ANUVA Volume 5 (2): 221-236, 2021

Available Online at: http://ejournal.undip.ac.id/index.php/anuva

Korelasi Antara *Information Privacy Concern* dan Perlindungan Privasi Pengguna Twitter di Indonesia

Firamia Dyah Pawestri[1*)], Jumino[2]

[1,2]*Program Studi S-1 Ilmu Perpustakaan, Fakultas Ilmu Budaya, Universitas Diponegoro, Jl. Prof. Soedarto, SH, Kampus Undip Tembalang, Semarang, Indonesia*

[*)] Korespondensi: firamiadyah@gmail.com

Abstract

[Title: The Correlation of Information Privacy Concern and Privacy Protection Behavior of Twitter Users in Indonesia] *Privacy is an important matter in today's society. However, cases of cybercrime that threaten the privacy of internet users, including users of social services such as Twitter, are increasing. The objective of this research is to understand the relationship of information privacy concern and privacy protection behavior and the relationship of the components of Protection Motivation Theory, which are perceived severity, perceived vulnerability, response efficacy, self-efficacy, rewards, and response costs, and information privacy concern of Twitter users in Indonesia. Using simple random sampling, the questionnaire was distributed online on Twitter from 13 November 2020 to 15 November 2020. In that time frame, 156 data were obtained. The collected data were analyzed using Structural Equation Modeling. The analysis shows that information privacy concern positively and significantly affected privacy protection behaviors. Perceived severity, perceived vulnerability, response efficacy, and self-efficacy positively and significantly affect information privacy concern. Meanwhile, rewards negatively and significant effect on information privacy concern. Response costs were found to have no significant affect information privacy concern.*

Keywords: twitter; information privacy concern; privacy protection behavior; protection motivation theory

Abstrak

Privasi adalah sesuatu yang penting di era ini. Namun, kasus kejahatan dunia maya yang mengancam privasi pengguna internet yang jumlahnya semakin banyak, termasuk pengguna layanan jejaring sosial seperti Twitter. Tujuan dari penelitian ini adalah untuk memahami hubungan *information privacy concern* dan perilaku perlindungan privasi serta hubungan antara komponen-komponen *Protection Motivation Theory*, yaitu *perceived severity, perceived vulnerability, response efficacy, self-efficacy, rewards,* dan *response costs,* dan *information privacy concern* pengguna Twitter di Indonesia. Dengan menggunakan simple random sampling, kuesioner dibagikan secara daring di Twitter pada tanggal 13 November 2020 sampai 15 November 2020. Dalam rentang waktu tersebut didapatkan 156 data. Data yang terkumpul lalu dianalisis dengan menggunakan *Structural Equation Modeling*. Hasil menunjukkan *information privacy concern* berpengaruh positif dan signifikan *terhadap* perilaku perlindungan privasi. *Perceived seveerity, perceived vulnerability, response efficacy, dan self-efficacy* memiliki pengaruh positif serta signifikan terhadap *information privacy concern*. Sedangkan *rewards* secara negatif dan signifikan *mempengaruhi information privacy concern*. *Response costs* tidak memiliki pengaruh yang signifikan terhadap *information privacy concern*.

Kata kunci: twitter; *information privacy concern*; perilaku perlindungan privasi; *protection motivation theory*

1. Pendahuluan

Era informasi merupakan era yang berbasis pada teknologi informasi. Teknologi informasi, secara sederhana, diartikan sebagai perangkat yang digunakan untuk mengolah, menyimpan, juga menyebarkan informasi. Penciptaannya ditujukan untuk mempermudah kehidupan manusia.

Teknologi informasi seperti komputer serta telepon genggam serta akses internet yang mudah adalah salah satu penyebab naiknya popularitas layanan jejaring sosial. Masyarakat saat ini menggunakan layanan jejaring sosial untuk mencari informasi dan berkomunikasi satu sama lain (Bodendorf dan Kaiser,

2010). Selain itu, layanan jejaring sosial mengizinkan seseorang untuk membagikan pengalaman, informasi, opini, preferensi, dan ulasan pada suatu produk (Lim, Heinrichs dan Lim, 2017). Layanan jejaring sosial juga menawarkan ruang untuk menjaga hubungan antar teman dan membuat relasi baru (Rohani, 2009).

Layanan jejaring sosial yang pertama dikenal adalah Six Degrees. Diciptakan oleh Andrew Weinreich pada tahun 1997 dan bertahan sampai tahun 2001. Setelah Six Degrees, banyak bermunculan layanan jejaring sosial lain. Beberapa contohnya adalah Facebook, LinkedIn, MySpace, Instagram, dan Twitter.

Twitter merupakan layanan jejaring sosial yang mengizinkan penggunanya untuk untuk membagikan informasi secara real-time melalui posting pengalaman dan pemikiran mereka (Mistry, 2011). Sebagai sistem micro-blogging, Twitter biasa digunakan untuk memperbarui status, memulai percakapan, mempromosikan produk, dan bahkan untuk mengirim spam (Benevenuto *et al.*, 2010). Hal ini yang menjadikan Twitter sebagai salah satu jejaring sosial paling populer. Pada 2020, menurut data Statista, sebuah perusahaan yang mengkhususkan diri pada perhitungan data asal Jerman, Twitter memiliki 353 juta pengguna. Di Indonesia sendiri, jumlah pengguna Twitter telah mencapai 13,2 juta pengguna (Statista, 2020).

