Información Tecnológica
Vol. 29(2), 115-122 (2018)
http://dx.doi.org/10.4067/S0718-07642018000200115

Aceptación del Reconocimiento Facial Como Medida de Vigilancia y Seguridad: Un Estudio Empírico en Chile

Cristián J. Bravo[(1)], Patricio E. Ramírez[(1)]* y Jorge Arenas [(2)]
(1) Escuela de Ingeniería, Universidad Católica del Norte, Larrondo 1281, Coquimbo, Chile.
(e-mail: cristianjbv@gmail.com; patricio.ramirez@ucn.cl).
(2) Departamento de Administración de Empresas y Comercialización e Investigación de Mercados, Universidad de Sevilla, Ramón y Cajal 1, Sevilla, España. (e-mail: jarenas@us.es)

* Autor a quien debe ser dirigida la correspondencia

Recibido Jul. 10, 2017; Aceptado Sep. 26, 2017; Versión final Oct. 5, 2017, Publicado Abr. 2018

Resumen

El objetivo de este trabajo es analizar la aceptación por parte de los ciudadanos de la tecnología de reconocimiento facial como medida de seguridad. El estudio está basado en el índice de predisposición tecnológica (TRI) y el modelo de aceptación de las tecnologías (TAM). Luego de establecer un modelo de investigación, la metodología utiliza una encuesta a 220 chilenos para obtener los datos, que son analizados con la técnica de mínimos cuadrados parciales (*partial least squares*). Los resultados del análisis indican que la utilidad percibida del reconocimiento facial como medida de seguridad es explicada en un 50% por las variables normas sociales, percepción de responsabilidad, optimismo, grado de innovación, y percepción de inseguridad.

Palabras clave: vigilancia digital; preocupaciones por la privacidad; utilidad percibida; reconocimiento facial

Acceptance of Face Recognition as a Surveillance and Safety Measure: An Empirical Study in Chile

Abstract

The objective of this work is to analyze the acceptance by citizens of the facial recognition technology as a security measure. The study is based on the technology predisposition index (TRI) and the technology acceptance model (TAM). After establishing a research model, the methodology uses a survey of 220 Chileans to obtain the data, which are analyzed using the Partial Least Squares technique. The results of the analysis indicate that the perceived utility of facial recognition as a safety measure is explained 50% by the variables social norms, perception of responsibility, optimism, degree of innovation, and perception of insecurity.

Keywords: digital surveillance; privacy concerns; perceived usefulness; facial recognition

INTRODUCCIÓN

La implementar de vigilancia puede ser vista como una actividad destinada a tener mayor seguridad, pero también ha sido vista como una violación de la privacidad. El asunto es clave en una era digital, donde la información personal es transmitida en grandes volúmenes y a una alta velocidad (Georgiadou y Fischer-Hübner, 2010). Sin duda, todo avance tecnológico entrega beneficios, más aún si éste se utiliza para mejorar la protección de las personas y evitar actos no deseados, tales como, terrorismo, ciberdelitos, suplantación de identidad, entre otros (Aquilina, 2010). Sin embargo, estos beneficios envuelven algunos costos. En comparación con países norteamericanos o europeos, en Chile la situación en el uso de nuevas tecnologías para la seguridad es bastante desactualizada. Tecnologías como el reconocimiento facial es algo que sólo se utiliza de forma privada o con fines de investigación, en cambio en otras naciones es algo común y adoptado hace bastante tiempo por las entidades de seguridad pública. Situando a Chile en un punto medio, considerando que en América latina existen países con un desarrollo tecnológico inferior. Debido a lo anterior, surge una interrogante: ¿Se necesita mayor seguridad o mayor privacidad? El sentimiento de seguridad es algo que debiera ser reconfortante para cualquier persona, sin embargo, vivir sin una privacidad adecuada puede llegar a ser un problema para muchos (Hughes, 2015).

En este contexto, ¿Cuánto se puede conocer de la información personal sin que esto sea considerado una intrusión?, esta investigación desea aportar en la respuesta a esta interrogante. En particular, este estudio tiene como propósito evaluar la aceptación de una tecnología de vigilancia no implementada en Chile, siendo esta tecnología, dispositivos digitales que permitan la mejora en la seguridad de las personas mediante el reconocimiento facial, pudiendo establecer los límites a la intrusión y en qué grado el reconocimiento facial se puede implementar para cumplir dicha labor.

