

Literasi Privasi dan Perilaku Proteksi Konsumen Belanja Daring Generasi Y

Ananda Dwitha Yuniar & Alan Sigit Fibrianto

Universitas Negeri Malang
Jl. Semarang No. 5 Malang 65145
Email: ananda.dwitha.fis@um.ac.id

Abstract: *Inhibited conditions in communication process of the online shopping have led to privacy concerns. Some previous studies show privacy paradox. Measurements of online privacy literacy play an important role to fill the paradoxical privacy gaps. Moderated regression analysis (MRA) is used to measure causality between these variables with privacy breach experiences as the moderate variables. The total number of respondents is 283. The research finding shows that the higher the level of online privacy literacy, the user will be aware of the violation of privacy and able to be protective. However, violations of privacy cannot be considered as a trigger for consumers' protective behavior.*

Keywords: *online shopping, privacy literacy, privacy paradox*

Abstrak: *Kondisi yang terbatas dalam proses komunikasi belanja daring memunculkan perdebatan mengenai isu privasi. Beberapa penelitian sebelumnya menyatakan bahwa kekhawatiran konsumen terhadap privasi tidak memiliki konsistensi terhadap perilaku (paradoks privasi). Pengukuran literasi privasi memiliki peran yang cukup penting untuk mengisi gap paradoks privasi tersebut. Pengukuran kausalitas antarvariabel ini menggunakan moderated regression analysis (MRA) dengan pengalaman pelanggaran privasi sebagai variabel moderasi. Total responden yang berpartisipasi berjumlah 283 orang. Temuan penelitian menunjukkan bahwa semakin tinggi tingkat literasi daring pengguna, semakin sadar pula pengguna tersebut terhadap pelanggaran privasi dan memiliki kemampuan bersikap protektif. Namun, pelanggaran privasi tidak bisa dianggap sebagai pemicu tindakan protektif konsumen.*

Kata Kunci: *belanja online, literasi privasi, paradoks privasi*

Belanja *online* atau dalam jaringan (daring) bukan semata-mata kegiatan ekonomi tentang pertukaran uang dan barang. Belanja daring merupakan kegiatan komunikasi, interaksi, dan transaksi yang dilakukan antara penjual dan pembeli dengan menggunakan jaringan internet yang dimediasi layar komputer atau *smartphone*. Proses komunikasi dalam belanja daring meliputi hubungan interpersonal antara penjual dan pembeli hingga terjadi pertukaran

informasi. Berdasarkan karakteristiknya, belanja daring memiliki aturan dan kondisi yang terbatas dalam proses komunikasi maupun transaksinya, serta berbeda dengan proses belanja konvensional (*brick mortal*) yang dapat diselesaikan dalam satu waktu (Trepte, dkk., 2015, h. 336). Keterbatasan komunikasi dalam belanja daring menyebabkan komunikasi antara penjual dan pembeli berbasis pada kepercayaan (*trust*).

Keterbatasan serta perbedaan karakteristik antara belanja daring dengan belanja konvensional ini membuat konsumen harus mampu mengatasi segala tantangan, termasuk risiko privasi. Platform belanja daring yang memiliki fungsi utama sebagai *marketplace* dan menyumbang pertumbuhan perekonomian digital suatu negara dikenal dengan sebutan *e-commerce*. Menurut Metzger (2007, h. 336), privasi memiliki implikasi terhadap *e-commerce* karena melibatkan pengungkapan informasi pribadi, seperti nomor telepon seluler (ponsel), alamat rumah, alamat surat elektronik (surel), dan nomor kartu kredit. Mooney (2015, h. 8) menyatakan bahwa informasi privasi merupakan kerahasiaan pemikiran dan perlu dilindungi dari berbagai pelanggaran privasi, seperti *doxing* dan *hacking*. Pengungkapan informasi pribadi dalam proses belanja daring memunculkan isu penting mengenai privasi bagi konsumen karena konsumen diharuskan mengungkapkan informasi pribadi saat melakukan transaksi.

Proses pengungkapan informasi pribadi menimbulkan kepedulian konsumen terhadap privasi (*privacy concern*). Dalam transaksi *e-commerce*, kepedulian terhadap privasi muncul ketika konsumen berpotensi kehilangan kendali atas informasi pribadinya (Metzger, 2007, h. 336). Beberapa penelitian menaruh perhatian mengenai *privacy concern* konsumen dalam konteks belanja daring, khususnya *e-commerce* (Vasileiadis, 2014; Gupta & Dubey, 2016; Fortes & Rita, 2016). Hasil penelitian menunjukkan bahwa kepedulian terhadap privasi tidak memiliki konsistensi terhadap perilaku. Hal tersebut

berarti bahwa konsumen telah memiliki kepedulian dan kekhawatiran terhadap ancaman dan risiko privasi ketika mereka mengungkapkan informasi pribadi melalui internet, tetapi mereka tidak melakukan tindakan proteksi terhadap privasi mereka.

Tidak adanya konsistensi antara kekhawatiran konsumen terhadap privasi dengan perilaku konsumen ini disebut sebagai *privacy paradox* atau paradoks privasi (Kokolakis, 2015, h. 2). Paradoks privasi dapat memiliki pengaruh yang signifikan terhadap pertumbuhan *e-commerce* karena semakin paradoksnya perilaku konsumen terhadap privasi memudahkan pihak *e-commerce* mengumpulkan informasi pribadi dan preferensi konsumen sebanyak-banyaknya (Büchi, Just, & Latzer, 2016, h. 3). Informasi pribadi konsumen yang dihimpun dapat menjadi *big data* atau *e-commerce database* (basis data) yang memiliki nilai bisnis tinggi dan juga menyebabkan potensi pelanggaran privasi informasi lebih besar (Shinta, 2009, h. 53). Pelanggaran privasi ini disebabkan oleh penjualan informasi pribadi konsumen oleh *e-commerce* yang bersangkutan kepada perusahaan lain tanpa izin untuk kepentingan tertentu.

Perlindungan informasi pribadi konsumen merupakan salah satu isu penting dalam *e-commerce* di Indonesia (Kearney, 2015, h. 11) karena belum ada undang-undang yang mengatur secara khusus perlindungan informasi pribadi konsumen oleh pemerintah. Padahal di negara maju informasi maupun data pribadi konsumen mendapatkan perlindungan undang-undang.

