Estudio exploratorio de la victimización on-line en Chile: un enfoque desde la teoría de actividades rutinarias

Hugo Soto Ojeda
Investigador Centro de Estudios del Futuro

CENTRO DE ESTUDIOS DEL FUTURO
UNIVERSIDAD DE SANTIAGO DE CHILE

Estudio exploratorio de la victimización on-line en Chile: un enfoque desde la teoría de actividades rutinarias

Hugo Soto O.
Centro de Estudios del Futuro,
Universidad de Santiago de Chile

RESUMEN

Propósito – El propósito de este estudio es explorar la victimización por seis tipos de ciber-delitos en Chile y analizar su relación con actividades y prácticas cotidianamente desarrolladas on-line, además de otras variables demográficas. El estudio operacionaliza conceptos centrales de la teoría de actividades rutinarias para analizar por qué ciertos individuos y grupos tienen más probabilidad de ser víctima de un ciber-delito que otros. Los ciber-delitos analizados fueron: amenazas, hostigamiento sexual, estafa, robo de identidad bancaria, hacking e infección por virus o malware.

Metodología - Los datos analizados corresponden a una muestra de 1700 usuarios de internet quienes respondieron un cuestionario con preguntas referidas a usos de internet y medidas preventivas adoptadas. La variable dependiente del estudio se midió preguntando si el entrevistado había sufrido o no cada uno de los ciber-delitos considerados. Los datos fueron analizados mediante técnicas de análisis multivariado, concretamente, modelos de regresión logística binaria.

Resultados - Algunas actividades y prácticas on-line, así como variables demográficas, se relacionan significativamente con uno o varios de los ciber-delitos analizados. Estos resultados permiten concluir que el riesgo de victimización por delitos on-line no se distribuye aleatoriamente entre los usuarios de Internet, identificando algunos de los factores que explican por qué algunos individuos y grupos tiene una mayor probabilidad de victimización por este tipo de acciones delictuales.

CENTRO DE ESTUDIOS DEL FUTURO
UNIVERSIDAD DE SANTIAGO DE CHILE

I. INTRODUCCIÓN

El crecimiento del ciber-crimen es una importante fuente de preocupación en materia de seguridad y prevención del delito en Chile y el mundo. Ya sean delitos tradicionales con nuevos modus operandi posibilitados por el ciber-espacio -como las estafas- o nuevos delitos que no podrían ocurrir sin la existencia de computadores y almacenamiento de información - como el hacking- (Graboski 2001, Wall 2007). La prevalencia del ciber-delito está creciendo de manera significativa, impulsada por la explosiva masificación de Internet y otras nuevas tecnologías de información (Caneppele y Aebi 2017, Levi 2017).

En el caso de Chile, un informe de la empresa Fortinet estimó en 1.5 billones los intentos de ciberataques en 2019, dirigidos a la detección de vulnerabilidades en el ciber-espacio. Por otra parte, datos oficiales a partir de la Encuesta Nacional de Seguridad Pública (ENUSC) señalan que el porcentaje de víctimas de estafas por internet se ha duplicado entre 2015 y 2019, al igual que el porcentaje de victimas de amenazas. Del mismo modo, el porcentaje de victimas de robo de identidad bancaria casi se ha triplicado durante este período, aun cuando los niveles son todavía bajos (probablemente sub-estimados).

A pesar de la creciente relevancia de la ciber-seguridad en la agenda pública en Chile, la discusión y escasa evidencia sistemática existente ha estado concentrada en los ciber-delitos que afectan a empresas y el Estado, pero poco se conoce respecto de la ciber-victimización casera, esto es, la que afecta a personas y hogares. Así, gran parte de información disponible respecto de ciber-delitos en Chile proviene de informes privados que analizan las amenazas informáticas que enfrentan las empresas, y discuten tecnologías para enfrentarlas.

En relación a los ciber-delitos que afectan a personas y hogares en Chile, no existen estudios que identifiquen las características de las personas que ha sido víctima de ciber-delitos, ni de las circunstancias que facilitan la ocurrencia de la ciber-victimización. Si bien, existe una incipiente literatura jurídico-normativa respecto del ciber-delito que considera su ocurrencia a nivel de personas naturales, la evidencia empírica respecto de quiénes son las víctimas, en qué circunstancias se comete y cuáles son los factores que facilitan o explican que una persona sea o no víctima de ciber-delitos, es aun escasa en Chile. En este

sentido, existe la necesidad de desarrollar mayor conocimiento en esta área, pues el despliegue de políticas e iniciativas de prevención del ciber-delito requiere conocer qué factores están relacionados al mismo.

El presente estudio busca contribuir a ese propósito por medio del análisis empírico de 6 tipos de ciber-delitos en Chile: amenazas, hostigamiento sexual, estafa, robo de identidad bancaria, hacking e infección por virus o malware. A partir de una muestra de aproximadamente 1.700 usuarios de Internet en Chile, se analizó la relación entre la probabilidad de ser víctima de los delitos analizados y un conjunto de variables referidas al uso de internet y medidas de protección adoptadas. Los datos fueron analizados mediante técnicas de análisis multivariadas y en conjunto señalan que la victimización por ciber-delitos no se distribuye aleatoriamente entre los usuarios de internet, sino que está relacionada a determinados usos y practicas on-line.

II. ¿QUÉ SABEMOS SOBRE CIBER-VICTIMIZACIÓN?

En el contexto de creciente masividad del ciber-delito, éste ha emergido como un área relevante para la criminología del siglo XXI. Así, durante las últimas dos décadas un creciente, pero aún limitado, número de investigaciones han estudiado el impacto de las nuevas tecnologías de la información en la criminalidad, los factores que afectan el riesgo de ciber-victimización, y la pertinencia y aplicabilidad de los conceptos teóricos tradicionales de la criminología en su análisis (Holt and Bossler 2014) . Estos estudios han analizado un amplio rango de ciber-delitos, incluyendo hackeo (Bossler and Holt 2009; Choi 2008; Ngo and Paternoster 2011), robo de identidad y estafas (Holtfretter et al. 2008; Newman and Clarke 2003; Pratt et al. 2010; Bossler and Holt 2011; Holt and Turner 2012), amenazas y acoso (Bocij2004; Hinduja and Patchin 2009; Holt and Bossler 2009), y en conjunto dan cuenta del creciente interés de los estudios criminológicos en el ciber-crimen.

Gran parte de los estudios que han abordado la ciber-victimización lo hacen desde la perspectiva y herramientas conceptuales de la teoría de las actividades rutinarias (Vakhitova et. al. 2015). El precepto básico de esta teoría es que la comisión de delitos no depende solo de las motivaciones del potencial infractor,

sino que depende también de las características de los potenciales targets[1] y de las condiciones en que se da el encuentro entre ambos. Concretamente, desde esta perspectiva teórica se señala que un evento delictivo ocurre cuando se da el encuentro de un infractor motivado con un target adecuado, en condiciones de desprotección de este último. De este modo, la probabilidad de ocurrencia de un evento delictivo dependerá de la concurrencia de estos tres elementos, y la modificación de las propiedades de cualquiera de ellos afectará la probabilidad de ocurrencia del evento delictivo.