Un resguardo o vigilancia deja de ser gratificante cuando se percibe que la información personal está siendo mal utilizada y se transforma en una intrusión a la privacidad, sin embargo, frente a escenarios que ponen en riesgo nuestras vidas, la necesidad de un resguardo se hace visible y puede modificar un pensamiento negativo de aceptación frente a este tipo de tecnologías. Para este estudio se contextualizan las situaciones en las cuales la privacidad y la seguridad se ven comprometidas para tomar una decisión. Es decir, en los momentos en los cuales es necesario mantener una vigilancia, y de esta manera encontrar un fundamento válido para su aceptación por los encuestados, por ejemplo, cuando el individuo se ve expuesto de forma física a algún ataque terrorista (en un viaje, dentro de un estadio o centro comercial, etc.), o cuando se ve afectado por un ciberdelito (robo de credenciales, fraude). En concreto, el objetivo de este trabajo es analizar la aceptación por parte de los ciudadanos hacia el reconocimiento facial como medida de seguridad.

REVISIÓN DE LA LITERATURA Y MODELO DE INVESTIGACIÓN

Se presentan conceptos generales acerca del reconocimiento facial y posteriormente una definición de los modelos *Technology Acceptance Model* (TAM) y *Technology Readiness Index* (TRI), y los constructos asociados.

Reconocimiento facial

Tecnología de vigilancia es toda aquella tecnología donde su funcionamiento involucra a las personas como el ente vigilado y a un sistema digital como el agente vigilante (Kerr y Mann, 2006). La vigilancia permite al observante adelantarse a los acontecimientos o prevenir situaciones de riesgo. En particular, este estudio analizará el reconocimiento facial como una tecnología de vigilancia. El reconocimiento facial es un método con el cual es posible identificar a una persona por medio de una imagen o el cuadro de un video, este método se remonta a 1960, donde su concepto comenzó a ver la luz, sin embargo su utilización de forma masiva es más reciente. Actualmente los sistemas de reconocimiento facial son mucho más avanzados, cuentan con algoritmos más complejos, eficientes y eficaces. Lo anterior, debido a la activa investigación durante los últimos años en este tópico (García-Rios et al., 2014).

Estos sistemas de vigilancia se clasifican en dos categorías principales: basados en características y holística. La primera consiste en un procedimiento en el cual se procesan inicialmente las marcas distintivas del rostro (ojos, nariz, boca, etc.), y luego algunas medidas que describan esas regiones, en cambio, la categoría holística intenta identificar los rostros usando representaciones globales, es decir, descripciones basadas en la imagen completa, en vez de las características locales de la cara. Además, existen métodos híbridos que detectan puntos de referencia y luego aplican técnicas utilizadas por la categoría holística(Tome et al., 2015). En los últimos años, muchos países que han adoptado esta tecnología como medida de seguridad, se utilizan en aeropuertos o en áreas públicas y especialmente en lugares con una mayor posibilidad de eventos importantes según el criterio del vigilante. A la fecha, los sistemas que han implementado el reconocimiento facial cuentan con muchos avances, pero también con muchas limitantes y desafíos (nuevas plataformas, rendimiento, ubicuidad, áreas de apoyo, etc.) (Jain et al., 2016).

Modelo de aceptación de la tecnología (Technology Acceptance Model-TAM)

El modelo de aceptación de la tecnología, creado por Fred Davis en el año 1989, se basa en la Teoría de la Acción Razonada y la Teoría del Comportamiento Planeado. El TAM plantea que la aceptación de la tecnología se puede interpretar como la intención y la actitud hacia el uso, la cual se ve afectada por la utilidad percibida y facilidad de uso. La utilidad percibida se refiere al grado en el que una persona cree que al usar una tecnología en particular, su trabajo podría mejorar (Davis, 1989). La facilidad de uso se define como la creencia de una persona en que la tecnología no requerirá mayor esfuerzo para ser utilizada. Además el modelo plantea que facilidad de uso percibida afecta directamente en la utilidad percibida. El TAM es la base de otros modelos de estudio de la aceptación de tecnologías de información. Al abarcar un área tan grande como la tecnología, el TAM permite aplicarlo a diferentes aspectos de ésta, convirtiéndolo en un modelo dinámico y flexible.