Selain itu, data Google & Temasek (2016) menyatakan bahwa tantangan yang dihadapi oleh *e-commerce* Indonesia adalah sentimen konsumen yang buruk akibat adanya kecurangan dalam memanfaatkan informasi pribadi konsumen tanpa izin. Memanfaatkan, menghimpun, dan menyalahgunakan informasi pribadi konsumen merupakan bentuk pelanggaran hukum, tetapi kesadaran ini belum menjadi perhatian khusus di Indonesia karena kurangnya *peer group* yang mewadahi dan mendukung perdebatan mengenai perlindungan privasi.

E-commerce yang beroperasi di Indonesia telah membangun pendekatan untuk melindungi informasi pribadi atau privasi konsumen melalui fitur kebijakan privasi. Namun pada kenyataannya, sistem keamanan dan kebijakan privasi yang digunakan di situs *e-commerce* tidak sesuai dengan standar keamanan digital (Jumiati, Rosdiana, & Kusumastuti, 2017, h. 60). Pada tahun 2016, sistem keamanan yang tidak sesuai standar ini dibuktikan dengan terjadinya *cyber crime* pada platform besar di Indonesia, yakni *Tokopedia* dan *BukaLapak*. Kedua platform *e-commerce* tersebut diretas. Bahkan pelaku menyatakan bahwa mereka dengan leluasa dapat mengambil data penting konsumen, seperti alamat surel, kata sandi, nomor rekening, hingga nomor kartu kredit (Nistanto, 2016). Kejadian ini membuktikan bahwa kedua platform *e-commerce* besar sekelas *BukaLapak* dan *Tokopedia* pun tidak sepenuhnya dapat menjamin keamanan informasi pribadi konsumen. Melalui kejadian ini, tidak dapat dipungkiri bahwa

potensi distorsi informasi pribadi konsumen dapat terjadi pada *e-commerce* baru.

Problem paradoks atau ketidaksesuaian yang dimiliki oleh konsumen mendorong peneliti berasumsi bahwa konsumen belum melek penyalahgunaan informasi pribadi. Dalam penelitiannya, Trepte, dkk. (2015, h. 362) menyatakan bahwa kurangnya pengetahuan tentang tata cara melindungi privasi pengguna membuat tidak adanya kesesuaian dengan perilaku. Pengguna sebenarnya telah berusaha untuk mengontrol informasi mereka, tetapi mengalami masalah dalam praktiknya karena kurangnya literasi privasi daring. Park (2013, h. 217) menyatakan bahwa literasi privasi daring merupakan prinsip yang mendorong, mendukung, dan memberdayakan pengguna untuk melakukan kontrol atas informasi pribadi mereka. Selain itu, literasi privasi daring dipahami sebagai bagian dasar yang penting dalam domain perdebatan privasi digital (Park, Campbell, & Kwak, 2012, h. 1019).

Kegunaan internet dapat dirasakan oleh pengguna ketika mereka melakukan pengungkapan informasi pribadi. Pengguna sering tidak menyadari bahwa jejak aktivitas penjelajahan internet maupun pembelian daring tersimpan oleh sistem (Acquisti, Brandimarte, & Loewenstein, 2015, h. 510). Jejak dan informasi pribadi konsumen, mulai dari alamat surel, informasi akun bank, *history*, *cookie*, hingga alamat *Internet Protocol* (IP), dapat dijadikan aset data untuk kepentingan bisnis melalui sistem algoritma (Latzer, Hollnbuchner, Just, & Saurwein, 2014). Begitu pula dalam konteks belanja daring, informasi pribadi yang diberikan

sebagai ketentuan transaksi dapat menjadi *big data* yang menguntungkan. Memanfaatkan basis data konsumen dianggap sebagai strategi pemasaran baru yang dapat memiliki pengaruh besar pada peningkatan perekonomian digital (Agustiyanti, 2017) dan meningkatnya potensi pelanggaran privasi.

Kini, konsumen belanja daring mulai peduli dengan distorsi privasi mereka. Survei Mastel dan APJII (2016) menyatakan bahwa 98 persen konsumen daring membutuhkan perlindungan hukum dan kebijakan pemerintah mengenai data pribadi. Namun demikian, beberapa penelitian menyatakan bahwa *privacy concern* tidak memiliki konsistensi terhadap perilaku. Misalnya, penelitian yang dilakukan oleh Fortes dan Rita (2016) yang menyatakan bahwa konsumen merasakan tingkatan risiko ketika melakukan belanja daring, namun konsumen tetap melakukan keterbukaan berulang. Sementara itu, penelitian Vasileiadis (2014) menyatakan bahwa risiko konsumen terkait keamanan informasi privasi tidak menghalangi mereka untuk mengadopsi *mobile commerce*. Sedangkan penelitian Carrascal, Riederer, Erramilli, Cherubini, dan Oliveira (2013) menunjukkan bahwa individu menyadari informasi pribadi mereka tidak terlindungi, namun mereka tetap bersedia memberikannya.

Secara konseptual, elemen pengukuran literasi privasi ketiga penelitian tersebut memiliki kesamaan, namun ada perbedaan dengan penelitian Trepte, dkk. (2015), yaitu penelitian tersebut lebih mengedepankan pengetahuan tentang aspek hukum dan regulasi. Sementara itu, literasi privasi daring yang digunakan dalam penelitian di

ranah ilmu komunikasi ini adalah aspek-aspek yang mampu mengukur pengetahuan mengenai penggunaan media daring.

Secara singkat, literasi privasi merupakan kombinasi dari penerangan fakta (*knowing that*) dan prosedural (*knowing how*) pengetahuan tentang privasi daring. Dalam penelitian ini, aspek penerangan fakta literasi privasi mengacu pada pengetahuan pengguna mengenai kesadaran tentang praktik kerja institusi dan pemahaman terhadap kebijakan privasi. Sedangkan pengetahuan prosedural mengacu pada kemampuan pengguna dalam melakukan kontrol atau proteksi atas informasi pribadi ketika melakukan belanja daring.