Este enfoque en el evento delictivo antes que en las motivaciones del infractor, y la idea que la probabilidad de ocurrencia de un delito puede ser reducida modificando otras variables distintas a las motivaciones del infractor, hace de las teoría de actividades rutinarias, y de las teorías de la oportunidad más en general, un marco teórico particularmente útil para el análisis del ciber-crimen, dado el escaso conocimiento existente en relación a los autores de este tipo de delitos.

Como se señaló anteriormente, desde la teoría de actividades rutinarias se señala que una condición para que el delito ocurra es la presencia de un target adecuado en condiciones adecuadas. Los elementos que hacen que una target sea adecuado son sintetizados en el acrónimo VIVA para referirse a la medida en que el target es visible, fácil de transportar (inercia), valioso y accesible. Estos conceptos, que han probado su utilidad en relación a distintos tipos de delitos, han sido también aplicados en el análisis de las ciber-victimización.

Visibilidad refiere al grado de exposición del target a los potenciales atacantes o, en otras palabras, a la facilidad con que interesados pueden "ver" al eventual target. Aplicado al análisis de la ciber-victimización, visibilidad alude a la realización de actividades rutinarias on-line - tales como participar en redes sociales, navegar en internet, hacer transferencias bancarias o ver películas- que exponen al usuario a ser detectado por potenciales agresores (Holt and Bossler, 2013; Jansen and Leukfeldt, 2015). Inercia en el mundo físico refiere a las propiedades físicas de un target y la facilidad con que puede ser transportado. Yar (2005) sostiene que si bien los archivos digítales no tienen peso, aspectos tales como la velocidad de descarga y especificaciones técnicas de los archivos pueden ser vistas como formas de inercia en tanto determinan los niveles de

[1] Desde la teoría de actividades rutinarias se diferencia entre target y víctima. Mientras esta última puede o no estar presente en la comisión del delito, por ejemplo en un robo de casa o vehículo, el target siempre está.

resistencia que el target puede ofrecer. El valor que el agresor otorga al target, y que motiva el intento de apropiación, puede ser económico, como el caso de robo de identidad bancaria, o de status u otro tipo de gratificaciones emocionales, como en el caso de amenazas u hostigamiento sexual. Accesibilidad refiere a la capacidad del agresor de contactar el target (Felson, 1994). Es distinto a visibilidad, en tanto un target puede ser visible, pero difícil de alcanzar. En el caso de ciber-delitos, en los que el target por excelencia suele ser información de los usuarios, la medida de accesibilidad más común en las investigaciones sobre ciber-crimen suele ser la disponibilidad de información personal introducida, voluntaria o involuntariamente, al ciber-espacio.

Finalmente, la teoría de actividades rutinarias hace hincapié en las condiciones de vigilancia o protección (guardianship) en que se desarrolla el encuentro entre agresor y target, cuya presencia o ausencia afecta la probabilidad de ocurrencia del evento delictivo. Los estudios en ciber-crimen han operacionalizado este elemento de la TAR en medidas de protección agrupadas en digitales - como tener instalado un software antivirus- y personales -como usar contraseñas complejas (Akdermi y Lawless 2020). Como se describe más adelante, los resultados de investigaciones empíricas acerca del efecto de las medidas de protección en el riesgo de ciber-victimización son ambiguos (Williams 2015; Ngo and Paternoster, 2011; Reyns et al., 2016).

A partir del marco conceptual de la TAR, varios estudios han examinado empíricamente la relevancia de los elementos conceptualizados en la estimación del riesgo de ciber-victimización. Visibilidad y accesibilidad han sido usualmente medidas a partir de la participación en legítimas actividades on-line tales como como navegar, leer, comprar, hacer transferencias bancarias o participar en redes sociales. Marcum et. al (2010) encuentran que las frecuencia de participación en este tipo de actividades incrementa la probabilidad de ser víctima de hostigamiento sexual. Ngo y Paternoster (2011),Paek y Nalla (2015) y Reyns (2015) encuentran que la visibilidad a través de estas actividades incrementan el riesgo de pishing. Del mismo modo, Holt y Copes (2010) y Reyns (2015) han mostrado que participar en foros on-line, compartir información en redes sociales y acceder a contenido de adultos en la red, incrementan el riesgo de ser víctima de hackeo.

Otros estudios, han mostrado la relación del riesgo de virus o malware con actividades como comprar, hacer reservas e interactuar en redes sociales (Reyns, 2015), descargar programas, jugar en línea (Leukfeldt 2015), ver películas on line e ingresar a sitios de citas (Holt et. al. 2018) y, en términos más generales, con la frecuencia con que se accede a internet (Bergmann et al., 2018). Finalmente, Leukfeldt y Yar (2016) concluyen que la visibilidad del target juega un rol en los 6 tipos de delitos considerados en su estudio: hacking, virus, robo de identidad, fraude, amenazas y hostigamiento.

Del mismo modo, la gran mayoría de los estudios respecto de ciber-victimización incorporan en sus análisis el efecto de medidas de protección por parte de los usuarios de internet, ya sea sean medidas técnicas (como el uso de anti-virus) o medidas personales (por ejemplo, cambiar habitualmente las contraseñas). Al respecto, Reyns (2015), que analiza la ciber-victimización a partir de datos de la Canadian General Social Survey, encuentra que el uso de antivirus y la práctica de borrar correos de desconocidos disminuye la probabilidad de infección por malware, así como el cambio habitual de contraseñas reduce la probabilidad de pishing y hacking. Sin embargo, la gran mayoría de la literatura disponible no encuentra efectos significativos, o encuentra efectos contra-intuitivos, del uso de antivirus y otras medidas de protección en el riesgo de ciber- victimización por distintos delitos (Holt y Bossler 2009; Marcum et. al. 2010; Bossler y Holt 2013; Ngo y Paternoster 2011; Reyns, Henson y Fisher 2011; Leukfeldt y Yar 2016; Williams 2015; Akdemir y Lawless 2020).

III. EL PRESENTE ESTUDIO

El presente estudio se inserta en la línea de investigaciones descrita en el apartado anterior y explora la relación entre distintos usos cotidianos de internet y el riesgo de ciber-victimización en Chile. Este análisis contribuye a la literatura respecto de ciber-victimización y los factores que la afectan, en tres aspectos.

En primer lugar, mientras la casi totalidad de los estudios en ciber-victimización han sido realizados en el contexto de países desarrollados, este estudio analiza la relación entre los distintos usos de internet y la victimización por ciber-delitos en el contexto latinoamericano, particularmente en Chile. El único estudio latinoamericano conocido en esta línea de investigación, usando o no el marco teórico de la TAR, es el realizado por Rodriguez, Oduber y Mora (2017)

con una muestra de 300 estudiantes universitarios en Venezuela. Sin duda, se requiere más investigación sistemática en los factores de la ciber-victimización en nuestra región, y en general acerca del ciber-crimen en Latinoamérica. Este estudio espera contribuir a llenar parte de ese vacío, a partir del estudio de una muestra de usuarios de internet en Chile.