Índice de predisposición tecnológica (Technology Readiness Index-TRI)

El TRI 2.0 (Parasuraman y Colby, 2015) es una escala de 16 ítems, basado en el TRI 1.0 (Parasuraman, 2000), que sirve para medir cómo las personas adoptan y utilizan nuevas tecnologías para llevar a cabo tareas en su trabajo o su vida cotidiana. Utiliza cuatro dimensiones: optimismo, innovación, disconformidad e inseguridad. El optimismo es un punto de vista positivo acerca de la tecnología y la creencia de que esta ofrece a las personas una mejora en el control, flexibilidad y eficiencia en sus vidas. La Innovación es la tendencia a ser un pionero en la tecnología y líder intelectual. La disconformidad es una percepción de pérdida de control sobre la tecnología y una sensación de verse abrumado por ella. La inseguridad es una desconfianza sobre la tecnología y escepticismo respecto a su correcto funcionamiento (Parasuraman y Colby, 2001). Las primeras dos dimensiones se consideran positivas respecto al incremento de la predisposición tecnológica. La disconformidad e la inseguridad son inhibidores o con relación negativa respecto a la predisposición tecnológica.

Preocupaciones por la privacidad

Carpenter et al. (2016) desarrollaron una escala que permite entender el nivel de preocupación respecto a la privacidad de la información. El instrumento desarrollado se enfoca en las tres dimensiones (responsabilidad percibida, vulnerabilidad percibida y desconfianza percibida), que afectan las preocupaciones por la privacidad de los individuos. La responsabilidad percibida es el grado en el cual los individuos piensan que podrían ser más responsables por sus acciones al momento de generar un registro. La vulnerabilidad percibida es el grado en el cual los individuos estudiados creen que su información biométrica almacenada es susceptible a amenazas externas o accesos no autorizados. Y la desconfianza percibida se refiere al grado en el cual los individuos se preocupan por que la información que ellos proveen pueda ser usada para objetivos distintos a los estipulados inicialmente.

Modelo de investigación e hipótesis

El modelo de investigación propuesto utiliza TAM y TRI, como se ilustra en la figura 1, además agrega el constructo preocupación por la privacidad de la información, modelado en base a Carpenter et al. (2016).La variable “Percepción de Utilidad” fue elegida del TAM, pues según la literatura es uno de los principales contribuyentes al uso de nuevas tecnologías, esto debido a que – en general - las personas adoptan nuevas tecnologías basándose en sus funcionalidades más que en su facilidad de uso (Davis, 1989).

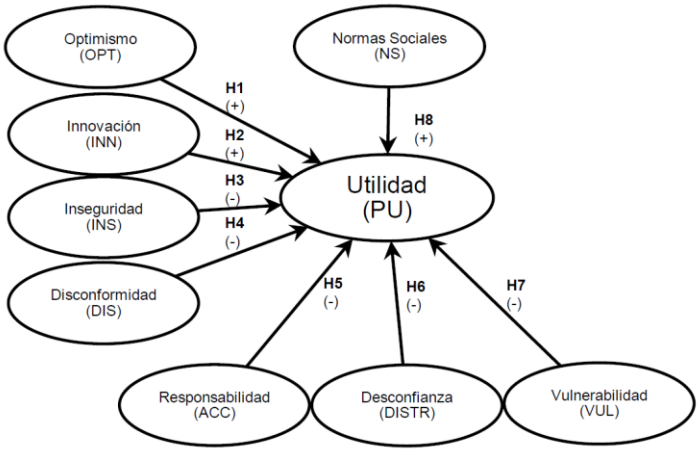

Fig. 1: Modelo de Investigación

Las personas que son optimistas e innovadoras en relación a la tecnología se cree que tienen actitudes positivas hacia la nueva tecnología y el uso de la tecnología. Por lo tanto, proponemos que el optimismo y el nivel de innovación tienen efectos positivos en cómo la gente percibe y se relaciona con la nueva tecnología (Godoe y Johansen, 2012; Parasuraman y Colby, 2015). Así, formulamos las siguientes hipótesis: H1) El optimismo está relacionado positivamente a la percepción de utilidad del reconocimiento facial como medida de seguridad; y H2) La innovación está relacionada positivamente a la percepción de utilidad del reconocimiento facial como medida de seguridad.

