, dan Hong dimuat dalam jurnal *Computers in Human Behavior* volume 70. Tujuannya adalah untuk mengidentifikasi variabel yang menyebabkan seorang pengguna jejaring sosial menjadi korban penipuan dan bagaimana hal tersebut mempengaruhi *online privacy concerns* dan perlakukan perlindungan privasi.

Untuk lebih memahami korban penipuan melalui internet, selain menggunakan *protection motivation theory*, Chen, Beaudoin, dan Hong juga menggunakan *extended parallel process model, self-control theory,* dan *routine activity theory* sebagai variabel. Sesuai dengan studi terkini pada *self-control theory*, *willingness* dan *knowledge* diambil sebagai variabel. Dari *routine activity theory,* variabel yang diambil adalah *information disclosure*, belanja online, mengunduh file, konsumsi informasi online, dan membuka email dari sumber yang tidak dikenal.

Chen, Beaudoin, dan Hong mengumpulkan 11.741 data survei yang dibagikan mulai tanggal 23 November sampai 30 Desember 2013. Survei tersebut dilakukan secara daring pada penduduk Amerika Serikat yang berusia 18 tahun atau lebih. Dari 11.741 data yang terkumpul, hanya 11.543 data yang dapat sesuai dengan kriteria dan dapat dianalisis. Ke-11.543 data tersebut dianalisis dengan menggunakan pemodelan persamaan struktural (*structural equation modeling*/SEM).

Hasil dari penelitian Chen, Beaudoin, dan Hong menunjukkan bahwa *willingness*, *information disclosure*, belanja online, dan membuka email dari sumber yang tidak dikenal secara signifikan menunjukkan hubungan dengan menjadi korban penipuan di internet. Sementara *knowledge*, mengunduh file, dan konsumsi informasi online tidak menunjukkan hubungan yang signifikan. Selain itu, diketahui juga bahwa hubungan yang signifikan terjadi antara menjadi korban penipuan dan *online privacy concerns*. Hubungan *online privacy concerns* dan perilaku perlindungan privasi diketahui dengan tiga tindakan yang dilakukan

pengguna internet, yaitu: memasang anti-virus, memperbarui anti-virus, dan mengganti kata sandi secara berkala.

Persamaan yang dimiliki oleh penelitian Chen, Beaudoin, dan Hong dengan penelitian penulis adalah topik yang diangkat, yaitu *information privacy concerns* dan perilaku perlindungan privasi. Hanya saja, pada penelitian Chen, Beaudoin, dan Hong lebih berfokus pada variabel yang menyebabkan seorang pengguna jejaring sosial menjadi korban penipuan. Kedua penelitian menerapkan metode penelitian kuantitatif dengan teknik analisis data *structural equation modelin* (SEM). Penelitian milik Chen, Beaudoin, dan Hong juga menggunakan PMT sama seperti milik penulis. Namun, yang membedakan, Chen, Beaudoin, dan Hong menambahkan *extended parallel process model, self-control theory*, dan *routine activity theory*. Partisipan pada penelitian Chen, Beaudoin, dan Hong adalah warga negara Amerika Serikat yang berusia lebih dari sama dengan 18 tahun, sementara partisipan dari penelitian penulis adalah pengguna Twitter.

Keempat adalah penelitian milik Yohana Widiyaningsih (2018) dengan judul "Perilaku Perlindungan Privasi pada Pengguna Instagram di Kalangan Siswa Sekolah Menengah Atas Kota Surabaya". Penelitian tersebut dilakukan pada tahun 2018 di sepuluh sekolah yang tersebar di lima kecamatan: Genteng, Sukolilo, Tandes, Krembangan, dan Sawahan. Kesepuluh sekolah tersebut adalah SMAN 2 Surabaya, SMAN 5 Surabaya, SMAN 20 Surabaya, SMAS Dr. Soetomo, SMAN 11 Surabaya, SMAS Tri Karya Surabaya, SMAS Stella Maris, SMAS Tamiriyah Surabaya, SMAN 21 Surabaya, dan SMA Katolik ST Louis 2. Tujuannya adalah untuk mengkaji perilaku perlindungan privasi siswa Sekolah Menengah Atas

(SMA) di Kota Surabaya yang menggunakan Instagram dengan menggunakan Model APCO. Model APCO sendiri adalah model gagasan Smith, Dinev, dan Xu pada tahun 2011 yang terdiri dari tiga bagian yang berkesinambungan, yaitu: *antecedents*, *privacy concerns,* dan *outcomes*. *Antecedents* atau anteseden dalam Bahasa Indonesia, merujuk pada faktor awal seorang individu untuk fokus terhadap isu privasi atau *privacy concerns*. Dalam penelitian ini, anteseden yang digunakan adalah *privacy awareness* dan demografi. *Privacy concerns* adalah fokus terhadap isu privasi. Empat dimensi *privacy concerns* menurut Smith (1996) adalah *collection, errors, secondary use,* dan *improper access*. Terakhir, *outcomes* merupakan hasil atau reaksi individu yang dalam konteks ini adalah perilaku perlindungan privasi dan dibentuk melalui pemikiran tentang *risk* dan *trust*.

Penelitian milik Yohana Widiyaningsih dilakukan dengan melalui pendekatan kuantitatif deskriptif. Sampel diambil dengan menggunakan teknik *multistage random sampling* yang membagi populasi ke dalam beberapa tingkatan fraksi sehingga diperoleh sejumlah sampel yang dapat merepresentasikan populasi. Lima kecamatan di Kota Surabaya menjadi sampel primer dan pelajar Sekolah Menengah Atas (SMA) menjadi unit elementer. Dari masing-masing sekolah, diambil sepuluh siswa secara acak.