En segundo lugar, este estudio examina el riesgo de victimización por diferentes tipos de ciber-delitos. La mayoría de los estudios revisados analizan factores asociados a la victimización por uno o un subconjunto de ciber-delitos parecidos (Choi 2008, Bossler y Holt 2009, Reyns 2015, entre otros), o categorías más amplias que agregan delitos de un mismo tipo (Akdemir y Lawless 2020). En esta investigación, se examinó la relación entre usos de internet y seis tipos de ciber-delitos: Amenazas, hostigamiento sexual, estafa, robo de identidad bancaria, hackeo e infección por virus o malware. El análisis diferenciado de cada uno de estos ciber-delitos revela que los distintos usos de internet están relacionados con algunos tipos de ciber-delitos y no con otros.

Finalmente, con la excepción de aquellos estudios que analizan datos de ciber-victimización recogidos en el contexto de encuestas con propósitos más generales (Reyns 2015, Akdemir y Lawless 2020), la mayoría de los estudios revisados utiliza muestras relativamente pequeñas de estudiantes universitarios (ejemplo, Holt y Bossler 2013; Ngo y Paternoster 2011, Rodriguez et. al. 2017). Sin embargo, la generalización de resultados basados en muestras de estudiantes universitarios es cuestionable en la medida que es esperable que las habilidades informáticas de los estudiantes universitarios sea mayor al del conjunto de la población (Van Wilsen 2013, Subtel 2017). Este estudio, en cambio, se hace sobre una muestra que considera distintos niveles de educación y perfiles demográficos.

IV. DATOS Y METODOLOGÍA

Los datos utilizados en este estudio provienen de una muestra por conveniencia de usuarios de internet que respondieron una encuesta aplicada entre junio y julio del año 2020. Para la recolección de la información se aplicó un cuestionario on-line con preguntas referidas a experiencias de ciber-victimización - esto es si ha sufrido o no cada uno de seis tipos de ciber-delitos, usos de internet y medidas de prevención adoptadas. El contacto con los participantes de la encuesta se realizó mediante el envío masivo de un correo electrónico invitando

a responder la encuesta, para lo que se proveía un enlace electrónico. La invitación fue enviada a 10.000 correos electrónicos, seleccionados desde una base de datos provista por la empresa encuestadora, considerando diferentes perfiles de usuarios en términos de grupos socioeconómicos, grupos etarios y sexo. En total se recibieron 2.071 respuestas. Debido a falta de información suficiente en algunas de ellas, los análisis y modelos de regresión presentados en este artículo fueron realizados sobre la base de una muestra final de 1696 casos.

En términos generales, el 60% de los de la muestra final es de sexo femenino y 40% de sexo masculino. El 17.86% de la muestra analizada tiene entre 15 y 24 años; 22.25% entre 25 y 34 años; 33.87% entre 35 y 44 años; y 21% tiene 55 años o más (4.9% no indica). En términos socio-educacionales, el 59% de la muestra tiene educación universitaria (completa o incompleta) y el 57.6% pertenece a grupos socioeconómicos altos y medios altos[2], sobrerrepresentado la participación de estos grupos en comparación a su distribución en la población en general.

En cuanto a los dispositivos usados para acceder a Internet, el 57% de los entrevistados los hace por medio del teléfono móvil, el 20% a través de computador de escritorio, y el 21% de ellos lo hace mediante laptop o computador portátil. Análisis de las tasas de victimización en cada uno de estos grupos de usuario, muestran que no hay diferencias significativas en el porcentaje de victimas de ciber-delito en general, ni en cada uno de los tipos de incidentes analizados.

Variable dependiente

Los entrevistados fueron consultados respecto de si habían sufrido algunos de los siguientes tipos de ciber-delitos en los últimos 12 meses: Amenaza, Acoso u hostigamiento sexual, Hackeo, Estafa, Robo de identidad bancaria, e Infección del dispositivo por Virus o Malware. El fraseo exacto de cada una de las preguntas fue:

Amenaza: En los últimos 12 meses, ¿Ha sufrido amenazas de daño o ataque físico hechos mientras está conectado a Internet o a través de correo electrónico?

[2] La clasificación de grupos socio-económicos es posterior a la aplicación de la encuesta y se realiza según descripción de los grupos socioeconómicos de Adimark. Para la clasificación se consideran los antecedentes señalados por los propios encuestados: auto clasificación, nivel de renta, estudios del jefe de hogar y ocupación del jefe de hogar

Acoso: En los últimos 12 meses, ¿Ha sido víctima de acoso u hostigamiento a través de mensajes indecentes u obscenos, comunicaciones, imágenes no solicitadas o requerimientos de carácter sexual?

Hackeo: En los últimos 12 meses, ¿Ha sido afectado por el hackeo o acceso no autorizado al computador, teléfono u otro dispositivo para robar, alterar, destruir información o solicitar pago para desbloquear computador o dispositivo?

Estafa: En los últimos 12 meses, ¿Ha sido afectado por alguna estafa al comprar a través de Internet productos o servicios que nunca llegaron, eran falsos, o en definitiva nunca existieron?

Robo identidad bancaria: En los últimos 12 meses, ¿Usted ha sido afectado por suplantación de identidad en su cuenta bancaria o tarjetas de crédito o comerciales?

Virus: En los últimos 12 meses, ¿Ha sido afectado por Infección con virus o malwares del computador, teléfono u otro dispositivo con acceso a Internet?

Las respuestas posibles a cada una de las preguntas (Sí/No) fueron dicotómicamente codificadas (1= víctima, 0= No victima). Adicionalmente se creó una nueva variable "victimización general" que toma valor 1 si el entrevistado sufrió alguno de los incidentes preguntados y 0 si no sufrió ninguno de ellos. Estas variables fueron analizadas mediante modelos de regresión logit para variables dependiente binarias.

Variables independientes

El principal objetivo de este estudio es identificar factores de riesgo para la victimización on-line usando el marco teórico de la teoría de actividades rutinarias, e investigaciones previas, en tanto guía para el análisis. Varios ítems de la encuesta aplicada fueron usados para crear múltiples medidas de las actividades rutinarias que los usuarios realizan en la web, las que pudieran incrementar o disminuir su nivel de visibilidad, accesibilidad y protección, y estar relacionados al riesgo de victimización. Así mismo, se incluyó en los modelos analizados, características de los encuestados – sexo, edad, GSE- que pudieran reflejar rutinas on-line omitidas o que pudieran influenciar el riesgo de victimización más allá del efecto de las oportunidades on-line.

Visibilidad: la exposición on-line fue medida mediante preguntas que capturan actividades on-line que eventualmente pudieran crear oportunidades de victimización mediante la visibilidad o exposición de los usuario a potenciales victimarios. Las actividades consideradas fueron: navegar en la red, utilización de redes sociales, descarga o visualización de películas, lectura on-line y venta de productos. Cada una de estas variables miden la frecuencia con que con que los sujetos de la muestran participan en esas actividades on-line en el último mes. Las posibles respuestas fueron: ***todos los días, al menos una vez a la semana pero no todos los días, al menos una vez al mes, pero no todas las semanas, y nunca***. Las respuestas fueron codificadas con valor 4 indicando participación diaria y valor 1 indicando que el entrevistado no ha usado nunca Internet para la actividad referida.