Los sentimientos de inseguridad relacionados con la tecnología están asociados con la ambigüedad y el bajo uso de ella (Parasuraman y Colby, 2001). De acuerdo con investigaciones previas(Godoe y Johansen, 2012), asumimos que la inseguridad predice niveles más bajos de utilidad percibida. Por otra parte, la disconformidad podría tener un impacto negativo en la utilidad percibida, si bien existen datos que apoyan (Parasuraman y Colby, 2001) y que refutan esta idea (Godoe y Johansen, 2012), se esperaría que la gente vea el valor de utilidad de un sistema de vigilancia tecnológica en forma distinta si él o ella está más o menos conformes con su utilización. Con esto en consideración, formulamos las siguientes hipótesis: H3) La inseguridad está relacionada negativamente a la percepción de utilidad del reconocimiento facial como medida de seguridad; yH4) La disconformidad está relacionada negativamente a la percepción de utilidad del reconocimiento facial como medida de seguridad.

Carpenter et al., (2016) proponen que las principales dimensiones de las preocupaciones de privacidad relacionadas con la tecnología biométrica son las percepciones de responsabilidad, la desconfianza y la vulnerabilidad. Por tanto, un aumento en los niveles de estas percepciones debería aumentar el grado de utilidad que distinguen las personas en un sistema de vigilancia tecnológica. Así, formulamos las siguientes hipótesis: H5) La responsabilidad percibida está relacionada negativamente a la percepción de utilidad del reconocimiento facial como medida de seguridad; H6) La desconfianza percibida está relacionada negativamente a la percepción de utilidad del reconocimiento facial como medida de seguridad; y H7) La vulnerabilidad percibida está relacionada negativamente a la percepción de utilidad del reconocimiento facial como medida de seguridad.

Finalmente, Venkatesh y Davis (2000) demostraron que las normas sociales - la percepción individual sobre lo que las personas importantes para un individuo piensan que es correcto - son un importante predictor de la utilidad percibida de un sistema tecnológico. Esta propuesta ha sido ratificada en múltiples ocasiones y tecnologías, como ejemplos en Chile están Ramírez (2014), Rondán et al. (2015a), Rondán et al. (2015b). Con esto en consideración, formulamos la siguiente hipótesis: H8) Las normas sociales están relacionadas positivamente a la percepción de utilidad del reconocimiento facial como medida de seguridad.

METODOLOGÍA

Para validar el modelo propuesto se realizó un estudio empírico en Chile los meses de octubre y noviembre del 2016. El método de muestreo fue no probabilístico, por conveniencia. El cálculo del tamaño mínimo de la muestra se determinó usando reglas aceptadas para el análisis con PLS. Según estas reglas, este tamaño está determinado por el mayor valor entre dos posibilidades: (1) diez veces el mayor número de indicadores formativos utilizados para medir una variable latente o (2) diez veces el mayor número de relaciones del modelo dirigidas a una variable latente particular (Hair et al., 2014; Peng y Lai, 2012). En el caso de modelo propuesto, estas reglas determinaron un mínimo de 80 encuestados. Las escalas de medida para las variables del modelo se basaron en la literatura y se midieron con una escala Likert de 5 puntos. La encuesta diseñada puede ser solicitada a los autores. La muestra total fue de 220 ciudadanos, 155 respuestas se obtuvieron en forma presencial en la ciudad de Coquimbo y el resto de forma electrónica mediante las redes sociales. El 53% de los encuestados son de sexo masculino, el 67% con educación superior, y su rango de edad va de los 20 a 65 años. El análisis estadístico de los datos se desarrolló mediante el modelado de ecuaciones estructurales con PLS (*Partial Least Squares*), basado en las fases propuestas por (Ramírez-Correa, 2014). El software utilizado para los cálculos fue SmartPLS 3.1.5 (Ringle et al., 2014).

