Pengaruh intensi, pengalaman menggunakan internet, kondisi pemfasilitasan, dan undang-undang informasi & transaksi elektronik No. 11/2008 terhadap cybercrime

JRAK
1,1

63

Achmad Syaiful Hidayat Anwar

Universitas Muhammadiyah Malang, Jawa Timur

Jl. Raya Tlogomas 246 Malang

Email: ipoel@yahoo.com

Abstract

The aims of this research is to test the influence of intension, experience using the internet, facilitating conditions and undang-undang Informasi & Transaksi Elektronik (ITE) No. 11/2008 on cybercrime. This research uses survey methods. Cluster sampling and purposive sampling method are used to determine research sample.

The respondents are internet users who use the internet at warnet and are located in Yogyakarta, Surabaya and Malang. Some 300 questionnaires have been distributed and received back. A total of 291 questionnaires revealed to be analyzed by using multiple regression analysis.

Based on the analysis results can be concluded that intention, experience using the Internet, facilitating conditions and UU ITE No. 11/2008 positively influence the occurrence of cybercrime. For further research, it is advisable to increase research variables also affect the occurrence of cybercrime, among others, and increase the number of samples. It aims to obtain research results more representative so that results can be generalized.

Keywords: *cybercrime, internet, UU ITE No. 11/2008*

Pendahuluan

Perkembangan dan pemanfaatan internet telah mengubah perilaku individu, masyarakat, pemerintah dan para pelaku bisnis dalam berinteraksi, berkomunikasi, bertransaksi dan mendistribusi informasi. Perubahan perilaku ini distimuli oleh ketersediaan dan berbagai kemudahan yang ditawarkan melalui pemanfaatan teknologi internet. Melalui pemanfaatan teknologi internet, individu, masyarakat dan para pelaku bisnis dapat berinteraksi atau beraktivitas dengan pihak lain tanpa harus melakukan kontak fisik dan tidak lagi dibatasi oleh jarak, tempat dan waktu. Keefektifan, kemudahan, efisiensi proses bisnis dan keunggulan kompetitif, merupakan kontribusi yang dapat diperoleh melalui pemanfaatan internet. Tentunya hal ini dapat dicapai apabila juga didukung oleh kualitas sumberdaya manusia yang baik, ketersediaan dan kualitas teknologi informasi, serta jaminan keamanan dan pengendalian (SDM, teknologi, data dan atau informasi) yang efektif.

Selain memberikan berbagai kemudahan, pemanfaatan internet dalam bisnis juga mengandung berbagai risiko dan potensi gangguan-gangguan. Hal ini dapat berarti bahwa, para pengguna internet tidak selalu menggunakan atau memanfaatkan internet untuk kegiatan yang positif. Berkembangnya *hacker* dan *cracker* merupakan salah bentuk perilaku negatif para pengguna internet. Masalah pornografi, *carding*, akses data dan informasi secara ilegal, interupsi, intersepsi penye-

Jurnal Reviu Akuntansi
dan Keuangan

ISSN: 2088-0685

Vol.1 No. 1, April 2011

Pp 63-71

baran virus dan penyalahgunaan *email* merupakan beberapa contoh potensi gangguan yang dapat disebabkan oleh perilaku para pengguna internet yang tidak etis. Aspek perilaku negatif pengguna internet dapat menghambat atau mengancam keberlangsungan aplikasi sistem informasi berbasis internet suatu entitas bisnis.

Pengembangan Hipotesis

Cybercrime

Cybercrime merupakan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer dan internet (www.lintasberita.com). Raharjo (2006) mendefinisi *cybercrime* sebagai kejahatan yang dilakukan dengan dan memanfaatkan teknologi. Terkait dengan *cybercrime*, Rahardjo (2001) mengklasifikasi *cybercrime* menjadi dua, yaitu *computer fraud* dan *computer crime*. *Computer fraud* meliputi kejahatan atau pelanggaran dari segi sistem organisasi komputer. Sedangkan *computer crime* merupakan kegiatan berbahaya, dalam hal ini menggunakan media komputer dalam melakukan pelanggaran hukum (*computer as a tool*). Untuk menginvestigasi dan menganalisis kedua kejahatan di atas, maka digunakan forensik komputer dalam teknologi informasi.