Salah satu alasan utama yang mendorong konsumen memilih berbelanja daring adalah faktor kenyamanan yang memungkinkan aktivitas tersebut dapat dilakukan di manapun dan kapanpun. Faktor lain yang juga menjadi pendorong adalah ketersediaan dan keberagaman produk, komparasi harga, dan penghematan biaya (Rose, Clark, Samouel, & Hair, 2012). Namun, berbelanja daring juga tidak terlepas dari beberapa kekurangan. Lissitsa dan Kol (2016, h. 310) menjelaskan bahwa salah satu kekurangan paling riskan dalam berbelanja daring adalah adanya ancaman atau risiko terhadap informasi pribadi konsumen yang datang dari pihak *e-vendor*, sehingga konsumen harus memiliki kemampuan proteksi untuk menghindari hal tersebut. Hal ini sesuai dengan pernyataan Trepte, dkk. (2015, h. 339), yaitu pengetahuan prosedural sebagai elemen literasi privasi daring mengacu pada kemampuan pengguna melakukan kontrol atau proteksi atas informasi pribadi mereka.

Kemampuan pengguna dapat diukur menggunakan basis *Protection Motivation Theory* (PMT). Rogers menyatakan bahwa ‘*protecting motivation*’ merupakan faktor yang mengarahkan individu untuk mencegah ancaman/risiko (Youn, 2009, h. 397). PMT disusun sebagai dua subproses perantara yang digunakan konsumen dalam mengevaluasi ancaman (*threat-appraisal process*) dan memilih alternatif (*coping appraisal*). Dalam konteks *privacy behavior*, konsumen dapat mendorong motivasi proteksi mereka dan terlibat dalam perilaku pengurangan risiko (Youn, 2009, h. 399).

Strategi yang dapat diterapkan oleh pengguna meliputi penghindaran, yakni mengabaikan ancaman hingga memilih untuk tidak menggunakan internet. Menurut Youn (2009, h. 399), ada dua indikator untuk mengukur kemampuan penghindaran pengguna, yakni *fabricate* dan *refrain*. *Fabricate* merupakan tanggapan konsumen untuk memalsukan informasi pribadi mereka. Sedangkan *refrain* adalah kemampuan konsumen meningkatkan kontrol dalam melakukan interaksi dengan *website* (*e-commerce*). Cho, Sánchez, dan Lim (2009, h. 407) menyatakan bahwa semakin besar kepedulian individu tentang pengumpulan informasi oleh para pemasar dan praktik pengambilan informasi lainnya, maka semakin besar pula kemungkinan seseorang mencoba mengadopsi *privacy protection behaviour*.

Penelitian terbaru oleh Büchi, Just, dan Latzer (2016) menyatakan bahwa *privacy protection behaviour* berfokus pada *self-help* dalam tindakan proteksi. *Self-help* berkaitan

dengan kemampuan pengguna dalam menggunakan internet. Dengan kata lain, *self-help* dapat digunakan untuk mengukur kemampuan pengguna untuk melawan distorsi privasi. *Self-help* meliputi aspek teknis termasuk *privacy-enhancing technologies*, *cookie management*, hingga *do-not-track technologies*. Kemampuan *self-help* proteksi privasi ini penting karena organisasi/platform mendapat keuntungan dari pengumpulan dan pertukaran data pribadi konsumen (Saurwein, Just, & Latzer, 2015). Selain itu, Büchi, Just, dan Latzer (2016, h. 12) juga menambahkan bahwa kemampuan perilaku proteksi tersebut juga didukung adanya pengalaman pelanggaran privasi (*privacy breaches*). Perilaku proteksi didukung oleh sikap pengguna untuk melindungi informasi pribadi mereka dan menjadi penguat perilaku karena adanya pengalaman atau kecurigaan pelanggaran privasi.

Artikel ini menyajikan hasil penelitian yang mengukur literasi privasi konsumen dalam belanja daring. Hasil tersebut merupakan jawaban terhadap dua pertanyaan. Pertama, seberapa besar pengaruh literasi privasi daring konsumen generasi Y (gen Y) urban terhadap kemampuan bersikap proteksi ketika melakukan belanja daring? Kedua, sejauh mana pengaruh variabel pengalaman pelanggaran privasi mampu memoderasi elemen literasi privasi daring terhadap kemampuan bersikap proteksi?

Penelitian terdahulu yang terkait dengan literasi privasi dalam media daring serta kemampuan individu dalam melindungi informasi privasi mereka dapat ditelusuri dari tiga penelitian. Pertama, penelitian Park

(2013) yang bertujuan untuk mengetahui sejauh mana peran dari literasi digital terhadap kemampuan kontrol terhadap informasi pribadi pengguna media daring. Variabel bebas dalam penelitian Park adalah literasi yang mencakup tiga hal, yaitu keakraban dengan aspek teknis, kesadaran terhadap praktik institusi (*e-commerce*), dan pemahaman terhadap kebijakan privasi. Variabel terikatnya adalah perilaku kontrol atas informasi yang meliputi dimensi sosio-teknis. Hasil penelitian tersebut menunjukkan bahwa pengguna yang terliterasi dengan baik lebih mempraktikkan kontrol informasi dibandingkan dengan pengguna yang kurang terliterasi. Faktor sosio-demografi, seperti tingkat pendapatan dan pendidikan juga berpengaruh positif terhadap kemampuan mengontrol informasi.

Kedua, penelitian Trepte, dkk. (2015) yang bertujuan untuk mengelaborasi peran dari literasi privasi dalam menjelaskan perilaku konsumen dan sikap (*attitude*) pengguna tentang privasi. Metode yang digunakan adalah analisis isi. Literasi privasi dalam penelitian ini mengacu pada pengetahuan dan strategi *data protection*. Mereka membuat konsep untuk mengetahui dan menganalisis tingkat literasi privasi yang disebut *online privacy literacy scale* (OPLIS) yang terdiri dari lima elemen, yaitu pengetahuan tentang praktik organisasi, pengetahuan tentang aspek teknis, pengetahuan tentang aspek hukum dan legal, pengetahuan tentang *European directives on privacy*, dan pengetahuan tentang regulasi informasi pribadi. Hasil penelitian tersebut menunjukkan bahwa individu yang peduli terhadap privasi sebenarnya ingin

bertindak sesuai dengan kepeduliannya, tetapi kurangnya literasi privasi menghambat mereka berperilaku konsisten.

Ketiga, penelitian Büchi, Just, dan Latzer (2016) yang lebih berfokus pada kemampuan pengguna media daring dalam melakukan proteksi diri terhadap informasi pribadi mereka. Pendekatan pada fenomena ini didasarkan pada asumsi bahwa *protective behaviour* tergantung pada sikap terhadap privasi, pengalaman, dan tingkat keterampilan menggunakan internet. Ada beberapa elemen pengukur kemampuan *self-protection*, antara lain pengaturan, penyamaran, hingga penghapusan. Studi tersebut menerangkan bahwa perilaku proteksi didasarkan pada pengalaman pelanggaran terhadap privasi mereka. Seharusnya individu yang memiliki keahlian dan keterampilan digital dapat menghindari pelanggaran privasi dan tidak menyebabkan individu merasakan ancaman yang lebih besar.