RESULTADOS

Un primer resultado descriptivo indica que la percepción de utilidad del reconocimiento facial como medida de seguridad fue evaluada por los encuestados con un 3,4 en una escala de 1 al 5 (1.Totalmente en desacuerdo; 2. En desacuerdo; 3. Ni de acuerdo ni en desacuerdo; 4. De acuerdo; y 5. Totalmente de acuerdo). Esto significa que en promedio los encuestados están relativamente más de acuerdo con la utilidad de esta tecnología de vigilancia. En relación al análisis basado en modelado de ecuaciones estructurales, en la Tabla 1 se muestran las cargas de los indicadores de cada una de las variables latentes, siendo la mayoría superiores a 0,7, aceptándose la fiabilidad individual. La Tabla 2 representa el VIF de cada variable latente, todos los valores de aceptan, confirmando la validez interna. También en esta tabla se presentan los

coeficientes CA, CR y AVE, los dos primeros son superiores a 0,7 y el tercero mayor a 0,5, debido a esto se acepta la fiabilidad de los constructos y su validez convergente. Una prueba de la validez discriminante se muestra en la Tabla 3.

La Figura 2 muestra los valores de los betas calculados, y los niveles de significación en base a un procedimiento de *bootstrapping*. Estos resultados soportan las hipótesis H1, H3 y H8. Respecto a las hipótesis H2 y H5, los resultados indican un comportamiento inverso respecto a lo planteado en las hipótesis. Estos mismos resultados no apoyan a las hipótesis H4, H6 y H7 (pues tienen relaciones no significativas). La Tabla 4 muestra los índices de ajuste del modelo, y si bien todos los índices señalan la bondad del modelo estructural, se destaca que el ajuste global (*Goodness of Fit* - GoF) está por encima del umbral indicado como ajuste amplio (Wetzels et al., 2009).

Tabla 1: Ítems y cargas de las variables latentes

Código	*Ítem*	*Carga*
ACC1	Mis registros asociados al reconocimiento facial pueden ser usados en mi contra si hago algo malo	0,78
ACC2	Seré más responsable de las cosas que hago si soy monitoreado por un sistema de reconocimiento facial	0,79
ACC3	Usar un sistema de reconocimiento facial permite a las personas rastrear lo que yo hago	0,68
ACC4	Las organizaciones de seguridad pública (Por ejemplo: Carabineros, PDI, etc.) tendrán mayores pruebas de lo que yo hago si uso el reconocimiento facial	0,67
DIS1	Cuando solicito soporte de un proveedor de servicios o productos tecnológicos, ocasionalmente siento que me encuentro en desventaja porque él sabe más que yo	0,73
DIS2	Las líneas de soporte técnico NO son muy útiles debido a que no explican cosas en términos que yo entienda	0,79
DIS3	A veces pienso que los sistemas tecnológicos NO están diseñados para ser usados por personas comunes	0,67
DIS4	NO existen manuales para productos o servicios tecnológicos que sean escritos en lenguaje simple	0,71
DISTR2	Confío que el registro obtenido por el sistema de reconocimiento facial NO será usado para otros propósitos que no sean seguridad del sistema	0,78
DISTR3	Las entidades de vigilancia NO usarán mi registro biométrico para llevar a cabo verificaciones de antecedentes	0,85
DISTR6	Las entidades de vigilancia pueden ser confiable respecto a mi información biométrica	0,70
INN1	Otras personas me solicitan consejo acerca de nuevas tecnologías	0,80
INN2	En general, soy de los primeros en mi grupo de amigos en adquirir nuevas tecnologías cuando aparecen	0,59
INN3	Usualmente entiendo las nuevas tecnologías sin la ayuda de otros	0,96
INN4	Me mantengo al día con los nuevos desarrollos tecnológicos de mi área de interés	0,61
INS1	Las personas dependen demasiado en que la tecnología haga cosas por ellos	0,64
INS2	Demasiada tecnología distrae a las personas a un punto en que llega a ser peligroso	0,88
INS3	La tecnología disminuye la calidad de las relaciones, ya que reduce la interacción personal	0,80
INS4	NO me siento confiado de hacer transacciones comerciales con una organización que solo puede ser accedida por Internet	0,63
NS1	Las personas que son importantes para mí piensan que debiera aceptar el reconocimiento facial	0,93
NS2	Las personas que influencian mi comportamiento piensan que debiera utilizar el reconocimiento facial	0,94
NS3	Las personas cuyas opiniones yo valoro prefieren que yo use el reconocimiento facial	0,94
OPT1	Las nuevas tecnologías contribuyen a tener una mejor calidad de vida	0,81
OPT2	La tecnología me entrega mayor libertad al movilizarme	0,77
OPT3	La tecnología le entrega a las personas mayor control sobre su diario vivir	0,80
OPT4	La tecnología me hace más productivo en mi vida personal	0,70
PU1	Pienso que el reconocimiento facial es útil en mi vida	0,85
PU2	El reconocimiento facial ayuda a resolver las cosas más rápido	0,91
PU3	El reconocimiento facial incrementa la productividad	0,90
VUL1	Cualquiera puede acceder a mi información biométrica que es almacenada en el sistema	0,66
VUL2	Los servidores que almacenan la información NO son seguros frente a Hackers	0,70
VUL3	Se almacenarán mis registros de reconocimiento facial de forma NO segura	0,87