Jarvenpaa dan Grazioly (dalam Nazar dan Syahrana, 2008) memaparkan bahwa, kejahatan dalam media internet berjumlah sangat besar serta memiliki bentuk yang beragam karena beberapa alasan. *Pertama*, identitas individu, atau organisasi dalam dunia internet mudah untuk dipalsukan, tetapi sulit dibuktikan secara hukum. *Kedua*, tidak membutuhkan sumber daya ekonomi yang besar untuk melakukan kejahatan dalam internet. *Ketiga*, internet menyediakan akses yang luas pada pengguna yang potensial menjadi korban. *Keempat*, kejahatan dalam internet, identitas pelaku tidak dikenal dan secara yuridis sulit mengejar pelaku. Rasa aman menggambarkan hal yang subjektif, yang memungkinkan konsumen untuk mempercayai bahwa informasi pribadi mereka (Privat dan moneter) akan tidak dapat dilihat, dan berpindah tanpa persetujuan. Berdasarkan paparan tersebut diatas, faktor pengguna teknologi, kapabilitas teknologi komputer dan jaringan internet, serta aspek keamanan operasi komputer dan jaringan internet, merupakan aspek penting yang seharusnya diperhatikan, mengingat berbagai ancaman kemungkinan akan muncul yang disebabkan oleh kedua faktor tersebut.

Sunardi (2008) mengidentifikasi faktor-faktor yang menyebabkan terjadinya *cybercrime*. Faktor-faktor tersebut antara lain; akses internet yang tidak terbatas, kelalaian pengguna komputer, mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik akan teknologi komputer, sistem keamanan jaringan yang lemah dan kurangnya kontrol masyarakat dan penegak hukum. Rahardjo (2001) telah mengidentifikasi bentuk-bentuk penyerangan atau kejahatan komputer pada sistem komputer antara lain; interupsi, intersepsi (pihak yang tidak berwenang berhasil mengakses asset atau informasi), modifikasi, dan pabrikasi (pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem).

Harris (2007) mengidentifikasi beberapa bentuk lain kejahatan atau kecurangan komputer. Beberapa bentuk kecurangan komputer tersebut antara lain; pemalsuan nilai evidentiary data, alterasi (pengubahan) data, sabotase komputer, disclosure rahasia perdagangan dan industrial serta akuisisi data secara ilegal. Lebih lanjut, Harris memaparkan beberapa kasus kejahatan komputer yang pernah terjadi, khususnya di Indonesia, antara lain; kasus penggelapan uang Melalui Komputer (Clearing) BRI Yogyakarta, kasus pembobolan BNI 46 cabang New York, kasus mutasi kredit fiktif melalui komputer oleh Bank Office Computer BDN Cab. Jakarta Bintaro Jaya, kasus pemalsuan nama domain Mustika Ratu.com di Amerika, kasus *hacking* pada situs KPU, kasus pembobolan kartu kredit melalui internet, kasus domain klikbca.com, dan beberapa kasus lain terkait dengan masalah keamanan sistem informasi berbasis internet atau berbasis web.

Intensi

Hartono (2007) mendefinisi intensi (niat) sebagai keinginan untuk melakukan perilaku. Dengan kata lain dapat dikatakan bahwa, seseorang berperilaku karena faktor keinginan, kesengajaan atau karena memang sudah direncanakan. Niat berperilaku (*behavioral intention*) masih merupakan suatu keinginan atau rencana. Dalam hal ini, niat belum merupakan perilaku, sedangkan perilaku (*behavior*) adalah tindakan atau kegiatan nyata yang dilakukan. Berdasarkan *Theory planned behavior* yang dikemukakan oleh Azjen (1988, 1991) menyatakan bahwa, perilaku tertentu, ditentukan oleh niat individu tersebut untuk melakukan perilaku tertentu. Ajzen (1991), Taylor dan Todd (1995) memaparkan bahwa, niat sebagai salah satu faktor yang mempengaruhi perilaku, telah ditetapkan di dalam acuan sistem informasi dan disiplin yang lain. Dalam penelitian ini, intensi mengarah pada niat atau keinginan individu untuk melakukan *cybercrime* atau berperilaku tidak etis pada saat menggunakan internet.