Ketiga penelitian tersebut tidak menyebutkan secara spesifik konteks yang mereka gunakan, baik dalam media sosial maupun belanja daring. Masing-masing penelitian juga memiliki perspektif, variabel, metode, dan wilayah generalisasi yang berbeda, meskipun berada dalam satu topik pembahasan yang sama, yaitu peran literasi privasi dalam media daring. Penelitian Büchi, Just, dan Latzer (2016) di atas menunjukkan adanya paradoks privasi, yaitu keterampilan (*skills*) dalam mengoperasikan media digital tidak berpengaruh terhadap perilaku proteksi, sehingga perlu adanya peran literasi media daring untuk mengukur sejauh mana

pengetahuan (*knowledge*) pengguna, bukan sebatas kemampuannya saja.

Penelitian ini menggunakan literasi privasi dalam konteks belanja daring, sehingga terlihat perbedaan dan pengembangan dari penelitian-penelitian sebelumnya. Penelitian ini pun berbeda karena mengisi kekosongan penelitian di Indonesia yang mengkaji tentang literasi privasi. Oleh karena itu, penelitian ini memiliki kebaruan dalam kajian ilmu komunikasi, khususnya tentang literasi dalam media digital.

METODE

Survei daring dilakukan untuk mengukur dan menganalisis sejauh mana tingkat literasi privasi konsumen belanja daring memengaruhi kemampuan berperilaku protektif atas informasi pribadi. Survei daring tersebut menggunakan *Google Forms* yang disebarluaskan selama dua bulan dengan perhitungan jumlah sampel minimum yang harus terkumpul

menggunakan formula Lemeshow, yaitu sebanyak 270 responden. Penelitian ini menggunakan paradigma positivistik, sehingga pengumpulan data dan interpretasi data bersifat objektif. Peneliti diposisikan terpisah dari objek penelitian, sehingga tidak ada intervensi jawaban yang diberikan oleh responden penelitian. Responden yang menjadi objek penelitian memiliki dua karakteristik. Pertama, konsumen belanja daring di Surabaya dan Jabodetabek (Jakarta-Bogor-Depok-Tangerang-Bekasi). Kedua wilayah tersebut dipilih karena memiliki jumlah pelaku belanja daring tertinggi di Indonesia (MARS Indonesia, 2016). Kedua, pelaku belanja daring berusia milenial atau biasa disebut sebagai generasi Y (gen Y), yaitu orang dalam rentang usia 18-30 tahun. Generasi ini disebut sebagai *digital natives* dan berada pada rentang usia yang menjadi target utama *e-commerce* dalam memasarkan produk maupun jasa.

Tabel 1 Pengukuran Variabel Literasi Privasi Daring

No	Variabel	Indikator	Pengukuran	Sumber	
1.	Literasi Privasi Daring	Keakraban dengan aspek teknis	Keakraban dengan aspek teknis yang terdapat pada <i>e-commerce</i> , mulai dari aspek yang bersifat generik hingga teknis yang berbasis keamanan digital.	Likert: Tidak sama sekali – Sangat familier	Park (2013); Gupta dan Dubey (2016)
		Kesadaran terhadap praktik institusi	Kesadaran terhadap praktik yang dilakukan <i>e-commerce</i> , seperti promosi dan iklan.	True – False	Park (2013)
		Pemahaman mengenai kebijakan yang berlaku di Indonesia	Pemahaman mengenai kebijakan, legalitas, dan aturan yang berkaitan dengan privasi yang berlaku.	True – False	
2.	Kemampuan berperilaku protektif	Kemampuan mengabaikan, menahan diri, mengatur, memonitor, memalsukan, dan menghapus informasi pribadi daring.	Likert: Tidak sama sekali – Sangat sering	Youn (2009); Park, (2013); Büchi, Just, dan Latzer (2016)	
3.	Pelanggaran Privasi	Pelanggaran penyalahgunaan	Binary (0-1)	Büchi, Just, dan Latzer (2016)	

Sumber: Olahan Peneliti

Kuesioner daring yang digunakan sebagai alat pengumpul data penelitian telah diuji coba. Data awal yang diuji validitasnya adalah *pretest* kuesioner yang disebarakan kepada konsumen urban di kedua lokasi penelitian. Pengujian validitas instrumen dilakukan dengan cara mengorelasikan setiap skor item dengan skor total menggunakan teknik korelasi Pearson (*Product Moment*). Tingkat signifikansi 10 persen menghasilkan r_{tabel} 0,288. Pengukuran reliabilitas dikatakan memberikan hasil yang konsisten atau reliabel jika nilai *Cronbach's Alpha* > 0,60.

HASIL

Pengujian validitas masing-masing variabel penelitian menunjukkan adanya satu item pertanyaan instrumen yang tidak valid atau $r_{tabel} > r_{IT}$ yakni variabel *Technology Familiarity* (X1), item pertanyaan (TF2), mengenai tingkat keakraban responden pada kegunaan utama dari surel pribadi, sehingga item

pertanyaan tersebut dibuang dan tidak digunakan sebagai alat ukur. Selain itu, semua nilai koefisien korelasi item atau sebanyak 48 item pertanyaan menghasilkan skor total (r_{IT}) > dari nilai korelasi tabel (r_{tabel}). Dengan demikian, item kuesioner pada variabel X1, X2, X3, Y, dan moderasi Z dinyatakan valid dan dapat digunakan sebagai alat pengumpul data penelitian. Pengukuran reliabilitas pada penelitian ini menggunakan *one shot*, yaitu pengukuran keandalan butir pertanyaan dengan sekali penyebaran kuesioner pada responden. Selanjutnya, hasil skor tersebut diukur korelasinya. Berdasarkan ringkasan hasil pengujian reliabilitas instrumen penelitian diketahui bahwa semua nilai *Cronbach's Alpha* > 0.6. Dengan demikian, item pertanyaan kuesioner pada masing-masing variabel dinyatakan reliabel atau konsisten dalam pengukuran masing-masing variabel.