Accesibilidad: la accesibilidad a la víctima (y sus datos) fue operacionalizada usando ítems del cuestionario que refieren a la información que los usuarios comparten en Internet. Para saber si los usuarios comparten información relativa a sus datos bancarios se preguntó con qué frecuencia realizan transferencias bancarias (1= nunca; 4= todos los días). Para saber si los usuarios comparten información personal en Internet se utilizaron tres preguntas dicotómicas (0=no, 1= si): sube contenido propio a redes sociales, comparte estados de ánimo en redes sociales y comparte fotografías en redes sociales. Además se consultó directamente si evita o no entregar información personal en redes sociales.

En materia de protección o guardianship se consideraron cuatro variables dicotómicas que indican comportamientos preventivos mientras se está en internet. En primer lugar, se preguntó a los encuestados si el dispositivo que usa para conectarse a internet cuenta con software antivirus, los cuales están destinados a proteger el dispositivo de ciertas amenazas tales como virus, adwares y spywares. En segundo lugar, se preguntó si el usuario habitualmente descarga actualizaciones y parches de softwares. La tercera variable considerada fue si el usuario usualmente borra, sin abrir, los e-mails de origen sospechoso. Finalmente, se consultó si el usuario sólo agrega personas conocidas a sus redes sociales.

Características individuales. La literatura, y particularmente la investigación empírica sobre ciber-victimización, reporta que ciertas características individuales consistentemente afectan el riesgo de victimización por ciber-delitos. En esta línea, el presente estudio considera variables de sexo, edad y

status socioeconómico en el análisis. La variable sexo fue medida como variable dicotómica donde 0=mujer y 1= hombre. La variable edad fue medida mediante una escala ordinal que considera 4 categorías: 15-24 años, 25-34 años, 35-54 años, y 55 años y más. El status socioeconómico se computó sintetizando información sobre nivel educacional, ocupación e ingresos. Los grupos considerados fueron ABC1a, C1b, C2, C3, y D-E.

Método de análisis

Dada la naturaleza dicotómica (Sí/ No) de las variables dependientes de interés (ciber-victimización), se estimaron 6 modelos de regresión logística binaria, uno por cada delito analizado. Mediante estos modelos de análisis multivariados es posible estimar el efecto de una variable independiente sobre la variable dependiente, controlando por las otras variables independientes consideradas en el modelo.

La estimación del efecto (Coef.) de cada variable independiente sobre la variable dependiente Victimización se muestra en la segunda columna de las tablas de resultados. Para facilitar su lectura, la cuarta columna de las mismas tablas presenta los Odds Ratios estimados (= exp(Coef.)). Si el OR estimado es igual a 1 debe entenderse que la variable independiente no tiene efecto sobre la variable dependiente. Si el OR estimado es superior o inferior a 1, significa que la presencia de la variable independiente aumenta o disminuye la probabilidad de ocurrencia de la variable independiente. Por ejemplo, si el OR estimado es de 1.45 significa que la presencia de la variable independiente aumenta en un 45% la realización de la variable dependiente (ciber- victimización). Por el contrario, si el OR estimado fuera 0.25 significaría que la presencia de la variable independiente reduce en un 75% la probabilidad de ocurrencia de la variable dependiente, o lo que es igual, que la ausencia de la variable independiente aumenta en 4 veces la probabilidad de ocurrencia e la variable dependiente.

La tercera columna de las tablas de resultados muestra los errores estándar asociados a las estimaciones. Estos errores se utilizan para el calcular el test de significancia, mediante el cual se decide si el efecto estimado es estadísticamente significativo. Dada la naturaleza exploratoria de este estudio se ha fijado el umbral de confianza en 90%, por lo que todo valor del test de significancia menor o igual a 0.1 es considerado indicador de un efecto estimado estadísticamente significativo.

Todos los supuestos de los modelos de regresión logística binaria fueron chequeados antes de realizar los análisis multivariados aquí presentados. El más importante de estos supuestos es la ausencia de multicolinealidad entre las variables independientes (Field 2009). La presencia de multicolinealidad, esto es de una alta correlación entre las variables independientes, puede llevar a estimaciones poco fiables. Para diagnosticar la presencia de multicolinealidad en los modelos a estimar se utilizó el test de Collin para calcular los estadísticos de tolerancia y el factor de inflación de varianza (VIF) e identificar eventuales multicolinealidades entre las variables independientes. Los resultados del test permiten descartar la existencia de multicolinealidad en el los modelos estimados. Todos los otros supuestos, tales como como una variable dependiente codificada binariamente y la independencia entre observaciones se cumplen.

V. RESULTADOS

A continuación se presenta los resultados de cada uno de los modelos estimados. Primero se presentan los resultados relativos a ofensas interpersonales – amenazas y hostigamiento sexual-, enseguida los referidos a delitos tecnológicos – hacking y virus-, y finalmente los referidos a estafa y robo de identidad bancaria.

Ciber-delitos interpersonales

La tabla 1 presenta los resultados del análisis multivariado de la victimización por amenazas y hostigamiento sexual. Los resultados del análisis muestran que los hombres tienen el doble de probabilidades de ser víctimas de amenazas por internet que las mujeres y que, esta probabilidad aumenta con la edad. Las mismas variables ejercen el efecto contrario en relación al hostigamiento sexual: las mujeres tienen casi el doble de probabilidades de ser víctimas de hostigamiento sexual que los hombres y, todo lo demás constante, los más jóvenes tiene una probabilidad significativamente mayor de sufrir un incidente de este tipo que los mayores. En relación al status socioeconómico de los encuestados, los resultados no muestran variaciones relevantes ni en la probabilidad de ser víctima de amenazas ni en la probabilidad de ser víctima de hostigamiento sexual entre los distintos grupos socio-económicos.

En relación a las variables referidas a la exposición de los usuarios en el ciber-espacio, vender productos a través de internet, actividad que claramente

incrementa la exposición de los usuarios en la red, aumenta significativamente la probabilidad de ser víctima de amenazas y la probabilidad de ser víctima de hostigamiento sexual. La frecuencia con que los usuarios realizan actividades de lectura en línea también está positivamente relacionada con la victimización por hostigamiento sexual y amenazas, aun cuando en este caso los resultados e la muestra no son extrapolables a la población. Del mismo modo, la navegación libre en internet está asociada a la victimización por amenazas y hostigamiento entre quienes respondieron la encuesta, pero estos resultados no son estadísticamente extrapolables a la población.