Ozman dan Rahman (2009) menganalisis mengenai penyalahgunaan internet di kalangan mahasiswa di UiTM. Hasil analisis menunjukkan bahwa, mereka melakukan *cyber crime* karena keingintahuan, untuk hiburan, hobi dan karena rasa bosan. Ponziani dan Suyanto (2009) mengkaji mengenai faktor-faktor yang mempengaruhi niat perilaku *knowledge sharing* oleh profesional bank. Hasil pengujian menunjukkan bahwa, niat perilaku *knowledge sharing* dipengaruhi oleh sikap terhadap *knowledge sharing*, norma subyektif, dan kepuasan kerja. Individu yang memandang positif terhadap aktivitas *knowledge sharing* akan semakin besar niatnya untuk melakukan aktivitas tersebut. Berdasarkan beberapa pemikiran tersebut dapat ditegaskan bahwa, *cybercrime* dapat terjadi karena memang ada niat (kesengajaan) para pengguna untuk melakukan kejahatan tersebut. Berdasarkan telaah literatur tersebut, hipotesis pertama penelitian ini yaitu;

H₁: Intensi berpengaruh terhadap *cybercrime*

Pengalaman

Rokhmah (2008) meneliti tentang pengaruh pengalaman terhadap penggunaan internet antara pengguna yang berdasarkan pengalaman dan pengguna yang berdasarkan tujuan. Hasil penelitian menunjukkan adanya pengaruh yang positif antara pengalaman optimal dengan sikap dalam menggunakan Internet (*browsing dan searching*). Tarigan (2007) memaparkan bahwa, dalam keterkaitan dengan makin maraknya kejahatan komputer dan internet peneliti menyatakan bahwa, keahlian *end users* (pengalaman dan keterampilan pengguna) dalam kaitannya dengan penggunaan komputer dan pengembangan aplikasi, merupakan faktor penyebab makin maraknya penyalahgunaan penggunaan komputer dan internet. Berdasarkan telaah literatur tersebut, hipotesis kedua penelitian ini yaitu;

H₂: Pengalaman berpengaruh terhadap *cybercrime*

Kondisi Pemfasilitasan

Triandis dalam Thompson et. al (1991) menyatakan bahwa; perilaku tidak dapat terjadi apabila kondisi objektif dalam lingkungan memprevensi perilaku. Dalam hal ini dapat dikatakan bahwa, perilaku seseorang tidak hanya disebabkan oleh niat, tujuan dan pengalaman. Perilaku yang tidak etis tersebut juga disebabkan oleh kondisi yang mendukung dan memfasilitasi seseorang untuk berperilaku. Berdasarkan telaah literatur tersebut, hipotesis ketiga yang diajukan dalam penelitian ini yaitu;

H₃: Kondisi pemfasilitasan berpengaruh terhadap *cybercrime*

Undang-undang ITE No. 11/2008

Keberadaan undang-undang ITE 11/2008 berfungsi sebagai pedoman, norma dan kontrol terhadap perilaku para pengguna internet. Hal ini bertujuan untuk memprevensi, mendeteksi atau mereduksi kejahatan internet, kecurangan dan perilaku pengguna internet yang tidak etis, yang dilakukan melalui penggunaan teknologi informasi. Pedoman, norma dan fungsi kontrol tercermin pada ketentuan yang terdapat dalam bab dan pasal-pasal UU ITE 11/2008. Ketentuan ini mengacu pada upaya regulator untuk mengarahkan dan mengendalikan perilaku para pengguna internet serta meningkatkan kepatuhan para pengguna terhadap UU ITE 11/2008. Peningkatan kepatuhan para pengguna internet diharapkan mampu mereduksi terjadinya kejahatan internet (*cybercrime*) dan perilaku negatif para pengguna internet. Berdasarkan telaah literatur tersebut, hipotesis keempat yang akan diuji dalam penelitian ini yaitu:

H_4 : Kepatuhan pada UU ITE 2008 berpengaruh terhadap *cybercrime*

Metode

Populasi dalam penelitian ini adalah individu para pengguna internet. Untuk penentuan sampel penelitian, peneliti menggunakan *cluster sampling* dan *purposive sampling*. Populasi dalam penelitian ini dibagi menjadi 3 kluster berdasarkan kota (wilayah) responden yaitu; Yogyakarta, Malang dan Surabaya. Pemilihan 3 kota tersebut berdasarkan pertimbangan *market* yang cukup besar dan potensial dan animo permintaan data cukup tinggi. Masing-masing kota akan dipilih 100 sampel dengan kriteria yaitu pengguna internet yang menggunakan internet atau yang mengakses internet di Warung Internet (WARNET).

Pengumpulan data dilakukan dengan mendistribusikan kuesioner secara langsung kepada individu pengguna internet. Pendistribusian kuesioner dilakukan oleh peneliti dengan dibantu beberapa enumerator. Hal ini dilakukan untuk a) meningkatkan *respon rate*, b) mempermudah dan mempercepat pendistribusian kuesioner dan c) untuk memberikan kemudahan pengisian kuesioner. Teknik analisis data meliputi uji validitas, uji reliabilitas dan uji hipotesis. Uji validitas dilakukan untuk menilai bahwa pengujian benar-benar mengukur apa yang seharusnya diukur. Uji reliabilitas dilakukan untuk akurasi, konsistensi dan ketepatan dari alat pengukur yang digunakan. Uji hipotesis dilakukan untuk menguji apakah variabel independen berpengaruh terhadap variabel dependen. Teknik analisis data dilakukan dengan menggunakan software SPSS ver. 15.0.

Hasil dan Pembahasan

Kuesioner yang dinyatakan memenuhi syarat untuk dianalisis berjumlah 291 dari 300 kuesioner yang telah dikembalikan oleh responden. Sebanyak 9 kuesioner tidak dapat dianalisis karena pengisian yang kurang lengkap. Tahapan analisis data dalam penelitian ini adalah sebagai berikut:

Uji Validitas dan Reliabilitas Instrumen Penelitian

Hasil pengujian validitas dan reliabilitas terhadap instrumen penelitian disajikan pada tabel 1 berikut ini.

Variabel	Item	Validitas		Keputusan	Koefisien Alpha
		Korelasi (R)	Signifikansi		
Intensi (X_1)	I1	0.837	0.000	Valid	0.878 (Reliabel)
	I2	0.835	0.000	Valid	
	I3	0.901	0.000	Valid	
	I4	0.848	0.000	Valid	

Tabel 1
Uji Validitas dan
Reliabilitas
Instrumen Penelitian

Variabel	Item	Validitas		Keputusan	Koefisien Alpha
		Korelasi (R)	Signifikansi		
Pengalaman (X ₂)	P1	0.878	0.000	Valid	0.672 (Reliabel)
	P2	0.858	0.000	Valid	
	K1	0.845	0.000	Valid	
Kondisi Pemfasilitasan (X ₃)	K2	0.890	0.000	Valid	0.880 (Reliabel)
	K3	0.885	0.000	Valid	
	K4	0.809	0.000	Valid	
	U1	0.808	0.000	Valid	
UU ITE (X ₄)	U2	0.783	0.000	Valid	0.721 (Reliabel)
	U3	0.688	0.000	Valid	
	U4	0.663	0.000	Valid	
Cybercrime (Y)	C1	0.903	0.000	Valid	0.670 (Reliabel)
	C2	0.827	0.000	Valid	

Sumber: data primer diolah

Berdasarkan hasil pengujian menunjukkan bahwa, semua item pertanyaan mempunyai nilai R_{hitung} dengan nilai signifikansi yang lebih kecil dari alpha 0.05, sehingga tidak ada item instrumen yang harus dikeluarkan dari pengujian. Sedangkan untuk reliabilitas menunjukkan bahwa hasil perhitungan *standardized item alpha* (SIA) lebih besar dari sebesar 0.6. Dengan demikian dapat dikatakan bahwa, butir-butir item pertanyaan yang digunakan sebagai pengukur variabel yang akan diuji adalah valid dan reliabel.