Tabla 2: Coeficientes del modelo de medida

Variable	*VIF*	*Alfa de Cronbach (CA)*	*Fiabilidad Compuesta (CR)*	*Varianza Promedio Extraída (AVE)*
ACC	1,44	0,72	0,82	0,54
DIS	1,46	0,71	0,82	0,52
DISTR	1,11	0,67	0,82	0,61
INN	1,43	0,84	0,83	0,57
INS	1,33	0,73	0,83	0,56
NS	1,40	0,93	0,95	0,87
OPT	1,28	0,78	0,86	0,60
PU	NC	0,86	0,92	0,79
VUL	1,28	0,61	0,79	0,56

Tabla 3: Análisis de validez discriminante

Variable	*ACC*	*DIS*	*DISTR*	*INN*	*INS*	*NS*	*OPT*	*PU*	*VUL*
ACC	0,73								
DIS	0,18	0,72							
DISTR	0,11	0,08	0,78						
INN	0,05	-0,40	0,03	0,75					
INS	0,24	0,42	0,15	-0,23	0,75				
NS	0,42	0,16	0,30	-0,01	0,17	0,93			
OPT	0,20	0,05	0,12	0,34	0,04	0,28	0,77		
PU	0,44	0,21	0,27	-0,11	0,29	0,65	0,26	0,89	
VUL	0,37	0,27	0,07	-0,10	0,32	0,11	0,02	0,19	0,75

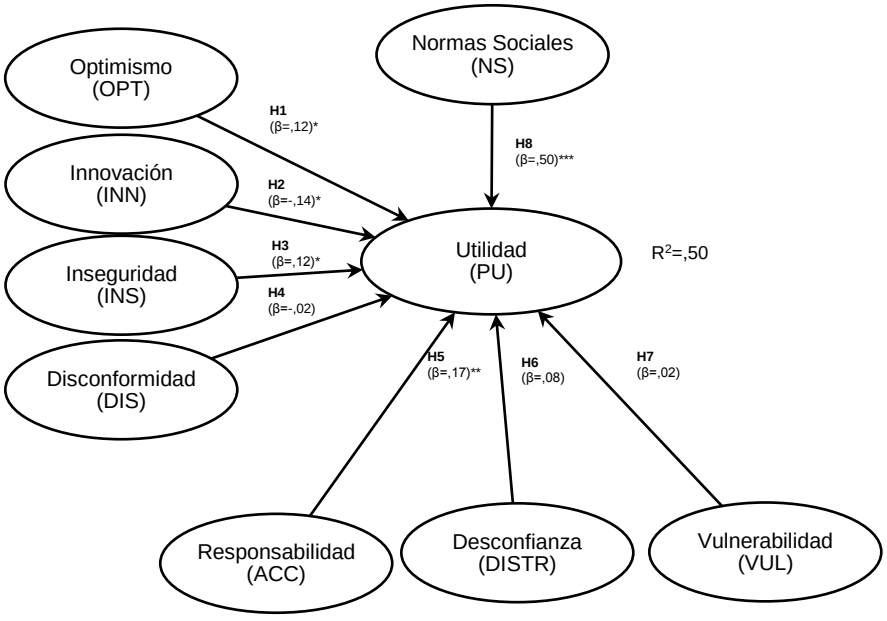

Fig. 2: Resultados del análisis PLS (* p <0,05; ** p <0,01;*** p<0,001)