Setelah mengukur dan menghitung hasil penelitian dalam bentuk data statistik dengan menggunakan SPSS 20, peneliti

Tabel 2 Hasil Uji Validitas dan Reliabilitas *One Shot*

Variabel	Koefisien Validitas (M)	Korelasi Tabel	Keterangan
X1	0.738	> 0.288	Valid
X2	0.538	> 0.288	Valid
X3	0.580	> 0.288	Valid
Y	0.650	> 0.288	Valid
Z	0.922	> 0.288	Valid

Variabel	Koefisien Reliabilitas	Batas Toleransi	Keterangan
X1	0.915	< 0.6	Reliabel
X2	0.643	< 0.6	Reliabel
X3	0.701	< 0.6	Reliabel
Y	0.925	< 0.6	Reliabel
Z	0.822	< 0.6	Reliabel

Sumber: Olahan Peneliti

melakukan pembahasan dengan tujuan menginterpretasikan, memperjelas makna, dan secara lebih detail menjabarkan gambaran nyata variabel yang diteliti dengan pembuktian teori-teori yang digunakan. Dengan demikian, pembahasan ini diharapkan dapat memudahkan pembaca dalam memahami hasil penelitian yang akan digambarkan secara objektif sesuai data empirik.

Penelitian ini menggunakan dua tahap analisis. Pertama, menggunakan deskriptif statistik agar pembaca memahami kondisi garis besar objek dan variabel penelitian. Kedua, data penelitian diolah dengan analisis regresi moderasi (MRA) untuk memoderasi variabel pengetahuan tentang aspek teknis (X1), pengetahuan tentang praktik institusi (X2) (dalam penelitian ini berkaitan dengan belanja daring), dan pengetahuan tentang kebijakan privasi (X3) terhadap variabel Y, yaitu kemampuan pengguna untuk bersikap protektif terhadap informasi pribadi mereka ketika melakukan belanja daring pada *e-commerce*. Pembahasan lebih lengkap terlihat dalam tabel 3.

Sebagian besar responden generasi Y yang berpartisipasi dalam penelitian

ini berumur antara 22-25 tahun sebesar 57,6 persen dari total 283 responden dan didominasi oleh responden perempuan, yaitu sebesar 60,8 persen. Selain itu, responden yang berdomisili di Jabodetabek dan Surabaya memiliki persentase yang hampir seimbang.

Tabel 4 menunjukkan bahwa pengetahuan konsumen tentang privasi dalam belanja daring di Indonesia berada pada rata-rata. Hal ini terlihat pada elemen keakraban dengan aspek teknis yang memiliki $M=3.13$ dan $SD=0.95$. Konsumen belanja daring lebih familier dengan aspek-aspek teknis yang bersifat generik, seperti HTML, IP Address, Cookies, dan Firewalls, serta dianggap sebagai aspek teknis yang mampu melindungi informasi pribadi ketika belanja pada platform *e-commerce*.

Sementara itu, pada elemen kesadaran dengan praktik *e-commerce*, seperti iklan, spam, dan phishing, konsumen Indonesia telah memiliki pengetahuan karena mampu menjawab dengan benar $M=0.72$ dan $SD=0.45$. Namun, sebagian konsumen masih memiliki pengetahuan yang terbilang lemah, sehingga mereka belum menyadari informasi pribadi mereka disalahgunakan.

Tabel 3 Statistik Deskriptif Demografi Responden (N = 283)

	%		%
Umur		Gender	
18 – 21	6.7	Perempuan	60.8
22 – 25	57.6	Laki-laki	39.2
26 – 29	35.3	Frekuensi Belanja Daring	
Domisili		Cukup Sering	32.9
Jabodetabek	47.3	Sering	50.5
Surabaya	52.7	Sering Sekali	16.6

Sumber: Olahan Peneliti

Tabel 4 Distribusi Pengetahuan Responden (N=283)

Variabel		M	SD
Literasi Privasi Daring			
Keakraban dengan aspek teknis		3.13	0.95
Kesadaran terhadap praktik <i>e-commerce</i>		0.72	0.45
Pemahaman terhadap kebijakan privasi		0.69	0.46
Kemampuan Proteksi Privasi		2.85	1.17

Variabel Z		Persepsi Responden		M
		Tidak	Ya	
Z1	%	44.2	55.8	0.56
Z2	%	47.3	52.7	0.53

Sumber: Olahan Peneliti

Sedangkan pada elemen ketiga, pemahaman terhadap kebijakan privasi $M=0.69$ dan $SD=0.46$ menyatakan bahwa konsumen belanja daring cukup paham tentang kebijakan privasi, namun banyak juga responden yang belum mengetahui kebijakan-kebijakan pemerintah yang berlaku di Indonesia tentang perlindungan informasi pribadi. Sebagian besar responden menyatakan pernah mengalami pelanggaran privasi dan mereka kini sedang mengalami pelanggaran privasi. Hal ini mengindikasikan bahwa konsumen Indonesia telah memiliki kesadaran bahwa privasi mereka dapat disalahgunakan ketika melakukan belanja daring, khususnya pada platform *e-commerce*.

PEMBAHASAN

Hasil literasi privasi menunjukkan regresi tahap pertama, kedua, dan ketiga mengindikasikan bahwa keakraban terhadap aspek teknis (X1) berpengaruh positif dan signifikan terhadap kemampuan proteksi privasi (Y). Hal ini berarti semakin tinggi keakraban pada aspek teknis cenderung dapat meningkatkan kemampuan proteksi privasi. Hasil ini mendukung hipotesis (1a) bahwa konsumen dengan tingkat keakraban tinggi dengan aspek teknis akan memiliki kemampuan bersikap protektif terhadap privasi. Hal ini sejalan dengan Park (2013) dan Trepte, dkk. (2015) yang menyatakan bahwa pengetahuan tentang aspek teknis merupakan bagian penting yang memiliki

Tabel 5 Regresi Moderasi *Sig < 0.1

Variabel	β	t value
X1	.308*	.000
X2	.157*	.002
X3	.091*	.006
Z	.300	.301
X1 X Z	.208*	.002
X2 X Z	-.100*	.023
X3 X Z	-.023	.461

Sumber: Olahan Peneliti

pengaruh positif terhadap kemampuan mengontrol hal-hal yang berhubungan dengan perlindungan informasi privasi. Dengan kata lain, aspek teknis merupakan elemen penting untuk mengukur pengetahuan konsumen dalam konteks literasi privasi daring. Aspek teknis *Platform Privacy Preference* (P3P) atau dikenal sebagai kebijakan privasi dan *phishing* merupakan item yang paling berkaitan langsung dengan keamanan privasi pada platform *e-commerce*. Namun demikian, persentase keakrabannya tidak tinggi dan responden lebih memiliki keakraban dengan aspek teknis yang bersifat generik, seperti HTML, *IP Address*, *Cookies*, dan *Firewalls*. Hal ini sesuai dengan istilah *digital natives* yang dikemukakan oleh Hershatter dan Epstein (2010, h. 212) bagi generasi Y yang memiliki keakraban dan pengetahuan tentang aspek teknis.