Uji Normalitas Data

Kenormalan sebaran data dan homogenitas ragam data dilakukan dengan menguji kenormalan data serta homogenitas ragam data berdasarkan nilai *standardize residual (error)*. Pada tabel 2 berikut ini hasil pengujian normalitas data dengan menggunakan *Kolmogorof-Smirnov Goodness of Fit Test* terhadap masing-masing variabel independen dan dependen.

Variabel	K-S Statistik	Nilai Signifikansi	Kesimpulan
<i>Standardized Residual of UU ITE, Intensi, Kondisi, Pengalaman, Cybercrime</i>	0.624	0.830	Data berdistribusi normal

Sumber : data primer diolah

Keterangan: K-S = Kolmogorov-Smirnov test Z

Tabel 2.
Uji Normalitas Data

Berdasarkan pengujian normalitas data dengan menggunakan uji Kolmogorov-Smirnov, terlihat pada *Standardized Residual* dari seluruh variabel menunjukkan nilai signifikansi (p) sebesar 0.830 yang lebih besar alpha 0,05 yang mengindikasikan bahwa pada data seluruh variabel independen dan dependen tersebut menyebar mengikuti sebaran normal (berdistribusi normal). Dengan demikian dapat dilakukan pengujian lebih lanjut karena asumsi kenormalan data telah terpenuhi.

Uji Korelasi

Sebelum dilakukan analisis regresi, maka perlu dilakukan uji korelasi dengan menggunakan korelasi *Product Momen Pearson* untuk mengetahui adanya hubungan antara intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 dengan *cybercrime*.

Item	Validitas		Kesimpulan	
	Korelasi (r)	Sig.		
Y	X1	0.547	0.000	Antara X1 dan Y ada hubungan yang signifikan
	X2	0.557	0.000	Antara X2 dan Y ada hubungan yang signifikan
	X3	0.568	0.000	Antara X3 dan Y ada hubungan yang signifikan
	X4	-0.668	0.000	Antara X4 dan Y ada hubungan yang signifikan

Sumber: data primer diolah

Tabel 3
Uji Korelasi *Product Momen Pearson*

Berdasarkan Tabel 3 menunjukkan bahwa, nilai signifikansi dari ke-4 variabel independen lebih kecil dari alpha 0.05. Dengan demikian dapat disimpulkan bahwa terdapat hubungan yang signifikan secara positif antara intensi, pengalaman, kondisi pemfasilitasan terhadap *cybercrime*. Sedangkan variabel kepatuhan para pengguna internet pada UU ITE mempunyai hubungan yang signifikan secara negatif dengan *cybercrime*. Artinya, semakin rendah intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan semakin tinggi kepatuhan para pengguna internet pada UU ITE No. 11/2008 secara nyata akan menurunkan *cybercrime*. Demikian sebaliknya, semakin tinggi intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan semakin rendah kepatuhan para pengguna internet pada UU ITE No. 11/2008 secara nyata akan meningkatkan *cybercrime*.

Mengenai pengaruh seberapa tinggi maupun rendahnya intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 tersebut terhadap *cybercrime*, dapat diketahui dengan menggunakan analisis bentuk hubungan (regresi), karena dari uji korelasi belum bisa menjelaskan hal tersebut.

Uji Regresi linier berganda

Berdasarkan hasil pengujian, maka hasil regresi dapat disusun dalam bentuk Tabel 4 sebagai berikut.

Variabel	Koefisien regresi (b)	Std. error	Beta (β)	t _{hitung}	Sig.	Keterangan
(Constant)	3.600	0.413		8.714	0.000	Signifikan
X1	0.124	0.030	0.176	4.139	0.000	Signifikan
X2	0.204	0.042	0.207	4.836	0.000	Signifikan
X3	0.131	0.019	0.276	6.987	0.000	Signifikan
X4	-0.237	0.022	-0.426	-10.691	0.000	Signifikan
R	= 0.808					
R Square	= 0.653					
Adjusted R square	= 0.648					
F _{hitung}	= 134.353					
Sign. F	= 0.000					
α	= 0.05					

Tabel 4.
Hasil Analisis Regresi
Linier Berganda

Sumber: data primer diolah

Koefisien determinasi

Ukuran dari derajat keeratan hubungan antara variabel intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 terhadap *cybercrime*, serta besarnya pengaruh ke-4 variabel independen terhadap keragaman dari variabel dependen ditunjukkan oleh nilai koefisien korelasi ganda (Multiple R) dan koefisien determinasi (R Square) yang dapat diinterpretasikan sebagai berikut.