Tabla 4: Índices de ajuste del modelo

Índice	Valor
Coeficiente de trayectoria promedio(APC)	0,11
R^2 promedio (ARS)	0,50
Factor de inflación de varianza promedio (AAVE)	0,62
Índice de Ajuste Global (GoF)	0,56

DISCUSIÓN

En el presente estudio se han estudiado las relaciones entre algunos rasgos de personalidad (optimismo, innovación, inseguridad y disconformidad) y una variable de TAM (percepción de utilidad), además del constructo preocupaciones por la privacidad. En general, el modelo planteado fue validado para Chile, sin embargo la relación establecida entre la variable innovación y la percepción de utilidad del reconocimiento facial como una tecnología de vigilancia no se comportó como se planteó en la hipótesis H2, ésta obtuvo una relación negativa, indicando que cuando una persona posee un nivel de innovación mayor, su percepción de utilidad respecto a la tecnología en estudio disminuye. Este efecto podría tener una explicación según (Walczuch et al., 2007), quienes concluyen que las personas con mayor nivel de innovación son más críticos frente a la tecnología, ya que al estar más cercanos a los nuevos desarrollos tienen mayores expectativas y demandas. Por otra parte, los resultados revelaron que no todas las dimensiones del TRI influencian la percepción de utilidad, siendo el optimismo el único motivador para la variable en cuestión y la innovación e inseguridad los inhibidores (la variable disconformidad resulto no influyente para este modelo, ya que su relación no es significativa).

Las variables relacionadas con las preocupaciones por privacidad fueron las que generaron mayor controversia, debido a que se esperaban relaciones muy influyentes, particularmente en la desconfianza y vulnerabilidad, sin embargo, estas fueron estadísticamente no significativas. Es más, en relación a las preocupaciones por privacidad asociadas a la responsabilidad, propuesta como hipótesis 5, los resultados indican que la relación es positiva, es decir, a mayor preocupación más utilidad percibida de la tecnología. En futuros trabajos debería ser analizado este hallazgo. A diferencia de las anteriores variables, las normas sociales fueron las que influyeron mayormente en la explicación de la utilidad percibida del reconocimiento facial como medida de seguridad. Dado que Chile está por debajo del promedio latinoamericano en victimización (Latinobarómetro, 2016), y que, según las últimas estadísticas, las tasas de victimización agregada de delitos consumados en las regiones de Antofagasta y Coquimbo son 25,6% y 21,1%, respectivamente, menores al promedio nacional de 26,4% (INE, 2016), creemos que los resultados de este estudio podrían variar en regiones o países con mayores índices de inseguridad.

CONCLUSIONES

El objetivo de este trabajo fue analizar la aceptación por parte de los ciudadanos hacia el reconocimiento facial como medida de seguridad. En base a los resultados obtenidos, cinco de las ocho variables antecedentes del modelo propuesto predicen un 50% de la percepción de utilidad de estas tecnologías biométricas. En orden de importancia, estas variables son: las normas sociales, la percepción de responsabilidad, el optimismo, el grado de innovación, y la percepción de inseguridad. Dentro de las fortalezas del presente estudio se destaca que la validación de las escalas de medida ajustadas a Chile permite futuras réplicas con el fin de mejorar el entendimiento sobre la aceptación de la población chilena del reconocimiento facial como una tecnología de vigilancia. Una importante implicancia práctica de estos resultados tiene relación con las normas sociales, pues al aumentar la percepción individual sobre lo que las personas importantes para un individuo piensan que es correcto aumenta la percepción de utilidad de esta tecnología de seguridad, por tanto, un posible camino para aumentar la aceptación de este tipo de tecnología por parte de los ciudadanos chilenos es realizar acciones de publicidad orientadas a mostrar como otros ciudadanos ven de utilidad el reconocimiento facial como medida de seguridad. La mayor limitación de este estudio es el número de individuos de la muestra y el uso de un procedimiento de muestreo no aleatorio. Finalmente, y dado el nivel moderado de predicción del modelo, en futuros estudios se debería explorar la incorporación de nuevas variables antecedentes o moderadoras.