Sebagai salah satu layanan jejaring sosial, antar pengguna Twitter dapat mengunjungi profil pengguna yang lain dengan mudah. Oleh karena itu, hampir semua yang muncul di Twitter akan menyebar dengan mudah. Seperti yang dituliskan Arendt (1958) jauh sebelum internet muncul bahwa semua yang muncul di ranah publik dapat dilihat dan didengar oleh semua orang dan memiliki publisitas seluas mungkin.

Masalah privasi tentu saja muncul dengan kebebasan akses yang dimiliki setiap pengguna Twitter maupun pengguna jejaring sosial lain. Selain itu, praktik akses data oleh pengembang aplikasi turut memperburuk masalah privasi pengguna (Xu *et al.*, 2012). Pada 2018, pihak Twitter mengumumkan bahwa mereka menemukan bug pada sistem dan meminta seluruh penggunanya untuk mengubah kata sandi untuk melindungi data pribadinya. Kasus ini bukanlah kasus yang pertama maupun kasus yang terakhir terkait keamanan privasi informasi pada Twitter.

Seperti yang dipaparkan oleh Kominfo, di Indonesia pemahaman mengenai pentingnya privasi informasi dan keamanannya masih lemah. Contohnya, ketika mendapatkan pesan berupa link palsu dari orang tak dikenal yang dapat membawa serangan *malware* pada ponsel atau komputer sehingga mengakibatkan pengambilan data pribadi secara ilegal sampai kerusakan di perangkat internal (Akraman dan Priyadi, 2018). Maka dari itu, penting untuk semua individu memahami mengenai privasi informasi sehingga mereka dapat melakukan perlindungan terhadap privasi tersebut.

Information privacy concern atau dapat juga disebut sebagai kepedulian terhadap privasi informasi, merupakan pandangan milik seorang individu mengenai seberapa sejauh mana privasi informasi dapat dilakukan. Artinya, individu tersebut dapat menentukan informasi mana yang boleh disebar dan informasi mana yang harus dijaga. Tentu saja, masing-masing individu memiliki *information privacy concern* yang

berbeda-beda, karena *information privacy concern* dipengaruhi oleh berbagai faktor eksternal, pengalaman, dan karakteristik pribadi (Malhotra, Kim dan Agarwal, 2004). Beberapa faktor yang mempengaruhi *information privacy concern* seseorang adalah komponen-komponen yang diambil dari *Protection Motivation Theory* (PMT) milik R.W. Rogers, yang terdiri atas *perceived severity, perceived vulnerability, response efficacy, self-efficacy, rewards,* dan *response costs*, seperti pada penelitian milik Dinev dan Hart (2004) dan penelitian milik Di Wang (2019).

Penelitian mengenai *information privacy concern* dan pengaruhnya terhadap perilaku perlindungan privasi terutama dalam layanan jejaring sosial telah dilakukan oleh peneliti-peneliti terdahulu, seperti penelitian Mohamed dan Ahmad (2012) dan penelitian Adhikari dan Panda (2018). Hasil yang mereka temukan menunjukkan bahwa information privacy concern seorang pengguna jejaring sosial akan mempengaruhi perilaku perlindungan privasinya. Namun, penelitian mereka tidak mengkhususkan pada satu layanan jejaring sosial, melainkan layanan jejaring sosial secara keseluruhan, dan tidak dilakukan di Indonesia.

Penelitian mengenai privasi sendiri di Indonesia pernah beberapa kali pernah dilakukan. Seperti penelitian milik Akraman dan Priyadi (2018) yang membahas mengenai privasi dan kesadaran keamanan informasi pengguna Android di Indonesia. Untuk penelitian mengenai privasi yang memfokuskan di layanan jejaring sosial contohnya adalah penelitian milik Widyaningsih (2018) mengenai perilaku perlindungan privasi pengguna Instagram khususnya siswa SMA di Surabaya dan penelitian milik Afandi, Kusyanti dan Wardani (2017) mengenai kesadaran keamanan, privasi informasi dan perilaku keamanan pengguna jejaring sosial LINE.

Namun sejauh yang peneliti ketahui, tidak ada penelitian yang pernah dilakukan di Indonesia yang secara khusus membahas mengenai *information privacy concern* dan hubungannya dengan perilaku perlindungan privasi, serta hubungan antara komponen-komponen *Protection Motivation Theory* (PMT) milik R.W. Rogers dengan *information privacy concern*. Maka dari itu, peneliti berkeinginan untuk meneliti hubungan antara *information privacy concern* dan perilaku perlindungan privasi serta hubungan antara *information privacy concern* dan komponen-komponen *Protection Motivation Theory* milik R. W. Rogers.

Selanjutnya, karena saat ini mayoritas orang di Indonesia menggunakan internet untuk mengakses layanan jejaring sosial, seperti pada data milik HootSuite (Kemp, 2020) dari 175,4 juta pengguna internet di Indonesia, sebanyak 160 juta adalah pengguna layanan jejaring sosial, maka dari itu penelitian ini akan berfokus di sosial media. Karena penelitian mengenai privasi di layanan jejaring sosial di Indonesia selama ini hanya ada pada layanan jejaring sosial Instagram dan LINE, maka peneliti memutuskan untuk mengkhususstakn penelitian pada layanan jejaring sosial Twitter. Selain itu, pengguna Twitter di Indonesia pun termasuk tinggi, hanya di bawah Amerika Serikat, Jepang, India, Brazil, Inggris dan Turkey, yaitu sebanyak 13,2 juta pengguna (Statista, 2020).