Berdasarkan Tabel 4 menunjukkan nilai koefisien korelasi ganda (*Multiple R*) sebesar 0.808 yang menyatakan besarnya derajat keeratan hubungan antara *cybercrime* dengan intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 mencapai 0.808 serta adanya hubungan yang kuat diantara intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 tersebut dengan *cybercrime*.

Untuk nilai koefisien determinasi menunjukkan sebesar 0.653, sedangkan koefisien determinasi yang telah terkoreksi dari faktor kesalahan atau bias dengan tujuan agar lebih mendekati ketepatan model dalam populasi digunakan *Adjusted R Square* (R^2) yaitu sebesar 0.648, yang menyatakan besarnya pengaruh dari intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 terhadap *cybercrime*. Artinya sebesar 64.8% keragaman dari *cybercrime* dipengaruhi oleh adanya intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008. Sedangkan sisanya 35.2% ditentukan oleh faktor lain di luar variabel yang diteliti.

Uji F

Untuk menunjukkan apakah semua variabel independen yang dimasukkan dalam model persamaan regresi linier berganda mempunyai pengaruh signifikan secara bersama-sama (simultan) terhadap variabel dependen, maka digunakan uji F sebagai uji kelayakan model. Berdasarkan Tabel 4 diperoleh hasil F_{hitung} sebesar 134,353 dengan nilai signifikansi (0.000) yang jauh lebih kecil dari alpha 0.05. Hal ini menunjukkan adanya pengaruh yang signifikan dari intensi pengguna internet untuk melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 terhadap *cybercrime*.

Sumbangan Efektif

Untuk menunjukkan variabel independen yang paling dominan mempengaruhi *cybercrime* dilakukan dengan cara menghitung besarnya sumbangan efektif (kontribusi) yang paling besar. Penilaian terhadap sumbangan efektif dilakukan dengan mengkomparasi hasil perkalian antara **koefisien korelasi** dengan **beta** tiap variabel independen. Hasil perhitungan sumbangan efektif tersebut disajikan pada tabel 5 berikut.

Variabel	R	Beta	Perhitungan	SE
Intensi	0.547	0.176	$0.547 \times 0.176 \times 100$	9.64%
Pengalaman	0.557	0.207	$0.557 \times 0.207 \times 100$	11.52%
Kondisi	0.568	0.276	$0.568 \times 0.276 \times 100$	15.69%
UU ITE	-0.668	-0.426	$-0.668 \times -0.426 \times 100$	28.42%
Total Sumbangan Efektif				65.27%

Sumber: data primer diolah

Tabel 5
Perhitungan
Sumbangan Efektif

Berdasarkan hasil perhitungan tersebut, ternyata variabel kepatuhan para pengguna internet pada UU ITE No. 11/2008 (X_4) menunjukkan sumbangan efektif yang paling besar yaitu sebesar 28,42%. Selanjutnya dari hasil perhitungan tersebut dapat diketahui bahwa variabel intensi, kondisi pemfasilitasan, dan kepatuhan para pengguna internet pada UU ITE No. 11/2008 ternyata mampu memberikan sumbangan efektif sebesar 65,27% terhadap *cybercrime*. Besarnya sumbangan efektif total ini sama dengan besarnya koefisien determinasi (R^2) yaitu sebesar 65.3%.

Simpulan

Berdasarkan hasil analisis secara umum dapat disimpulkan bahwa, intensi melakukan *cybercrime*, pengalaman menggunakan internet, kondisi pemfasilitasan dan UU ITE No. 11/2008 berpengaruh secara positif terhadap terjadinya *cybercrime*.