Penelitian ini tidak bisa menggali lebih dalam responden yang mengaku memiliki pengetahuan tentang aspek teknis. Misalnya, ketika responden menjawab familier tentang fungsi *cookies*, hal ini akan semakin terbukti ketika responden diberikan pertanyaan tambahan mengenai pengetahuan seperti apa yang mereka ketahui tentang *cookies*. *Cookies* merupakan perangkat lunak yang dapat merekam preferensi konsumen dan melalui perangkat lunak ini data dapat dilacak oleh platform. Hasil penelitian mengindikasikan bahwa konsumen cukup sering menggunakan perangkat lunak berbasis teknis, seperti memblokir dan menghapus *cookies*. Hal ini membuktikan bahwa generasi Y memiliki kemampuan bersikap protektif

terhadap privasi mereka. Dengan kata lain, antara keakraban dengan aspek teknis dan kemampuan proteksi berbanding lurus. Berbeda dengan penelitian Park (2013) yang menyatakan bahwa responden jarang menggunakan perangkat lunak berbasis *privacy enhancing technologies* (PET), responden pada penelitian ini tidak mengarah pada karakteristik umur tertentu.

Kesadaran terhadap praktik institusi merupakan pengetahuan konsumen tentang pelacakan, pengumpulan, dan penggunaan informasi pribadi konsumen secara ilegal (Trepte, dkk., 2015, h. 362). Regresi tahap pertama, kedua, dan ketiga menunjukkan bahwa kesadaran praktik institusi berpengaruh positif dan signifikan terhadap kemampuan proteksi privasi. Hal ini berarti semakin tinggi kesadaran konsumen mengenai praktik institusi cenderung dapat meningkatkan kemampuan proteksi privasi. Hasil ini mendukung hipotesis (1b) bahwa konsumen dengan tingkat kesadaran tinggi mengenai praktik institusi memiliki kemampuan bersikap protektif terhadap privasi. Hal ini juga sesuai dengan penelitian Park (2013) yang menyatakan bahwa responden dengan pengetahuan dan kesadaran mengenai praktik institusi, baik di *Social Networking Sites* (SNS) maupun platform *e-commerce*, memiliki pengaruh terhadap kemampuan kontrol dalam media digital, walaupun tidak signifikan.

Kesadaran konsumen akan praktik pengumpulan data merupakan indikator pengetahuan faktual yang dibutuhkan dalam privasi daring (Hoofnagle, King, Li, & Turow, 2010, h. 17). Sebagian

besar responden generasi Y cenderung memilih jawaban yang benar dan memiliki pengetahuan serta kesadaran terhadap praktik yang dilakukan *e-commerce* mulai dari promosi hingga adanya *phising*. Kesadaran ini mengindikasikan bahwa konsumen generasi Y menyadari informasi pribadi mereka dapat bernilai ekonomis. Mereka pun dapat melakukan penyesuaian dengan memiliki bekal kemampuan bersikap protektif terhadap privasi untuk tidak memberikan informasi pribadi mereka secara lengkap.

Penelitian sebelumnya menunjukkan bahwa implementasi strategi perlindungan privasi tidak hanya pengetahuan mengenai aspek teknis dan praktik institusi, tetapi juga tentang pemahaman terhadap kebijakan privasi yang mencakup aturan, legalitas, dan undang-undang (Trepte, dkk., 2015). Pemahaman terhadap aturan yang berlaku merupakan bentuk sikap pengendalian pengguna terhadap aturan karena ruang daring semakin tidak terbatas dan kompleks. Jika konsumen mengetahui hak dan batasan mereka melalui aturan atau kebijakan, maka mereka pun dapat melindungi informasi pribadi sekaligus dapat bertanggung jawab terhadap optimalisasi pengungkapan informasi pribadi (Turow, Hennessy, & Bleakley, 2008, h. 422).

Hasil penelitian menunjukkan bahwa pada regresi tahap pertama, kedua, dan ketiga kesadaran praktik institusi berpengaruh positif dan signifikan terhadap kemampuan proteksi privasi. Hal ini berarti semakin tinggi kesadaran praktik institusi cenderung dapat meningkatkan kemampuan proteksi privasi. Hasil

ini mendukung hipotesis (1c) bahwa konsumen dengan tingkat pengetahuan tinggi terhadap kebijakan privasi memiliki kemampuan bersikap protektif terhadap privasi. Pengukuran pemahaman konsumen terhadap kebijakan privasi didasarkan pada pertanyaan spesifik tentang kebijakan dan aturan yang berlaku di Indonesia. Hasil ini sejalan dengan penelitian Park (2013) yang menyatakan bahwa pemahaman terhadap kebijakan privasi dalam menggunakan media digital memberikan pengaruh terhadap kemampuan kontrol informasi, walaupun hasilnya tidak signifikan.

Kausalitas ketiga elemen literasi privasi daring memainkan peran cukup penting. Hal ini dibuktikan dengan adanya pengaruh positif dan signifikan dari semua elemen pengetahuan tentang aspek teknis (X1), pengetahuan tentang praktik institusi (dalam penelitian ini berkaitan dengan belanja daring) (X2), dan pengetahuan tentang kebijakan privasi (X3), baik pada regresi tahap pertama, kedua, dan ketiga, terhadap variabel kemampuan pengguna untuk bersikap protektif (Y). Kausalitas ini tidak mudah untuk diartikan dan dijabarkan karena sifat *cross-sectional* data survei. Penggunaan metode eksperimental atau *Focus Group Discussion* dapat menutupi kekurangan penelitian ini karena penelitian yang mencakup tingkat pengetahuan akan lebih dapat diambil kesimpulan apabila peneliti dapat terlibat langsung di lapangan menemui responden.