En relación a las variables asociadas a la accesibilidad a datos personales on-line, los resultados muestran que los usuarios que comparten contenido propio en redes sociales tienen más del doble de probabilidades de ser víctimas de hostigamiento sexual, en comparación con quienes no comparten contenidos propios, y 41% más probabilidades de ser víctimas de amenazas. Asi mismo, la frecuencia con que los usuarios que reportan realizar transferencias bancarias está positivamente relacionada a la victimización por amenazas, aun cuando tal relación no es estadísticamente significativa.

Finalmente, en relación a las variables referidas a medidas preventivas, la victimización por amenazas es menor entre los encuestados que señalan nunca entregar información personal en redes sociales y entre aquellos que señalan que siempre borran sin abrir los e-mail sospechosos, pero solo esta última es extrapolable a la población, con un 30% de reducción en el riesgo de sufrir un incidente de este tipo. En relación a hostigamiento sexual, tomar la precaución de sólo agregar conocidos a las redes sociales reduce en un 40% el riesgo de victimización por este tipo de delitos.

Tabla (1): Análisis multivariado de Amenazas y Hostigamiento

	Amenazas			Hostigamiento		
	Coef.	Std. Err.	OR	Coef.	Std. Err.	OR
Exposición						
Navegación libre	0.150	0.111	1.162	0.081	0.107	1.085
Redes sociales	0.002	0.126	1.002	-0.090	0.133	0.914
Películas	-0.074	0.092	0.929	0.058	0.082	1.060
Lectura	0.148	0.098	1.160	0.217 **	0.086	1.243
Venta	0.348***	0.095	1.416	0.212 **	0.086	1.236
Teletrabajo	0.427	0.078	1.043	-0.074	0.061	0.929
Accesibilidad						
Transferencias	0.164	0.128	1.178	-0.041	0.114	0.960
Contenido propio	0.394*	0.206	1.482	0.782***	0.187	2.185
Protección						
Borra correos sospechosos	-0.353*	0.214	0.702	-0.121	0.185	0.886
Sólo agrega conocidos	0.181	0.235	1.198	-0.503***	0.179	0.605
No entrega información personal	-0.184	0.244	0.832	-0.094	0.206	0.911
Antivirus/ firewalls u otros	-0.007	0.265	0.993	0.279	0.223	1.322
Descarga actualizaciones y parch	0.084	0.185	1.088	-0.092	0.160	0.912
Características individuales						
Sexo(0=mujer, 1=hombre)	0.713 ***	0.189	2.040	-0.546***	0.181	0.579
Edad	0.190*	0.111	1.210	-0.467***	0.098	0.627
GSE	0.039	0.080	1.040	-0.002	0.072	0.998
Constante	-4.813	0.860	0.008	-1.438	0.780	0.237
-2Log-likelihood	1094.049			905.240		
Modelo X^2	139.6***			57.12***		
Nagelkerke R^2	0.08			0.16		

Nota: *p <0.1; ** p<0.05; *** p<0.01

Ciber-delitos tecnológicos

La tabla (2) muestra los resultados del modelo de regresión logística para hacking y victimización por virus o malwares. Entre los encuestados, los hombres reportan una mayor proporción de victimas por hackeo y virus que las mujeres. Sin embargo, en ninguno de los dos casos esta relación es estadísticamente significativa y, por tanto, no es extrapolable a la población. En relación a la edad, hay una relación positiva con el riesgo de ser víctima de virus: a mayor edad, mayor probabilidad de infección del dispositivo usado para conectarse a internet. El status socioeconómico de los encuestados está significativamente asociado al riesgo de infección por virus o malware, siendo este riesgo mayor entre los usuarios de los grupos socioeconómicos más bajos.

Entre las variables que miden la exposición de los usuarios en internet, leer en línea aumenta significativamente el riesgo tanto de hackeo como de virus. La venta de productos está significativamente asociada al riesgo de hackeo, y la descarga o visualización de películas está significativamente asociada al riesgo de infección por virus.

La frecuencia con que los usuarios encuestados realizan transferencias bancarias está positivamente relacionada al riesgo de hackeo. Esta relación puede ser explicada por el hecho que en gran medida el hackeo de dispositivos está motivado por el deseo de adquirir información para cometer fraudes. Las personas que hacen transferencias bancarias necesitan ingresar información de tarjetas de crédito o débito, las que es de especial interés para quienes desean acceder a información bancaria de potenciales víctimas (Leukfeldt y Yar, 2016).

En términos de factores de protección, la descarga de actualizaciones de softwares y parches está asociada a una reducción de 40% en el riesgo de victimización por hackeo. Del mismo modo, los encuestados que señalan descargar actualizaciones y parches en cuanto aparecen reportan un 15% menos prevalencia de hackeo que quienes no lo hacen, pero en este caso la relación no es estadísticamente extrapolable a la población.

Llama la atención que la prevalencia de infección por virus o malware es la misma entre quienes tienen antivirus en sus dispositivos y quienes no lo tienen. Esta aparente ineficacia de los softwares antivirus puede ser explicada por posibles problemas de endogeneidad entre la variable independiente y la independiente; en otras palabras, pudiera ser que la instalación de software

antivirus sea una respuesta a la victimización, con lo que el efecto preventivo de los mismos se vería subestimado. Otra explicación podría ser que aun cuando los usuarios tengan softwares antivirus instalados, éstos no estén actualizados y por tanto sean incapaces de proteger los equipos frentes a ataques con malware de última generación.

Tabla (2): Análisis multivariado de Hacking y Virus

	Hacking			Virus/malware		
	Coef.	Std. Err.	OR	Coef.	Std. Err.	OR
Exposición						
Navegación libre	0.114	0.121	1.121	-0.105	0.088	0.901
Redes sociales	-0.076	0.132	0.927	0.148	0.109	1.160
Peliculas	0.083	0.097	1.086	0.119 *	0.072	1.127
Lectura	0.219***	0.102	1.244	0.202**	0.084	1.224
Venta	0.253***	0.100	1.287	-0.109	0.096	0.897
Teletrabajo	-0.017	0.077	0.983	0.089	0.068	1.093
Accesibilidad						
Transferencias	0.246*	0.136	1.279	-0.015	0.108	0.985
Contenido propio	0.107	0.211	1.113	0.180	0.167	1.197
Protección						
Borra correos sospechosos	-0.295	0.224	0.745	-0.080	0.193	0.923
Sólo agrega conocidos	0.045	0.238	1.046	0.085	0.200	1.089
No entrega información personal	0.300	0.279	1.350	0.122	0.221	1.130
Antivirus/ firewalls u otros	-0.145	0.257	0.865	0.039	0.226	1.040
Descarga actualizaciones y parches	-0.508***	0.194	0.601	-0.163	0.156	0.849
Características individuales						
Sexo	0.283	0.200	1.327	0.241	0.161	1.272
Edad	0.048	0.114	1.049	0.181**	0.092	1.199
GSE	0.195**	0.087	1.215	0.246***	0.071	1.279
Constante	-4.828	0.908	0.008	-4.069	0.734	0.017
-2Log-likelihood	844.802			1173.204		
Model X^2	41.00***			30.8***		
Nagelkerke R^2	0.61			0.37		

Nota: *p <0.1; **p<0.05; ***p<0.01

Ciber-fraudes

La tabla (3) muestra que las estafas a través de internet está significativamente relacionadas al sexo de los usuarios, de modo tal que los hombres tienen un 33% menos probabilidad de ser víctimas de estafa on-line que las mujeres. Los resultados del análisis muestran, además, que la probabilidad de estafa se reduce en los grupos socioeconómicos más bajos, lo que es coherente con la idea que el atractivo, en términos de potenciales ganancias, juega un rol importante en el riesgo de victimización por este tipo de delitos. En la muestra analizada, se observa además que

la edad reduce el riesgo de victimización por estafa, sin embargo, los tests de significancia estadística no permiten extrapolar esta relación al conjunto de la población.