Penelitian ini tentunya masih memiliki beberapa keterbatasan. Keterbatasan pada penelitian ini antara lain; pertama, responden pada penelitian hanya mencakup para pengguna internet yang melakukan akses internet di warung internet (WARNET). Berkaitan dengan *cybercrime*, terdapat kemungkinan para pengguna

internet melakukan kejahatan di lokasi lain. Lokasi lain yang dapat digunakan oleh para pengguna internet untuk menggunakan internet antara lain; di perkantoran, di cafe yang menyediakan layanan hotspot area, lembaga pendidikan dan di rumah.

Kedua, peneliti tidak memasukkan variabel lain yang diduga juga dapat berpengaruh terhadap terjadinya *cybercrime*. Keterbatasan yang ketiga terkait dengan sampel penelitian. Jumlah sampel yang digunakan pada penelitian ini masih relatif kecil yakni, hanya mencakup 3 kota dengan jumlah responden sebanyak 100 untuk masing-masing kota. Keempat, peneliti belum bisa memastikan apakah responden belum atau sudah pernah melakukan *cybercrime*. Hal ini dapat menimbulkan kesulitan untuk menjustifikasi jawaban yang telah diberikan oleh responden.

Solusi alternatif lain yang dapat digunakan untuk mengurangi terjadinya *cybercrime*, pihak pengelola warnet dapat bekerja sama dengan berbagai pihak antara lain; pihak kepolisian, aparat penegak hukum, dan pihak lain yang kompeten dan memiliki keahlian di bidang teknologi komputer, internet dan teknologi jaringan.

Mengingat semakin maraknya kasus kejahatan internet, terutama yang berhubungan dengan kegiatan bisnis, para pelaku bisnis hendaknya juga selalu waspada dan selalu mengutamakan faktor pengendalian dan keamanan. Untuk penelitian selanjutnya, peneliti disarankan untuk menambah variabel penelitian yang belum dimasukkan dalam model penelitian dan memperbanyak jumlah sampel. Hal ini bertujuan untuk memperoleh hasil penelitian yang lebih representatif sehingga hasilnya dapat digeneralisasi. Pemilihan responden yang pernah melakukan *cybercrime* disarankan untuk dijadikan responden pada penelitian selanjutnya. Alternatif yang dapat dilakukan yaitu dengan melakukan interview dengan komunitas *hacker* atau *cracker*. Hal ini menjadi penting untuk dilakukan agar peneliti lebih mudah untuk menjustifikasi jawaban responden.

Daftar Pustaka

- Ajzen, I. 1988. *From Intentions to Actions: A Theory of Planned Behavior*. Action Control: From Cognition to Behavior, J. Kuhl and J. Beckman, eds., Springer Verlag, New York.
- _____. 1991. "The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes". www.cw.utwente.nl. Tanggal Akses 15 April 2009.
- Algifari. 1997. *Statistik Induktif untuk Ekonomi dan Bisnis*. Akademi Manajemen Perusahaan YKPN, Yogyakarta
- Arikunto, S. 2002. *Prosedur Penelitian*. PT Asdi Maha Satya. Jakarta
- Dajan, A. 1995. Pengantar Metode Statistik. Jilid I. Pustaka LP3ES Indonesia. Jakarta.
- Fox, S. 2000. "Trust and privacy online: why Americans want to rewrite the rules, Pew Internet and American Life Project". www.pewinternet.org. Tanggal Akses, 15 April 2009.
- Hall, J. A., dan Tommie S. 2007. *Audit dan Assurance Teknologi Informasi*. Edisi 2. penerbit Salemba Empat. Jakarta.
- Hartono, J. 2004. *Metodologi Penelitian Bisnis: Salah Kaprah dan Pengalaman-pengalaman*. BPFE-UGM.
- _____. 2007. *Sistem Informasi Keperilakuan*. Andy Offset. Yogyakarta
- _____. 2008. *Metodologi Penelitian Sistem Informasi*. Andy Offset. Yogyakarta
- Hasan, M. Iqbal. 2002. *Pokok-pokok metodologi penelitian dan aplikasinya*. Ghalia Indonesia. Jakarta.
- Jumaili, Salman. 2005. "Kepercayaan Terhadap Teknologi Sistem Informasi Baru Dalam Evaluasi Kinerja Individual". *Materi Simposium Nasional Akuntansi VIII, Solo*.