Pengalaman Pelanggaran Privasi

Penelitian ini menggunakan pengalaman pelanggaran privasi sebagai variabel moderasi. Hal ini berbeda dengan

penelitian Park (2013) yang menggunakan moderasi umur, gender, dan pendidikan sebagai variabel yang memoderasi tingkat literasi privasi daring terhadap kemampuan kontrol. Efek moderasi pengalaman pelanggaran privasi diadopsi dari penelitian Buchi, dkk. (2016) yang menggunakan variabel pengalaman pelanggaran privasi (*privacy breach*) mampu memoderasi (*strong predictor*) variabel keahlian menggunakan internet dan secara signifikan memengaruhi kemampuan pengguna bersikap protektif terhadap privasi.

Melalui kuesioner, peneliti memberikan dua pertanyaan mengenai pengalaman pelanggaran privasi ini. Pertama, “Apakah ketika melakukan kegiatan belanja daring privasi Anda pernah dilanggar?” Pertanyaan ini didasarkan pada pengalaman yang pernah mereka alami (*past experience*). Sebagian besar responden gen Y urban atau sebesar 55.8 persen mengaku pernah mengalami pelanggaran privasi. Kedua, “Apakah Anda merasa informasi pribadi Anda sedang disalahgunakan oleh *e-commerce* terkait?” Pertanyaan ini didasarkan pada pengalaman yang sedang terjadi. Sebagian besar responden atau 52.7 persen mengaku privasi mereka sedang dilanggar oleh platform *e-commerce*. Persentase tersebut memunculkan pemahaman bahwa konsumen gen Y urban di Indonesia telah memiliki kesadaran dan kepekaan terhadap pelanggaran privasi yang mereka alami.

Hasil penelitian pada regresi kedua menunjukkan bahwa pengalaman pelanggaran privasi konsumen (Z)

berpengaruh positif dan signifikan terhadap kemampuan proteksi privasi konsumen (Y). Hasil ini mendukung hipotesis (H2) yang menyatakan bahwa konsumen yang memiliki pengalaman pelanggaran privasi ketika belanja melalui *e-commerce* akan semakin kuat bersikap protektif terhadap privasi. Hasil ini sejalan dengan penelitian yang dilakukan oleh Buchi, dkk. (2016) yang menyatakan bahwa pengalaman pelanggaran privasi menjadi *strong predictor* kemampuan proteksi privasi pengguna. Dienlin dan Trepte (2015, h. 286) juga menyatakan bahwa pengalaman pelanggaran dan gangguan privasi, baik yang telah terjadi maupun yang saat ini sedang dialami konsumen, akan meningkatkan kesadaran individu dan memungkinkannya bersikap *defence*.

Uji pada regresi tahap ketiga menunjukkan bahwa interaksi antara keakraban pada aspek teknis (X1) dan pengalaman pelanggaran privasi konsumen (Z) signifikan terhadap kemampuan proteksi privasi. Hasil ini mendukung hipotesis (2a) yang menyatakan bahwa pengalaman pelanggaran privasi mampu memoderasi keakraban dengan aspek teknis terhadap kemampuan bersikap protektif terhadap privasi.

Pada regresi ketiga diperoleh informasi bahwa interaksi antara kesadaran praktik institusi (X1) dan pengalaman pelanggaran privasi konsumen signifikan terhadap kemampuan proteksi privasi. Pengalaman pelanggaran privasi konsumen dinyatakan mampu memoderasi pengaruh kesadaran praktik institusi terhadap kemampuan

proteksi privasi. Hasil ini mendukung hipotesis (2b) yang menyatakan bahwa pengalaman pelanggaran privasi mampu memoderasi kesadaran terhadap praktik institusi terhadap kemampuan bersikap protektif. Hal ini dapat diartikan bahwa variabel moderasi (pengalaman pelanggaran privasi konsumen) bersifat semu.

Selanjutnya, pada regresi ketiga diperoleh informasi bahwa interaksi antara pemahaman terhadap kebijakan privasi dan pengalaman pelanggaran privasi konsumen tidak signifikan terhadap kemampuan proteksi privasi. Hasil ini tidak mendukung hipotesis (2c) yang menyatakan bahwa pengalaman pelanggaran privasi mampu memoderasi pengetahuan mengenai kebijakan privasi terhadap kemampuan bersikap protektif. Dengan demikian, hasil negatif dan tidak signifikan tersebut menunjukkan bahwa pengalaman pelanggaran privasi konsumen tidak mampu memoderasi pengaruh pemahaman mengenai kebijakan privasi terhadap kemampuan konsumen gen Y urban untuk bersikap protektif terhadap privasi. Hal ini berarti bahwa variabel moderasi (pengalaman pelanggaran privasi konsumen) bersifat independen (*exogenous moderator*).

Hasil dari regresi ketiga ini terlihat paradoks sebab seharusnya konsumen yang memahami dan memiliki kebijakan privasi, serta menyadari adanya pelanggaran privasi akan memiliki signifikansi kemampuan bersikap proteksi terhadap privasi. Dienlin dan Trepte (2015, h. 290) menyatakan bahwa pengalaman pelanggaran dan gangguan privasi, baik yang telah terjadi maupun yang saat ini sedang dialami

konsumen, akan meningkatkan kesadaran individu dan memungkinkannya bersikap protektif. Namun, hasil penelitian ini tidak demikian. Hal ini terjadi karena pelanggaran privasi yang dialami konsumen milenial di Indonesia belum memicu tindakan tertentu, sehingga penelitian ini tidak dapat menggali hal tersebut.

Hal di atas dapat terjadi juga karena kurangnya sosialisasi yang dilakukan oleh Kementerian Komunikasi dan Informatika (Kominfo) mengenai pelaporan pelanggaran yang dialami oleh konsumen belanja daring. Konsumen urban gen Y yang tidak memiliki kemampuan beraktivitas dengan internet secara memadai di antara terpaan berbagai macam bentuk platform *e-commerce* dapat menjadi kemungkinan lainnya. Hal tersebut sesuai dengan yang disampaikan oleh Trepte, dkk. (2015, h. 362) bahwa sikap tertentu individu dipengaruhi oleh tiga aspek, yakni kemauan, kemampuan, dan pengalaman yang memicu tindakan bahwa privasi mereka harus dilindungi.