2. Landasan Teori

2.1 *Information Privacy Concern* dan Perilaku Perlindungan Privasi

Privasi informasi saat ini telah menjadi isu yang serius di lingkungan online (Son and 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 dan Gross, 2006). *Information privacy concerns* mengacu pada pandangan subjektif individu mengenai keadilan dalam konteks privasi informasi (Campbell, 1997). Meskipun jejaring sosial telah dilengkapi dengan langkah-langkah keamanan, hal itu bergantung pada pengguna untuk mengaktifkannya (Adhikari dan Panda, 2018). Milne, Labrecque dan Cromer (2009) mendefinisikan perilaku perlindungan sebagai tindakan khusus berbasis komputer yang dilakukan seseorang untuk menjaga keamanan informasi. Hubungan antara *information privacy concern* 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.

H_1: *Information privacy concern* berpengaruh positif dan signifikan terhadap perilaku perlindungan privasi pengguna Twitter di Indonesia.

2.2 Motivation Protection Theory sebagai Anteseden *Information Privacy Concern*

Teori milik Ronald W. Rogers, *Protection Motivation Theory* (PMT), dikemukakan pada tahun 1975 melalui artikel "*A Protection Motivation Theory of Fear Appeals and Attitude Change*". 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 dan Panda, 2018).

1. *Perceived Severity*

Perceived severity atau keparahan yang dirasakan menurut LaRose et al. (dalam (Adhikari dan 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 dan Ahmad, 2012). Dengan demikian, *perceived severity* yang tinggi akan memaksa seseorang untuk mengadopsi tindakan perlindungan (Wang, Duong dan Chen, 2016).

H_2: *Perceived severity* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

2. *Perceived Vulnerability*

Seperti yang digambarkan oleh Lee, Larose dan Rifon (2008), *perceived vulnerability* adalah sejauh mana seseorang percaya bahwa dirinya bisa mendapat ancaman. Pada tahun 2004, penelitian milik

Dinev dan Hart menemukan bahwa *perceived vulnerability* mempengaruhi *online privacy concerns*. 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.

H_3: *Perceived vulnerability* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

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 dan Panda, 2018; Mohamed dan Ahmad, 2012). Pengguna yang percaya bahwa risiko hilangnya informasi dapat ditangani dengan tindakan perlindungan akan lebih memperhatikan privasi informasi mereka (Adhikari dan Panda, 2018).

H_4: *Response efficacy* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

4. *Rewards*

Rewards atau imbalan berkaitan dengan manfaat yang diharapkan setelah melakukan suatu perilaku (Lee, Larose dan Rifon, 2008; Mohamed dan Ahmad, 2012). Dalam PMT, disebutkan bahwa *rewards* dari perilaku berisiko melemahkan niat seorang individu untuk melindungi diri dari risiko (Rogers, 1975; Maddux dan Rogers, 1983). 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 dan Panda, 2018).

H_5: *Rewards* berpengaruh negatif dan signifikan terhadap *information privacy concern pengguna* Twitter di Indonesia.

5. *Self-Efficacy*

Self-efficacy adalah keyakinan milik seseorang pada kemampuannya untuk melakukan suatu perilaku dapat disebut sebagai dasar perubahan sosial (Bandura, 1989; Compeau, Higgins dan Huff, 1999). *Self-efficacy* dalam penelitian Korzaan dan Boswell (2008) mempengaruhi *information privacy concerns* seorang individu. Pada penelitian lain diketahui bahwa *self-efficacy* memiliki hubungan yang positif dengan motivasi untuk melindungi informasi daring (Chai *et al.*, 2009) dan menjadi prediktor pada intensi untuk mengadopsi perilaku perlindungan seperti perlindungan dari virus di internet (Lee, Larose dan Rifon, 2008; Milne, Labrecque dan Cromer, 2009).

H_6: *Self-efficacy* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

6. *Response Costs*

Response costs mengukur biaya yang harus dibayar seseorang (misalnya waktu, uang, dan usaha) ketika melakukan perilaku perlindungan (Zhang dan McDowell, 2009). Jika biaya yang harus dilakukan seorang individu untuk melakukan perilaku yang direkomendasikan tinggi, maka kemungkinan individu tersebut akan melakukannya menjadi rendah.

H_7: *Response costs* berpengaruh negatif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

3. Metode Penelitian

Penilitian ini memiliki tujuan untuk memahami hubungan antara *information privacy concern* dan perilaku perlindungan privasi dan hubungan komponen-komponen *Protection Motivation Theory*, yaitu *perceived severity, perceived vulnerability, response efficacy, self-efficacy, rewards,* dan *response costs,* dan *information privacy concern* pengguna Twitter di Indonesia. Peneliti ingin mencari hubungan antar variabel, yaitu: hubungan antar variabel *information privacy concern* dan variabel perilaku perlindungan privasi, hubungan antar variabel *information privacy concern* dan variabel *perceived severity*, hubungan antar variabel *information privacy concern* dan variabel *perceived vulnerability*, hubungan antar variabel *information privacy concern* dan variabel *response efficacy*, hubungan antar variabel *information privacy concern* dan variabel *rewards*, hubungan antar variabel *information privacy concern* dan variabel *self-efficacy*, dan hubungan antar variabel *information privacy concern* dan variabel *response costs*. Maka dari itu, metode kuantitatif merupakan metode penelitian yang paling cocok untuk diterapkan karena menurut Subana & Sudrajat (2005), metode kuantitatif digunakan ketika peneliti ingin menguji teori, mendeskripsikan statistik, dan mencari hubungan antar variabel.