- Laudon, K. C., dan J. P. Laudon. 2008. *Sistem Informasi Manajemen*. Edisi 10. Penerbit Salemba Empat. Jakarta.
- Lim, Harry. 1999. "Security: 5 Kesalahan Utama dalam Security". www.google.co.id. Tanggal Akses; 10 Juni 2009
- Malhotra, Y and D. Galletta. 2005. "A Multidimensional Commitment Model of Volitional System Adoption and Usage Behavior". *Journal of Management Information Systems*.
- Nazar, M. R. dan Syahrani. 2008. "Pengaruh Privasi, Keamanan, Kepercayaan dan Pengalaman Terhadap Niat untuk bertransaksi Secara Online". Artikel *Simposium Nasional Akuntansi XI*. Pontianak
- Nugraha, E. 2009. "Perubahan Perilaku Masyarakat Terhadap Penggunaan Teknologi Informasi (Internet) Pasca Diberlakukannya UU ITE No.11 2008". www.egiyakuza.blogspot.com. Tanggal Akses, 10 Juni 2009.
- Ozman M. dan A. A. Rahman. 2009. "Penyalahgunaan Internet Di Kalangan Mahasiswa; Kajian Kes di UiTM". *Artikel penelitian*. Malaysia.
- Ponziani, R. M. dan Suyanto. 2009. "Faktor-faktor yang Mempengaruhi Niat perilaku Knowledge Sharing Oleh Profesional Bank". *Simposium Nasional Sistem Teknologi Informasi (SNSTI)*, Universitas Gajah Mada. Yogyakarta
- Raharjo, A. 2006. "Kebijakan Kriminalisasi dan Penanganan *Cybercrime* di Indonesia". www.unsoed.ac.id. Tanggal akses 15 Juni 2008.
- Rahardjo, B. 2001. "Keamanan Sistem Informasi Berbasis Internet". <http://budi.insan.co.id>. Tanggal akses 15 Juni 2008.
- Rokhmah, B. E. 2008. "Pengaruh Pengalaman Optimal (*Flow*) terhadap Penggunaan Internet antara Pengguna yang Berdasarkan Pengalaman dan Pengguna yang Berdasarkan Tujuan". *Simposium Nasional Sistem Teknologi Informasi (SNSTI)*, Universitas Gajah Mada. Yogyakarta
- Romney, M. B. dan Steinbart, P. J. 2003. *Accounting Information Systems*. Ninth Edition. Prentice Hall.
- Santoso, S. 2003. *Buku Statistik Multivariat*. Penerbit PT Elex Media Komputindo. Jakarta.
- Steel, R.G.D and Torrie, J.H., 1995, *Principles and Procedures of statistics*. Alih bahasa: Bambang sumantri (IPB). Cetakan keempat. Penerbit Gramedia Pustaka Utama. Jakarta.
- Sugiyono. 2003. *Statistika Untuk Penelitian*. Cetakan ke-5. CV Alfabeta. Bandung.
- Sunardi, Teddy. 2008. "Faktor-Faktor Penyebab Cybercrime dan jenis kejahatan Internet". <http://qnoyzone.blogdetik.com>. Tanggal Akses 15 Oktober 2009
- Tarigan, J. 2007. "*Biometric Security*: Alternatif Pengendalian dalam Sistem Informasi Akuntansi Terkomputerisasi". www.puslit.petra.ac.id. Tanggal Akses 10 Juni 2008.
- Taylor, S., and Todd, P. A. 1995. "Understanding Information Technology Usage – a Test of Competing Models". *Information Systems Research*.
- Thompson. R. L; Higgins. C. A dan Howell. J. M. 1991. "Personal Computing: Toward a Conceptual Model of Utilization". *MIS Quarterly*.
- Wasesa, S. A. 2009. "Pengguna Internet di Indonesia Meningkat". Makalah seminar Kompetensi Profesional Komunikasi di Era Kekuasaan Media Baru. www.antaranews.com. Tanggal Akses 15 Oktober 2009.