SIMPULAN

Privasi merupakan sesuatu yang begitu mudahnya diabaikan, khususnya dalam konteks belanja daring di Indonesia. Hal ini dapat disebabkan oleh kurangnya *peer group* yang memfasilitasi dan mendukung perdebatan mengenai privasi yang wajib untuk dilindungi dan penyalahgunaan informasi privasi tanpa izin merupakan bentuk pelanggaran hukum. Berbagai macam risiko privasi yang dapat mengganggu keamanan informasi pribadi konsumen ketika berbelanja daring

melalui *e-commerce* meliputi risiko penyalahgunaan informasi pribadi, risiko privasi teknologi, risiko privasi platform *e-commerce*, dan risiko transaksi.

Hasil penelitian menyatakan bahwa dari total tujuh hipotesis atau dugaan penelitian yang telah disusun, enam hipotesis terjawab melalui regresi hierarki tiga tahap dan menunjukkan bahwa semakin tingginya keakraban pada aspek teknis cenderung dapat meningkatkan kemampuan proteksi privasi. Berikutnya, semakin tingginya kesadaran konsumen mengenai praktik institusi cenderung dapat meningkatkan kemampuan proteksi privasi. Selanjutnya, semakin baiknya kesadaran praktik institusi cenderung dapat meningkatkan kemampuan proteksi privasi. Hasil ini menjelaskan bahwa pemahaman terhadap kebijakan privasi berpengaruh terhadap kemampuan proteksi privasi. Peran dari variabel moderasi pengalaman pelanggaran privasi pada hipotesis kedua (H2) menghasilkan pengaruh positif dan signifikan terhadap kemampuan proteksi privasi. Hal ini berarti semakin banyaknya pengalaman pelanggaran privasi konsumen cenderung dapat meningkatkan kemampuan proteksi privasi, meskipun peningkatannya tidak signifikan.

DAFTAR RUJUKAN

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information [review]. *Science*, 347(6221), 509–514.
- Agustiyanti. (2017, Juni 5). OJK minta fintech lindungi konsumen dan data negara. *CNN Indonesia*. <[https://www.cnnindonesia.com/ekonomi/20170604230717-78-219392/ojk-](https://www.cnnindonesia.com/ekonomi/20170604230717-78-219392/ojk-minta-fintech-lindungi-konsumen-dan-data-negara)
- minta-fintech-lindungi-konsumen-dan-data-negara>
- Büchi, M., Just, N., & Latzer, M. (2016). Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society*, 20(8), 1-18.
- Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & Oliveira, R. (2013, May). *Your browsing behavior for a big mac: Economics of personal information online*. Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, 189-200.
- Cho, H., Sánchez M. R., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *Journal of New Media & Society*, 11(3), 395–416.
- Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285–297.
- Fortes, N. & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management Business Economic*, 22(3), 167–176.
- Google & Temasek. (2016). *E-conomy sea: Unlocking the \$200 billion digital opportunity in Southeast Asia*. <https://www.thinkwithgoogle.com/_qs/documents/4859/e-conomy_handout_1_20160525_eXq5Gdl.pdf>
- Gupta, P., & Dubey, A. (2016). E-commerce study of privacy, trust and security from consumer's perspective. *International Journal of Computer Science and Mobile Computing*, 5(6), 224-232.
- Hershatter, A., & Epstein, M. (2010). Millennials and the world of work: An organization and management perspective. *Journal of Business and Psychology*, 25(2), 211-223.
- Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN Electronic Journal*, 1-20.

- Jumiati, Rosdiana, H., & Kusumastuti, R. (2017). Why a policy is needed to protect privacy information in Indonesia's e-commerce. *Paper presented at IAPA International Conference 2016*, Universitas Gadjah Mada, Yogyakarta, Indonesia.
- Kearney, A. T. (2015). Lifting the barriers to e-commerce in ASEAN. *ASEAN Research Institute*. <<https://www.atkearney.co.uk/documents/10192/Lifting+the+Barriers+to+E+Commerce+in+ASEAN.pdf/>>
- Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 1-29.
- Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2014). *The economics of algorithmic selection on the Internet*. Working Paper–Media Change & Innovation Division. University of Zurich, Zurich. <http://www.mediachange.ch/media/pdf/publications/economics_of_algorithmic_selection.pdf>
- Lissitsa, S., & Kol, O. (2016). Generation X vs. generation Y—A decade of online shopping. *Journal of Retailing and Consumer Services*, 31, 304-312.
- MARS Indonesia. (2016). *Studi e-commerce Indonesia 2016*. <<http://www.marsindonesia.com/products/business-reports/studi-e-commerce-indonesia-2016>>
- Mastel & APJII. (2016). *Infografis konklusi survey ekosistem DNA (device, network & apps)*. <<https://apjii.or.id/content/read/39/282/Hasil-Survey-Ekosistem-DNA-Nasional-APJII-dan-MASTEL>>
- Metzger, J. M. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 12, 335-361.
- Mooney, C. (2015). *Online privacy and business*. San Diego, CA: Reference Point Press, Inc.
- Nistanto, R. K. (2016, Juli 20). Begini cara Herdian membobol server bukalapak dan tokopedia. *KOMPAS.com*. <<http://tekno.kompas.com/read/2016/07/20/22030007/begini.cara.herdian.membobol.server.bukalapak.dan.tokopedia>>
- Park, J. Y. (2013). Digital literacy and privacy behavior online. *Communication Research*, 40(2), 215-236.
- Park, J. Y., Campbell W. S., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, 28(3), 1019–1027.
- Rose, S., Clark, M., Samouel, P., & Hair, N. (2012). Online customer experience in e-retailing: An empirical model of antecedents and outcomes. *Journal of Retailing*, 88(2), 308-322.
- Saurwein, F., Just, N., & Latzer, M. (2015). Governance of algorithms: Options and limitations. *Info*, 17(6), 35–49.
- Shinta, D. 2009. *Cyber law: Perlindungan privasi atas informasi pribadi dalam e-commerce menurut hukum internasional*. Bandung, Indonesia: Widya Padjajaran.
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “online privacy literacy scale” (OPLIS). Dalam S. Gutwirth, R. Leenes, & P. de Hert (eds), *Reforming european data protection law* (Vol. 20, h. 333–365). Dordrecht, Belanda: Springer.
- Turow, J., Hennessy, M., & Bleakley, A. (2008). Consumers' Understanding of Privacy Rules in the Marketplace. *Journal of Consumer Affairs*, 42(3), 411–424.
- Vasileiadis. (2014). Privacy concerns and trust in the adoption of m-commerce. *Social Technologies*, 4(1), 179–191.
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs*, 43(3), 389-418.