Penelitian ini memiliki populasi yang besar, yaitu pengguna Twitter di Indonesia. Bila populasi dalam sebuah penelitian memiliki jumlah yang besar dan peneliti tidak dapat mempelajari keseluruhannya, peneliti dapat menggunakan sampel dari populasi tersebut. Karena populasi relatif homogen, maka digunakan teknik simple random sampling guna mendapatkan sampel. Akhirnya, sebanyak 156 responden terkumpul sebagai sampel.

Data dari 156 responden didapatkan melalui kuisioner. Pada penelitian ini, kuesioner dibuat dengan menggunakan layanan google form. Sebanyak 29 pertanyaan tertutup atau pertanyaan dengan pilihan jawaban disusun dalam kuesioner dan 5-point Skala Likert digunakan untuk mengukur jawaban responden.

4. Hasil dan Pembahasan

4.1 Uji Outlier

Dalam sebuah penelitian, sering kali ditemukan data outlier atau data yang karakteristiknya jauh berbeda dari data milik observasi lain dan memiliki nilai ekstrim (Ghozali, 2011). Data outlier dapat ditemukan dengan mencari mahalanombis distance (d_2) dan chi-squares (x_2) pada derajat kebebasan 29 dan tingkat

signifikansi 0,001. Jika nilai mahalanombis distance (d_2) kurang dari nilai chi-squares (x_2), berarti data tersebut bukan merupakan data outlier.

Setelah dilakukan uji outlier, tidak ditemukan adanya kasus multivariate outlier pada data. Nilai chi-square pada derajat kebebasan 29 dan tingkat signifikansi 0,001 adalah 58,301 dan seluruh nilai mahalanobis distance milik 156 data observasi yang dapat dilihat pada kolom mahalanobis d-squared menunjukkan angka kurang dari 58,301. Nilai mahalanobis distance paling tinggi dimiliki oleh data observasi ke-97 dengan 44,255 yang mana masih lebih kecil dari 58,301. Sementara nilai mahalanobis distance yang paling rendah dimiliki oleh data observasi ke-49 dengan 26,791 yang tentu saja jauh lebih kecil dari 58,301.

4.2 Uji Normalitas

Tujuan dilakukannya uji normalitas adalah untuk memastikan bahwa data yang diambil telah berdistribusi normal. Suatu data dapat dikatakan berdisstribusi normal apabila data tersebut memiliki critical ratio (nilai kritis) di antara nilai mutlak interval critical ratio yang telah ditentukan. Dengan signifikansi $\alpha = 1$ % atau 0,001, maka nilai mutlak adalah ±2.58. Sehingga nilai critical ratio data harus ≥ - 2,58 dan ≤ 2,58.

Tabel 1. Hasil Uji Normalitas

Indikator	**Nilai *Critical Ratio***
PPP6	-2.388
PPP5	-1,304
PPP4	-1,046
PPP3	-2,224
PPP2	-2,235
PPP1	-2,175
IPC4	-1,682
IPC3	-0,975
IPC2	-1,434
IPC1	-1,319
RC3	-1,589
RC2	-1,434
RC1	-1,483
SE3	-1,408
SE2	-0,543
SE1	-1,223
RW3	-1,789
RW2	-1,505
RW1	-0,685
RE3	-1,119

RE2	0,095
RE1	-1,862
PV3	-2,228
PV2	-1,803
PV1	-1,677
PS4	-1,737
PS3	-0,486
PS2	-1,842
PS1	-0,462

Berdasarkan tabel 1, dapat dilihat jika hasil dari nilai critical ratio seluruh indikator telah sesuai dengan standar nilai critical ratio yang ditentukan. Maka dari itu, data yang diperoleh telah terdistribusi normal.

4.3 Uji Multikolinieritas

Untuk memastikan tidak adanya gejala multikolinieritas (korelasi yang terlalu tinggi atau terlalu rendah) dalam hubungan antar variabel eksogen, dilakukan uji multikolinieritas (Sarjono, 2011). Mengutip dari Santoso (2015), suatu model dikatakan baik apabila model tersebut tidak memiliki korelasi antar variabel eksogen. Multikolinieritas dikatakan tidak terjadi jika nilai korelasi dalam hubungan antar variabel eksogen tidak lebih dari 0,9.