En relación a la victimización por robo de identidad bancaria, se observa que en la muestra analizada, al igual que lo observado en relación a estafa, los hombres y usuarios de sectores socioeconómicos más bajo reportan menos porcentajes de victimización, y que ésta disminuye con la edad. Sin embargo, sólo esta última variable es estadísticamente significativa.

Entre las variables que tratan de medir la exposición de los usuarios a potenciales delincuentes, sólo la descarga o visualización on-line de películas está significativamente relacionada al riesgo de victimización por estafa: mientras mayor la frecuencia con que se realiza esta actividad, mayor la probabilidad de ser víctima de estafa on-line[3]. Ninguna de las variables asociadas a exposición está significativamente relacionada al robo de identidad bancaria.

De las variables que miden la accesibilidad a datos personales, la frecuencia con que los usuarios realizan transferencias bancarias esta significativa y positivamente asociada tanto al riesgo de victimización por estafa como al robo de identidad bancaria, en otras palabras, realizar transferencias bancarias aumenta significativamente el riesgo para ambos tipos de delitos. Subir contenido propio a redes sociales, en cambio, no tiene relación significativa con estos delitos, aun cuando entre la muestra observada, quienes con mayor frecuencia realizan esta actividad reportan en mayor proporción haber sido víctimas de robo de identidad bancaria.

[3] Para observar mejor el efecto de esta variable en el riesgo de victimización por estafa , se estimó un modelo el que la variable “frecuencia con que descarga y mira películas on line” fue reemplazad por una variable dummy para indicar si realiza o no esta actividad. Los resultados señalan que quienes ven películas on-line tienen el doble de probabilidades de ser victimizados (B= 2.06; p-value< 0.01) que quienes nunca ven películas on-line

En relación a las medidas de protección consideradas en el análisis, borrar los e-mails sospechosos y sólo agregar conocidos a redes sociales están significativa y negativamente relacionados al riesgo de victimización por estafa. Quienes borran, sin abrir, lo e-mails sospechosos tienen un 33% menos probabilidad de ser víctimas de este delito, en comparación a quienes no toman esta medida. Del mismo modo, quienes solo agregan personas conocidas a sus redes sociales tienen un 30% menos probabilidad de ser víctimas de estafas on-line. Ninguna de las medidas de protección consideradas están significativamente relacionadas a una reducción en el riesgo de robo de identidad bancaria, aun cuando los encuestados que señalan borrar correos sospechosos y tener instalados softwares antivirus reportaron un 12% y 22% menos robos de identidad bancaria.

Tabla (3): Análisis multivariado de Estafa y Robo de Identidad Bancaria

	Estafa			Robo de ident. bancaria		
	Coef.	Std. Err.	OR	Coef.	Std. Err.	OR
Exposición						
Navegación libre	-0.134	0.108	0.874	0.159	1.240	1.173
Redes sociales	0.068	0.141	1.070	-0.147	0.156	0.863
Películas	0.184**	0.094	1.202	-0.066	0.134	0.936
Lectura	0.033	0.100	1. 034	0.104	0.144	1.110
Venta	0.127	0.102	1.135	0.031	0.154	1.032
Teletrabajo	-0.099	0.069	0.905	-0.048	0.102	0.953
Accesibilidad						
Transferencias	0.239*	0.135	1.270	0.563***	0.197	1.756
Contenido propio	0.014	0.200	1.014	0.124	0.292	1.132
Protección						
Borra correos sospechosos	-0.408*	0.216	0.665	-0.124	0.363	0.884
Sólo agrega conocidos	-0.356*	0.217	0.701	0.291	0.400	1.338
No entrega información persona	0.375	0.270	1.455	0.460	0.450	1.584
Antivirus/ firewalls u otros	0.226	0.279	1.254	-0.258	0.406	0.772
Descarga actualizaciones y parch	0.061	0.188	1.063	0.080	0.276	1.084
Características individuales						
Sexo	-0.403**	0.203	0.668	-0.073	0.280	0.929
Edad	-0.175	0.114	0.839	0.336**	0.172	1.400
GSE	-0.152*	0.081	0.859	-0.142	0.116	0.868
Constante	-2.258**	0.887	0.105	-5.761	1.285	0.003
-2Log-likelihood	884.933			483.813		
Model X^2	37.26***			29.07**		
Nagelkerke R^2	0.54			0.67		

VI. DISCUSIÓN

La victimización por ciber-delitos se ha convertido en una creciente preocupación para la ciudadanía, empresas y gobiernos debido al significativo aumento de cada vez más sofisticados delitos en el ciberespacio. Esta preocupación se acrecienta al considerar que las tendencias e impulsos (en sí deseables) a la masificación del acceso y uso de internet conllevarán nuevas oportunidades para la comisión de delitos, los que sin duda seguirán al alza.

Este artículo reporta los resultados de una investigación exploratoria respecto del riesgo de ser víctima de un ciber-delito en Chile, analizado a partir de un marco teórico bien establecido: la teoría de actividades rutinarias. Específicamente, el presente estudio testeó la aplicabilidad de tres elementos claves de este marco teórico en la explicación del riesgo de ser víctima de un ciber-delito en Chile: exposición, accesibilidad y protección. Los resultados del estudio sugieren que la victimización por los ciber-delitos considerados es función de la oportunidades para la comisión de delitos que ofrece la interacción on-line, oportunidades que en cierto grado son facilitadas por las actividades on-line que día a día son desarrolladas por las personas.

Los resultados sugieren que variables relacionadas a la exposición on-line de las personas están significativamente relacionadas a 5 de los 6 tipos de ciber-delitos considerados; siendo la excepción el robo o suplantación de identidad bancaria, que pareciera no estar afectado por la exposición de los sujetos, al menos tal y como aquí fue medida. Los resultados sugieren además que distintas actividades en internet afectan de distinto modo la probabilidad de ser víctima de cada ciber-delito en particular. De este modo, se encontró que descargar o ver películas on-line está significativamente asociado al riesgo de ser víctima de estafa e infección por malware. En la misma línea, quienes dedican más tiempo a leer on-line tienen significativamente más probabilidad de ser víctimas de hostigamiento sexual, hackeo e infección por malware. Adicionalmente, la mayor exposición derivada de la venta de productos por Internet está significativamente asociada a un aumento en la probabilidad de ser víctima de amenazas, hostigamiento sexual y hackeo. Otras variables relacionadas al grado de exposición on-line, tales como navegación libre en internet y el teletrabajo, no muestran evidencia significativa de estar relacionadas con la probabilidad de ser víctima de alguno de los ciber-delitos considerados.