REFERENCIAS

Aquilina, K., Public security versus privacy in technology law: A balancing act?, Computer Law & Security Review, 26(2), 130-143 (2010)

Carpenter, D., Maasberg, M., Hicks, C., y Chen, X., A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system, International Journal of Information Management, 36(5), 735-747 (2016)

Davis F.D., Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS quarterly, 13(3), 319-340 (1989)

García-Rios, E., Escamilla-Hernández, E., Nakano-Miyatake, M., y Pérez-Meana, H., Sistema de Reconocimiento de Rostros Usando Visión Estéreo, Información Tecnológica, 25(6), 117-130 (2014)

Georgiadou, Y., Fischer-Hübner, S., Surveillance and Privacy, En J. Berleur, M. D. Hercheui y L. M. Hilty (Eds.), What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience, IFIP Advances in Information and Communication Technology, 328, 175-177 (2010)

Godoe, P., y Johansen, T., Understanding adoption of new technologies: Technology readiness and technology acceptance as an integrated concept, J. of European Psychology Students, 3(1), 38-52 (2012)

Hair, J. F., Sarstedt, M., Hopkins, L., y Kuppelwieser, V. G., Partial least squares structural equation modeling (PLS-SEM), European Business Review, 26(2), 106-121 (2014)

Hughes, R. D., Two concepts of privacy, Computer Law & Security Review, 31(4), 527-537 (2015)

INE, Instituto Nacional de Estadísticas, Presentación de resultados XII encuesta nacional urbana de seguridad ciudadana ENUSC 2015. (En línea: http://www.ine.cl, acceso: Octubre, 2017) (2016)

Jain, A. K., Nandakumar, K., y Ross, A., 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters, 79, 80-105 (2016)

Kerr, I., y Mann, S., Exploring equiveillance. (En línea: http://www.anonequity.org, acceso: Enero, 2006), Blog on nymity (2007)

Latinobarómetro, Latinobarómetro Informe 2016 (En Línea: http://www.latinobarometro.org, acceso: Octubre, 2017) (2016)

Peng, D. X., y Lai, F., Using partial least squares in operations management research: A practical guideline and summary of past research, Journal of Operations Management, 30(6), 467-480 (2012)

Parasuraman, A.,Technology Readiness Index (Tri), Journal of Service Research, 2(4), 307-320 (2000)

Parasuraman, A., y Colby, C. L.,Techno-Ready Marketing: How and Why Your Customers Adopt Technology: The Free Press (2001)

Parasuraman, A., y Colby, C. L., An Updated and Streamlined Technology Readiness Index, Journal of Service Research, 18 (1), 59-74(2015)

Ramírez, P. E., Uso de internet móvil en Chile: explorando los antecedentes de su aceptación a nivel individual, Ingeniare. Revista Chilena de Ingeniería, 22 (4), 560-566 (2014)

Ringle, C., Wende, S., y Becker, J., Smartpls 3.1. 5. University of Hamburg, Hamburg, Germany (2014)

Rondán, F. J., Arenas, J., y Ramírez, P.E., Travel buying behavior in social network site users: to buy online vs. offline, Journal of theoretical and applied electronic commerce research, 10(1), 49-62 (2015)

Rondan, F.J., Arenas, J., y Ramírez, P.E., A comparison of the different versions of popular technology acceptance models: A non-linear perspective, Kybernetes, 44(5), 788-805 (2015)

Tome, P., Vera, R., Fierrez, J., y Ortega, J., Facial soft biometric features for forensic face recognition, Forensic Science International, 257, 271-284 (2015)

Venkatesh, V., y Davis, F. D., A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management science, 46(2), 186-204 (2000)

Wetzels, M., Odekerken-Schroder, G., y van Oppen, C., Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration, MIS Quarterly, 33(1), 177-196 (2009)

Walczuch, R., Lemmink, J., y Streukens, S.,The effect of service employees' technology readiness on technology acceptance. Information Management, 44(2), 206-215 (2007)