Tabel 2. Hasil Uji Multikolinieritas

			Estimate
Perceived_Severity	<->	Perceived_Vulnerability	0,358
Perceived_Severity	<->	Response_Efficacy	0,527
Perceived_Severity	<->	Rewards	0,228
Perceived_Severity	<->	Self_Efficacy	0,502
Perceived_Severity	<->	Response_Costs	-0,017
Perceived_Severity	<->	Information_Privacy_Concern	0,630
Perceived_Severity	<->	Perilaku_Perlindungan_Privasi	0,279
Perceived_Vulnerability	<->	Response_Efficacy	0,401
Perceived_Vulnerability	<->	Rewards	0,118
Perceived_Vulnerability	<->	Self_Efficacy	0,279
Perceived_Vulnerability	<->	Response_Costs	0,156
Perceived_Vulnerability	<->	Information_Privacy_Concern	0,401
Perceived_Vulnerability	<->	Perilaku_Perlindungan_Privasi	0,450
Response_Efficacy	<->	Rewards	0,238
Response_Efficacy	<->	Self_Efficacy	0,276
Response_Efficacy	<->	Response_Costs	-0,068
Response_Efficacy	<->	Information_Privacy_Concern	0,534

Response_Efficacy	<->	Perilaku_Perlindungan_Privasi	0,349
Rewards	<->	Self_Efficacy	0,030
Rewards	<->	Response_Costs	0,182
Rewards	<->	Information_Privacy_Concern	-0,042
Rewards	<->	Perilaku_Perlindungan_Privasi	-0,010
Self_Efficacy	<->	Response_Costs	0,047
Self_Efficacy	<->	Information_Privacy_Concern	0,548
Self_Efficacy	<->	Perilaku_Perlindungan_Privasi	0,266
Response_Costs	<->	Information_Privacy_Concern	-0,124
Response_Costs	<->	Perilaku_Perlindungan_Privasi	0,133
Information_Privacy_Concern	<->	Perilaku_Perlindungan_Privasi	0,424

Berdasarkan tabel 2, terlihat jika seluruh nilai korelasi dalam hubungan antar variabel telah lebih kecil dari 0,9. Kesimpulannya, tidak ditemukan adanya multikolinieritas dalam hubungan antar variabel milik penelitian ini.

4.4 Model Pengukuran untuk Uji Confirmatory Factor Analysis (CFA)

Kegunaan dari model pengukuran atau measurement model adalah untuk menunjukkan apakah variabel manifest telah merepresentasikan variabel laten. Hal ini dapat dicapai melalui analisis konstruk atau Confirmatory Factor Analysis (CFA). Variabel laten yang disusun berdasarkan teori memiliki variabel manifest (indikator). Dengan CFA, dapat diketahui kevalidan indikator-indikator tersebut sebagai pengukur unidimensionalitas dari konstruk laten. Secara lebih sederhana, yang dilakukan dalam model pengukuran adalah menguji validitas dan reliabilitas konstruk.

Kriteria yang digunakan dalam uji validitas konstruk adalah Convergent Validity (CV) dan Discriminant Validity (DV). Menurut Hair (dalam Adhikari dan Panda, 2018), CV dapat terpenuhi apabila harga loading factor suatu indikator > 0,5. Sementara DV terpenuhi apabila nilai Average Variance Extracted (AVE) milik variabel > 0,5. Yang dimaksud dengan Average Variance Extracted (AVE) adalah suatu koefisien yang berguna untuk menunjukkan varian dalam indikator melalui faktor umum (Widhiarso, 2016). Sementara untuk uji reabilitas konstruk, nilai Construck Reliability (CR) masing-masing variabel harus > 0,7 (Fornell & Larcker, 1981).

Tabel 3. Hasil Uji Validitas Konstruk dan Uji Reliabilitas Konstruk

Indikator	Loading Factor	CR	AVE
PS1	0,871	0,925	0,754
PS2	0,878		
PS3	0,839		
PS4	0,885		
PV1	0,913	0,940	0,839

PV2	0,919		
PV3	0,916		
RE1	0,914		
RE2	0,824	0,912	0,777
RE3	0,903		
RW1	0,924		
RW2	0,927	0,926	0,807
RW3	0,841		
SE1	0,910		
SE2	0,904	0,931	0,817
SE3	0,898		
RC1	0,931		
RC2	0,882	0,930	0,815
RC3	0,895		
IPC1	0,890		
IPC2	0,931	0,939	0,794
IPC3	0,896		
IPC4	0,846		
PPP1	0,884		
PPP2	0,816		
PPP3	0,905	0,952	0,767
PPP4	0,867		
PPP5	0,900		
PPP6	0,880		

Dari tabel 3, terlihat bahwa skor *loading factor* semua indikator > 0,5. Serta memiliki skor AVE > 0,5 dan CR > 0,7. Maka dapat disimpulkan jika seluruh variabel dan indikator yang dipakai bersifat valid dan reliabel.

4.5 Model Struktural untuk Uji Hipotesis

Setelah menguji validitas konstruk dan reabilitas indikator di model pengukuran, tahapan selanjutnya adalah mencari hasil model struktural. Kegunaannya adalah untuk menguji hipotesis. Dalam melakukan uji hipotesis, yang harus diperhatikan adalah nilai critical ratio (CR) dan p value. Ketika suatu hipotesis memiliki nilai CR > 1,96 serta nilai p value < 0,05, maka hipotesis tersebut dapat diterima.

Tabel 4. Hasil Uji Hipotesis

Hipotesis	Estimate	S.E.	C.R.	P	Label
H_1	0,409	0,076	5,360	***	par_28
H_2	0,372	0,091	4,086	***	par_22

H_3	0,128	0,062	2.062	0,039	par_23
H_4	0,277	0,082	3.386	***	par_24
H_5	-0,180	0,060	-2.969	0,003	par_25
H_6	0,248	0,066	3.768	***	par_26
H_7	-0,081	0,054	-1.510	0,131	par_27

Berdasarkan hasil uji hipotesis yang ditunjukkan oleh tabel 4, sebanyak enam hipotesis diterima dan satu hipotesis ditolak. Keenam hipotesis yang diterima adalah H_1, H_2, H_3, H_4, H_5, dan H_6. Sementara H_7 ditolak.