La frecuencia del uso de redes sociales en sí pareciera no estar asociada al riesgo de ciber-victimización, sino que es el tipo de participación en ellas lo que importa. En efecto, compartir información en reses sociales mediante la publicación de contenido propio está significativamente correlacionado a un incremento en la probabilidad de ser víctima de amenazas y hostigamiento sexual.

Del mismo modo, compartir información personal mediante la realización de transferencias monetarias on-line está significativamente asociado al riesgo de victimización por hacking, estafa y robo de identidad bancaria. En relación a este último delito, la realización de transferencias on-line es la única actividad significativamente asociada a la victimización por robo de identidad bancaria, de modo que quienes más habitualmente realizan transferencias on-line tienen un 75% más probabilidad de ser víctimas de este delito que quienes realizan transferencias menos frecuentemente.

Desde la perspectiva de la teoría de las actividades rutinarias se espera que aquellos usuarios que han adoptado medidas de protección tengan menor riesgo de ser víctima de ciber-delitos. Los resultados de los análisis realizados en esta investigación que algunas medidas de protección funcionan para tipos específicos de ciber-delitos. Borrar correos sospechosos está significativamente asociado a una reducción en el riesgo de amenazas y estafas. Igualmente, la práctica de sólo agregar personas conocidas a redes sociales se correlaciona significativamente a una reducción en el riesgo de estafa y hostigamiento sexual on-line. Como era esperable, descargar actualizaciones y parches de softwares está significativamente asociado a una reducción en la probabilidad de ser víctima de hackeo: quienes habitualmente descargan las actualizaciones de software tienen un 40% menos probabilidad de ser víctimas de este delito en comparación con quienes señalan no tener esta práctica incorporada a sus rutinas. Al igual que otros estudios (Holt y Bossler 2013; Ngo and Paternoster 2011; Reyns et al. 2016; Williams 2015; Akdemir y Lawless 2020), los resultados de este estudio sugieren que los softwares anti-virus no tienen el efecto preventivo esperado: en ninguno de los modelos estimados se observa relación significativa entre disponibilidad de antivirus y ciber-victimización. Una explicación posible de este resultado contra-intuitivo es el diseño metodológico de este estudio, en el sentido que su naturaleza transversal no permite distinguir si el antivirus fue instalado antes o después de la victimización, o que la prevalencia de este tipo de softwares es tan alta entre los usuarios que no permite distinguir entre

víctimas y no víctimas. Sin embargo, no es posible descartar que los softwares antivirus utilizados sean ineficientes para detectar y prevenir nuevos malwares desarrollados a una velocidad mayor que los desarrollos de la industria respectiva.

Finalmente, los resultados muestran que las variables de control consideradas en los modelos se comportan más o menos de la manera esperada. El sexo del usuario es una variable significativa en relación a la probabilidad de tres tipos de ciber-delitos. Los hombres tienen 2 veces más probabilidad de ser víctimas de amenazas que las mujeres, mientras que éstas tienen un 72% más probabilidades de ser víctimas de hostigamiento sexual y un 49% más probabilidad de ser víctimas de estafa. La edad de los encuestados está diferencialmente asociada a la mayoría de los ciber-delitos considerados. A mayor edad, mayor la probabilidad de ser víctima de robo de

identidad bancaria, amenazas e infección por malware. Como contrapartida, los más jóvenes tienen significativamente mayor probabilidad de ser víctimas de hostigamiento sexual. En relación al grupo socio-económico de los usuarios, los resultados sugieren que los grupos más adinerados tienen significativamente menor probabilidad de ser víctima de hackeo e infección por malwares, y mayor probabilidad de ser víctimas de estafa. Es posible que la explicación a estos hallazgos esté dada por la mayor capacidad de estos grupos para adquirir softwares antivirus de mejor calidad, y por otra parte, por el mayor atractivo que tienen en tanto potenciales targets de estafas on-line.

VII. CONCLUSIONES

En conjunto, los resultados anteriormente discutidos evidencian que el riesgo de ser víctima de un ciber-delito no se distribuye aleatoriamente entre los usuarios de Internet. Existen patrones de concentración que implican una mayor probabilidad de victimización para unos grupos en comparación con otros. El análisis presentado muestra que existen variables asociadas a la exposición, accesibilidad y protección de los usuarios en Internet que están significativamente correlacionadas al riesgo de ciber-victimización. De este modo, perfiles de usos o actividades habituales desplegadas on-line, así como prácticas de autoprotección y/o prevención, contribuyen significativamente a incrementar o reducir el riesgo de ciber-victimización. Adicionalmente, los resultados muestran que el efecto de estas variables sobre el riesgo de victimización no es homogéneo entre las distintas categorías de ciber-delitos, resaltando la importancia de un análisis específico para cada ciber-delito.

En términos prácticos, los resultados de este estudio contribuyen a la generación de conocimiento base para el diseño de políticas e iniciativas de prevención. La identificación de factores y prácticas on-line que facilitan o previenen la ciber-victimización es un elemento central para la definición del qué, a quién y cómo de las políticas de prevención de la ciber-victimización. Estas políticas para ser efectivas deben ser pertinentes a los riesgos que distintos perfiles de usuarios tienen, por lo que la identificación de la relación entre el riesgo de victimización y las distintas prácticas y usos de internet por parte de la población resulta ser un elemento relevante en la focalización de iniciativas preventivas y estrategias comunicacionales y/o educativas.

Sin perjuicio de la contribución de este estudio a la literatura sobre ciber-criminalidad en Chile, los resultados deben ser analizados con precaución en tanto son producto de una investigación exploratoria no exenta de limitaciones. En primer lugar, la muestra analizada no es estrictamente una muestra aleatoria por cuanto no fue obtenida de un universo muestral previamente conocido, sino que se obtuvo a partir de respuestas espontáneas a correos enviados masivamente a una base de direcciones construida ad-hoc. Si bien esta limitación no afecta el objetivo del estudio –analizar la relación entre variables- sí afecta la representatividad de los distintos grupos en la muestra y por tanto la posibilidad de inferir parámetros poblacionales no sesgados, tales como la prevalencia o porcentaje de usuarios de internet que ha sido víctima de un

ciber-delito en Chile. Futuras investigaciones deberán abordar la dificultad de construir muestras aleatorias de usuarios de internet y evaluar las ventajas y desventajas de las encuestas on-line versus las encuestas presenciales para medir ciber-victimización y variables asociadas.

Una segunda limitación de este estudio es la naturaleza transversal de los datos analizados, vale decir, el hecho que sean mediciones en un momento específico. Esta característica de los datos analizados puede ser problemática en la medida que puede conducir a problemas de especificación de la relación entre dos variables, por ejemplo uso de antivirus y victimización por hacking. En otras palabras, así como el uso de antivirus puede afectar la probabilidad de ser víctima de hackeo, también la victimización por hackeo puede afectar la probabilidad de que alguien instale un software antivirus. Los datos transversales siempre corren el riesgo de sesgar las estimaciones debido a este problema de endogeneidad de algunas variables, por lo que futuras investigaciones en esta línea debieran considerar la incorporación de la dimensión temporal, sobre todo en la medición de medidas de protección on-line.