Hasil dari penelitian milik Yohana Widiyaningsih menunjukkan bahwa siswa Sekolah Menengah Atas (SMA) di Kota Surabaya sudah memiliki kesadaran akan isu privasi bukan karena pernah menjadi korban namun karena pemberitaan mengenai isu-isu privasi di media. Kesadaran inilah yang kemudian menjadi salah satu faktor *information privacy concerns*. Siswa pun sadar bahwa informasi tidak

hanya sekadar dikumpulkan tapi juga digunakan oleh Instagram. Hanya saja hal tersebut tidak menimbulkan kekhawatiran yang mendalam. Dalam mengisi informasi pribadinya di Instagram, siswa memahami bahwa informasi tersebut akan disimpan dalam *database* Instagram, sehingga mereka mengisinya dengan informasi yang benar. Meskipun demikian, siswa juga sadar bahwa ada pihak tidak berwenang yang dapat mengambil informasi tersebut. Mereka berharap bahwa Instagram dapat memberikan perlindungan pada informasi mereka. Dalam segi perilaku, siswa memiliki perilaku yang kurang terhadap perlindungan privasi di Instagram karena pada dasarnya, orientasi mereka menggunakan Instagram adalah untuk kesenangan berjejaring. Siswa pada akhirnya menjadi mengabaikan perilaku perlindungan privasi di Instagram.

Hasil lain yang ditemukan dalam penelitian Yohana Widiyaningsih adalah jenis kelamin dan usia memiliki keterkaitan dengan *privacy concerns*. Siswa perempuan dan siswa yang berusia lebih tua lebih memperhatikan *privacy concerns* di Instagram. Sementara *risk* dan *trust* kurang berdampak pada perilaku perlindungan privasi di Instagram. Selain itu, siswa yang memiliki *information privacy concerns* yang tinggi akan membentuk perilaku perlindungan privasi yang tinggi pula. Begitu juga sebaliknya, siswa yang memiliki *information privacy concerns* yang rendah akan membentuk perilaku perlindungan privasi yang rendah.

Persamaan penelitian penulis dan penelitian Yohana Widiyaningsih adalah kajian mengenai *information privacy concerns* dan perilaku perlindungan privasi. Adapun perbedaannya ada pada teknik analisis data dan anteseden yang digunakan. Jika pada penelitian oleh penulis, analisis data dilakukan dengan teknik *structural*

equation model (SEM) dan anteseden mengambil dari PMT, maka penelitian milik Yohana Widiyaningsih menggunakan metode penelitian kuantitatif deskriptif dan anteseden *privacy awareness* dan demografis berupa usia dan jenis kelamin.

Penelitian kelima berjudul "Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, dan Perilaku Keamanan pada Para Pengguna Media Sosial Line" oleh Afandi, Kusyanti, dan Wardani (2017). Tujuan dari penelitian Afandi, Kusyanti, dan Wardani adalah untuk menganalisis faktor-faktor yang mempengaruhi kesadaran pengguna Line dalam perilaku keamanan dengan menerapkan model *Users' Information Privacy Concerns* (IUPC). Model IUPC digunakan untuk mengoreksi kajian penelitian dengan judul "*Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users*" yang masih menggunakan model *Concern For Information Privacy* (CFIP). Afandi, Kusyanti, dan Wardani merasa bahwa model IUPC merupakan model yang lebih modern dan lebih cocok untuk digunakan di era internet.

Afandi, Kusyanti, dan Wardani memilih metode penelitian kuantitatif untuk menemukan hasil penelitian. Dalam menganalisis data mereka menggunakan teknik *structural equation model* (SEM). Total jumlah responden pada penelitian ini sebanyak 263 pengguna Line. Penelitian ini memiliki 8 konstruk, yaitu: *security awareness, self–efficacy, expectation, security behavior, cues to action, perceived severity, perceived security threat,* dan *internet users information privacy concerns.* Hasil dari penelitian Afandi, Kusyanti, dan Wardani menunjukkan *cues to action* memiliki hubungan yang positif dengan *perceived security threat*, begitupun

hubungan *self–efficacy* dengan *expectation, perceived security threat* dengan *internet users information privacy concerns,* dan *perceived security threat* dengan *security behavior*.

Persamaan penelitian Afandi, Kusyanti, dan Wardani dengan penelitian penulis adalah topik yang diangkat, yaitu *information privacy concerns* dan perilaku perlindungan, atau dalam penelitian Afandi, Kusyanti, dan Wardani adalah perilaku keamanan. Selain itu, penelitian penulis dan penelitian mereka sama-sama menggunakan metode penelitian kuantitatif dengan teknis analisis data *structural equation modeling* (SEM). Perbedaan yang ada pada penelitian Afandi, Kusyanti, dan Wardani dan penelitian penulis adalah jumlah konstruk penelitian. Konstruk pada penelitian mereka adalah *security awareness, self–efficacy, expectation, security behavior, cues to action, perceived severity, perceived security threat,* dan *internet users information privacy concerns.* Adapun konstruk penelitian milik penulis yang menerapkan PMT, yaitu: *perceived severity, perceived vulnerability, response efficacy, self-efficacy, rewards, response costs, information privacy concerns,* dan perilaku perlindungan privasi. Selain konstruk, responden dari penelitian Afandi, Kusyanti, dan Wardan dan penelitian penulis pun berbeda. Mereka memilih responden dari pengguna Line, sedangkan responden penulis adalah pengguna Twitter.