4.6 Pembahasan Hipotesis

Dari tujuh hipotesis yang diajukan, enam hipotesis diterima dan satu hipotesis ditolak. Berikut merupakan pembahasannya:

1. H_1: *Information privacy concern* berpengaruh positif dan signifikan terhadap perilaku perlindungan privasi pengguna Twitter di Indonesia.

   Berdasarkan hasil uji hipotesis yang telah dilakukan, diketahui bahwa *information privacy concern* berpengaruh positif dan signifikan terhadap perilaku perlindungan privasi pengguna Twitter di Indonesia, sehingga hipotesis diterima. Hasil penelitian ini sama dengan hasil dari penelitian Adhikari dan Panda (2018) dan penelitian Mohamed dan Ahmad (2012).

   Karena hipotesis diterima, maka dapat disimpulkan semakin tinggi *information privacy concern* pengguna Twitter di Indonesia, semakin tinggi pula perilaku perlindungan privasinya. Ketika seorang pengguna Twitter di Indonesia memiliki kepedulian terhadap *information privacy*, pengguna Twitter tersebut akan melakukan tindakan untuk melindungi privasinya.

2. H_2: *Perceived severity* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

   Berdasarkan hasil uji hipotesis yang telah dilakukan, diketahui bahwa *perceived severity* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia, sehingga hipotesis diterima. Hasil penelitian ini sama dengan hasil dari penelitian Adhikari dan Panda (2018), Mohamed dan Ahmad (2012), dan Wang (2019).

   Karena hipotesis diterima, maka dapat disimpulkan semakin tinggi *perceived severity*, semakin tinggi pula *information privacy concern*. Ketika seorang pengguna Twitter di Indonesia telah merasakan atau hanya sekadar mengetahui akibat dari kehilangan privasi informasi, pengguna tersebut akan memiliki *information privacy concern* yang tinggi.

3. H_3: *Perceived vulnerability* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

   Berdasarkan hasil uji hipotesis yang telah dilakukan, diketahui bahwa *perceived vulnerability* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia, sehingga hipotesis diterima. Hasil penelitian ini sama dengan hasil dari penelitian Adhikari

dan Panda (2018), Wang (2019), Crossler (2010), dan Dinev dan Hart (2004). Sementara penelitian Mohamed dan Ahmad (2012) memiliki hasil yang bertolak belakang.

Karena hipotesis diterima, maka dapat disimpulkan semakin tinggi *perceived vulnerability*, *information privacy concern*-nya juga akan meninggi. Ketika seorang pengguna Twitter merasa bahwa dirinya rentan akan ancaman privasi, pengguna Twitter juga akan semakin memperhatikan privasi informasinya.

4. H4: *Response efficacy* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

   Berdasarkan hasil uji hipotesis yang telah dilakukan, diketahui bahwa *response efficacy* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia, sehingga hipotesis diterima. Hasil penelitian ini sama dengan hasil dari penelitian Wang (2019) dan bertolak belakang dengan hasil penelitian penelitian Mohamed dan Ahmad (2012) dan penelitian Adhikari dan Panda (2018).

   Karena hipotesis diterima, maka dapat disimpulkan semakin besar *response efficacy*, semakin besar pula *information privacy concern* pengguna Twitter di Indonesia. Seorang pengguna Twitter yang yakin bahwa suatu koping respon seperti mengatur akun Twitter sebagai akun privat, pasti memiliki *information privacy concern*.

5. H_5: *Rewards* berpengaruh negatif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

   Berdasarkan hasil uji hipotesis yang telah dilakukan, diketahui bahwa *rewards* berpengaruh negatif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia, sehingga hipotesis diterima. Hasil ini sama dengan hasil dari penelitian milik Youn (2005).

   Karena hipotesis diterima dan hubungan yang ditunjukkan adalah negatif, artinya jika nilai *rewards* meningkat, maka nilai *information privacy concern* akan menurun. Begitupun sebaliknya, jika nilai *rewards* menurun, maka nilai *information privacy concern* akan meningkat. Keuntungan yang didapat pengguna Twitter di Indonesia ketika mereka tidak memperhatikan privasi informasi, seperti semakin banyaknya pengikut saat akun tidak dalam mode privat, sering kali membuat pengguna Twitter dengan suka rela mengorbankan privasi informasinya.

6. H_6: *Self-efficacy* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

   Berdasarkan hasil uji hipotesis yang telah dilakukan, diketahui bahwa *self-efficacy* berpengaruh positif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia, sehingga hipotesis diterima. Hasil penelitian ini sama dengan hasil dari penelitian Adhikari dan Panda (2018), Mohamed dan Ahmad (2012), dan Wang (2019).

   Karena hipotesis diterima, dapat disimpulkan jika *self-efficacy* tinggi, *information privacy concern* pun akan tinggi. Ketika seseorang pengguna Twitter memiliki *self-efficacy* atau kepercayaan

diri yang dalam konteks ini adalah kepercayaan diri mengatur setelan privasi, maka pengguna tersebut memiliki *information privacy concern*.

7. H_7: *Response costs* berpengaruh negatif dan signifikan terhadap *information privacy concern* pengguna Twitter di Indonesia.

   Berdasarkan hasil uji hipotesis, diketahui bahwa *response costs* tidak memiliki pengaruh yang signifikan pada *information privacy concern* pengguna Twitter di Indonesia, sehingga hipotesis ditolak. Temuan ini serupa dengan hasil penelitian milik Wang (2019).

   Karena hipotesis ditolak, maka dapat disimpulkan bahwa *response costs* tidak berpengaruh terhadap *information privacy concern*. Nilai dari *response costs* tidak akan menimbulkan efek apapun terhadap nilai *information privacy concern*. Hal ini mungkin dikarenakan pengguna Twitter di Indonesia tidak merasa mengatur setelan privasi adalah tindakan yang membutuhkan banyak biaya, waktu, dan usaha.

5. Simpulan

Penelitian ini memiliki tujuan untuk memahami hubungan *information privacy concern* dan perilaku perlindungan privasi serta hubungan antara komponen-komponen *Protection Motivation Theory*, yaitu *perceived severity, perceived vulnerability, response efficacy, self-efficacy, rewards,* dan *response costs,* dan *information privacy concern* pengguna Twitter di Indonesia. Data penelitian diambil dari 156 responden melalui kuesioner yang dibagikan di platform Twitter. Teknik analisis data yang digunakan adalah teknik analisis *Structural Equation Modeling* (SEM).

Sesuai dengan hasil dari penelitian, seorang pengguna Twitter yang memiliki *information privacy concern* akan melakukan perilaku perlindungan privasi. *Perceived severity* ditemukan memiliki berpengaruh positif terhadap *information privacy concern*. Hal ini menjelaskan bahwa ketika seorang pengguna Twitter pernah merasakan masalah privasi misalnya seperti pencurian identitas atau penyalahgunaan informasi pribadi, akan memiliki *information privacy concern* dan lebih mempedulikan privasi informasinya. Selanjutnya, *perceived vulnerability* ditemukan berpengaruh positif terhadap *information privacy concern*. Pengguna Twitter yang memiliki keyakinan bahwa dirinya memiliki potensi untuk mendapat masalah privasi akan cenderung memiliki *information privacy concern*. Variabel *response efficacy* pun mempengaruhi *information privacy concern* secara positif. Ini menunjukkan bahwa seorang pengguna yang melakukan tindakan-tindakan untuk mencegah dirinya mendapatkan masalah privasi, seperti mengatur akun Twitternya menjadi akun privat, pasti memiliki *information privacy concern. Rewards* menjadi satu-satunya yang berpengaruh negatif terhadap *information privacy concern* pengguna Twitter. Ketika seorang pengguna Twitter mendapat keuntungan dengan mengabaikan privasi informasinya, seperti memiliki banyak pengikut dan tweet yang diunggah akan dilihat lebih banyak orang, pengguna tersebut memiliki information privacy concern yang sangat rendah bahkan mungkin tidak memilikinya. Untuk *self-efficacy*, pengaruhnya adalah positif terhadap *information privacy concern*. Pengguna Twitter yang percaya bahwa ia memiliki kemampuan untuk melindungi informasi pribadinya

seperti kemampuannya dalam mengatur setelah privasi dan keamanan yang ada pada Twitter, adalah pengguna Twitter yang memiliki *information privacy concern*. Terakhir, *response costs* tidak memiliki pengaruh apapun pada *information privacy concern* pengguna Twitter. Sehingga, dapat dikatakan bahwa pengguna Twitter tidak memiliki masalah mengatur setelan privasi dan keamanan untuk akunnya. Waktu dan usaha bukanlah sesuatu yang mengganggu mereka dalam melakukan hal tersebut.

Daftar Pustaka

Acquisti, A. and Gross, R. 2006, 'Imagined Communities : Awareness , Information Sharing , and Privacy on the Facebook', pp. 36–58.

Adhikari, K. and Panda, R. K. 2018, 'Users ' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks Users ' Information Privacy Concerns and Privacy Protection Behaviors'. Taylor & Francis, 1762. doi: 10.1080/08911762.2017.1412552.

Afandi, I. A., Kusyanti, A. and Wardani, N. H. 2017, 'Analisis Hubungan Kesadaran Keamanan , Privasi Informasi , dan Perilaku', 1(9), pp. 783–792.

Akraman, R. and Priyadi, Y. 2018, 'Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia', 02, pp. 115–122.

Altman, I. 1975,. The environment and social behavior: Privacy personal space territory crowding. Monterey, CA: Brooks/Cole.

Arendt, Hannah. 1958,. The Human Condition 2nd ed. Chicago: University of Chicago Press.

Bandura, A. 1989, 'Regulation of cognitive processes through perceived self-efficacy.', *Developmental Psychology*, 25(5), pp. 729–735. doi: 10.1037//0012-1649.25.5.729.

Benevenuto, F. *et al.* 2010, 'Detecting Spammers on Twitter', *Ceas*, (Seventh annual Collaboration, Electronic messaging, AntiAbuse and Spam Conference), p. 10.

Bodendorf, F. and Kaiser, C. 2010, 'Detecting opinion leaders and trends in online communities', *4th International Conference on Digital Society, ICDS 2010, Includes CYBERLAWS 2010: The 1st International Conference on Technical and Legal Aspects of the e-Society*, pp. 124–129. doi: 10.1109/ICDS.2010.29.

Campbell, A. J. 1997, 'Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy', *Journal of Interactive Marketing*, 11(3), pp. 44–57. doi: 10.1002/(SICI)1522-7138(199722)11:33.0.CO;2-X.

Chai, S. *et al.* 2009, 'Internet and online information privacy: An exploratory study of preteens and early teens', *IEEE Transactions on Professional Communication*, 52(2), pp. 167–182. doi: 10.1109/TPC.2009.2017985.

Compeau, D., Higgins, C. A. and Huff, S. 1999, 'Social cognitive theory and individual reactions to computing technology: A longitudinal study', *MIS Quarterly: Management Information Systems*, 23(2), pp. 145–158. doi: 10.2307/249749.

Crossler, R. E. 2010, 'Protection motivation theory: Understanding determinants to backing up personal

data', *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 1–10. doi: 10.1109/HICSS.2010.311.

Dinev, T. and Hart, P. 2004, 'Internet privacy concerns and their antecedents -measurement validity and a regression model', *Behaviour and Information Technology*, 23(6), pp. 413–422. doi: 10.1080/01449290410001715723.

Kemp, Simon. 2020,. "Digital 2020: Indonesia". https://datareportal.com/reports/digital-2020-indonesia. Diunduh pada 30 Desember 2020.

Korzaan, M. L. and Boswell, K. T. 2008, 'The influence of personality traits and information privacy concerns on behavioral intentions', *Journal of Computer Information Systems*, 48(4), pp. 15–24. doi: 10.1080/08874417.2008.11646031.

Lee, D., Larose, R. and Rifon, N. 2008, 'Keeping our network safe: A model of online protection behaviour', *Behaviour and Information Technology*, 27(5), pp. 445–454. doi: 10.1080/01449290600879344.

Lim, J. S., Heinrichs, J. H. and Lim, K. S. 2017, 'Gender and Hedonic Usage Motive Differences in Social Media Site Usage Behavior', *Journal of Global Marketing*. Taylor & Francis, 30(3), pp. 161–173. doi: 10.1080/08911762.2017.1308615.

Maddux, J. E. and Rogers, R. W. 1983, 'Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change', *Journal of Experimental Social Psychology*, 19(5), pp. 469–479. doi: 10.1016/0022-1031(83)90023-9.

Malhotra, N. K., Kim, S. S. and Agarwal, J. 2004, 'Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model', *Information Systems Research*, 15(4), pp. 336–355. doi: 10.1287/isre.1040.0032.

Milne, G. R., Labrecque, L. I. and Cromer, C. 2009, 'Toward an understanding of the online consumer's risky behavior and protection practices', *Journal of Consumer Affairs*, 43(3), pp. 449–473. doi: 10.1111/j.1745-6606.2009.01148.x.

Mohamed, N. and Ahmad, I. H. 2012, 'Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia', *Computers in Human Behavior*. Elsevier Ltd, 28(6), pp. 2366–2375. doi: 10.1016/j.chb.2012.07.008.

Rogers, R. W. 1975, 'A Protection Motivation Theory of Fear Appeals and Attitude Change1', *The Journal of Psychology*, 91(1), pp. 93–114. doi: 10.1080/00223980.1975.9915803.

Rohani, V. A. 2009, 'On Social Network Web Sites : Definition , Features , Architectures and Analysis Tools', 1, pp. 3–11.

Son, J. Y. and Kim, S. S. 2008, 'Internet users' information privacy-protective responses: A Taxonomy and a nomological model', *MIS Quarterly: Management Information Systems*, 32(3), pp. 503–529. doi: 10.2307/25148854.

Statista. 2020,. "Leading countries based on number of Twitter users as of October 2020". https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/.

Diunduh 30 Desember 2020.

Subana, M., & Sudrajat. 2011,. Dasar –Dasar Penelitian Ilmiah. Bandung: Pustaka Setia.

Wang, D. 2019,. A Study of Determinants of Teenagers' Privacy Protection Intentions on Social Networking Sites. The Educational Review, USA, 3(10), 152–163. https://doi.org/10.26855/er.2019.10.004

Wang, T., Duong, T. D. and Chen, C. C. 2016, 'Intention to disclose personal information via mobile applications: A privacy calculus perspective', *International Journal of Information Management*. Elsevier Ltd, 36(4), pp. 531–542. doi: 10.1016/j.ijinfomgt.2016.03.003.

Widyaningsih, Y. 2018, 'Perilaku perlindungan privasi pada pengguna instagram di kalangan siswa sekolah menengah atas kota surabaya 1 yohana widiyaningsih 2', *Palimpsest*. Available at: http://repository.unair.ac.id/74816/3/JURNAL_Fis.IIP.59 18 Wid p.pdf.

Xu, H. *et al*. 2012, 'Measuring mobile users' concerns for information privacy', *International Conference on Information Systems, ICIS 2012*, 3(Ftc 2009), pp. 2278–2293.

Zhang, L. and McDowell, W. C. 2009, 'Am i really at risk? Determinants of online users' intentions to use strong passwords', *Journal of Internet Commerce*, 8(3–4), pp. 180–197. doi: 10.1080/15332860903467508.