Finalmente, si bien este estudio contribuye a identificar algunas prácticas on-line y factores asociadas al riesgo de ciber-victimización, es claro que mucha más investigación es requerida para desarrollar una cabal comprensión del ciber-delito y las medidas eficaces para prevenirlo. El ciber-crimen no es solo un asunto de tecnologías y conocimiento informático; en la medida que el comportamiento humano juega un rol central en la facilitación de este tipo de eventos (Cox y Fox 2011; Evans et. al. 2016), la comprensión del comportamiento on-line y de las prácticas cotidianas que los sujetos despliegan en Internet así como de su relación con el riesgo de victimización, juegan un rol central para la prevención de delitos en el ciber-espacio. En Chile, y Latinoamérica en general, el conocimiento a este respecto es aún incipiente por lo que la investigación multidisciplinaria en este ámbito debiera ser potenciada.

VIII. BIBLIOGRAFÍA

Akdemir, N. and Lawless, C.J. (2020), "Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach", ***Internet Research***, Vol. 30 No. 6, pp. 1665-1687

Bergmann, M.C., Dreißigacker, A., Von Skarczinski, B. and Wollinger, G.R. (2018), "Cyber-dependent crime victimization: the same risk for everyone?", ***Cyberpsychology, Behavior, and Social Networking***, Vol. 21 No. 2, pp. 84-90

Bossler, A.M. and Holt.J. (2009). "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory". ***International Journal of Cyber Criminology*** 3(1) pp 400-420.

Caneppele, S. y Aebi, M. (2019). "Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes", ***Policing: A Journal of Policy and Practice***, Volume 13, Issue 1, March 2019, Pages 66–79.

Choi, K.-S., Choo, K. and Sung, Y.-E. (2016), "Demographic variables and risk factors in computercrime: an empirical assessment", ***Cluster Computing***, Vol. 19 No. 1, pp. 369-377.

Choi, K.S. (2008). "Computer Crime Victimization and Integrated Theory: An Empirical Assessment". ***International Journal of Cyber Criminology*** 2(1), pp 308-333.

Cohen, L.E. and Felson, M. (1979), "Social change and crime rate trends: a routine activity approach", ***American Sociological Review***, Vol. 44 No. 4, pp. 588-608.

Cook, C.L. and Fox, K.A. (2011), "Fear of property crime: examining the effects of victimization, vicarious victimization, and perceived risk", ***Violence Victims and Offenders***, Vol. 26 No. 5,pp. 684-700.

Evans, M., Maglaras, L.A., He, Y. and Janicke, H. (2016), "Human behaviour as an aspect of cybersecurity assurance", Security and Communication Networks, Vol. 9 No. 17, pp. 4667-4679 Field, A. (2009), ***Discovering Statistics Using SPSS***, Sage Publications, London.Evans et. al. 2016

Felson, M. (2002). ***Crime and everyday life***. Sage.

Grabosky, P.N. (2001), "Virtual criminality: old wine in new bottles?", ***Social and Legal Studies***, Vol. 10 No. 2, pp. 243-250.

Holt, T.J. and Bossler, A.M. (2008), "Examining the Applicability of Lifestyle Routine Activities Theory for Crybercrime Victimization", ***Deviant Behavior*** , 30:1, 1-25

Holt, T.J. and Bossler, A.M. (2013), "Examining the relationship between routine activities and malware infection indicators", Journal of Contemporary Criminal Justice, Vol. 29 No. 4,pp. 420-436.

Holt, T. J., Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35, 20–40.

Holt, T.J. and Copes, H. (2010), "Transferring subcultural knowledge on-line: practices and beliefs of persistent digital pirates", ***Deviant Behavior***, Vol. 31 No. 7, pp. 625-654

Holt, T.J., Van Wilsem, J., Van De Weijer, S. and Leukfeldt, R. (2018), "Testing an integrated selfcontrol and routine activities framework to examine malware infection victimization", ***Social Science Computer Review***, Vol. 38 No. 2, pp. 187-206.

Holtfreter, K., Reising, M.D. and Pratt, T.C. (2008), Low Self-Control, Routine Activities, and Fraud Victimization. ***Criminology***, 46: 189-220.

Jansen, J. and Leukfeldt, R. (2015), "How people help fraudsters steal their money: an analysis of 600 online banking fraud cases", in Bella, G. and Lenzini, G. (Eds), 2015 ***Workshop on Socio-Technical Aspects in Security and Trust Workshop***, IEEE, Verona, pp. 24-31.

Koops, B.J. (2010), "The internet and its opportunities for cybercrime", ***Transnational Criminology Manual***, Vol. 1 No. 1, pp. 735-754.

Leukfeldt, E. (2015), "Comparing victims of phishing and malware attacks", ***International Journal of Advanced Studies in Computer Science and Engineering,*** Vol. 4 No. 5, pp. 26-32.

Leukfeldt, E.R. and Yar, M. (2016), "***Applying routine activity theory to cybercrime: a theoretical and empirical analysis***", Deviant Behavior, Vol. 37 No. 3, pp. 263-280.

Levi, M. (2017), "Assessing the trends, scale and nature of economic cybercrimes: overview and issues", ***Crime, Law and Social Change***, Vol. 67 No. 1, pp. 3-20.

Marcum, C.D., Higgins, G.E. and Ricketts, M.L. (2010), "Potential factors of online victimization of youth: an examination of adolescent online behaviors utilizing routine activity theory", ***Deviant Behavior***, Vol. 31 No. 5, pp. 381-410.

Ngo F., Piquero AR, LaPrade J, Duong B. (2020) Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online? Criminal Justice Review., 5(4):430-451.

Ngo, F. and Paternoster, R. (2011), "Cybercrime victimization: an examination of individual and situational level factors", ***International Journal of Cyber Criminology***, Vol. 5 No. 1, pp. 773-793.

Paek, S.Y. and Nalla, M.K. (2015), "The relationship between receiving phishing attempt and identity theft victimization in South Korea", ***International Journal of Law, Crime and Justice***, Vol. 43 No. 4, pp. 626-642.

Pratt, T., Holtfreter, K. and Reisig, M. (2010), "Routine online activity and internet fraud targeting: extending the generality of routine activity theory", ***The Journal of Research in Crime and Delinquency***, Vol. 47 No. 3, p. 267.

Reyns, B.W. (2015), "A routine activity perspective on online victimization: results from the Canadian general social survey", ***Journal of Financial Crime***, Vol. 22 No. 4, pp. 396-411.

Reyns, B.W., Henson, B., Fisher, B.S., Fox, K.A. and Nobles, M.R. (2016), "A gendered lifestyle-routine activity approach to explaining stalking victimization in Canada", ***Journal of Interpersonal Violence***, Vol. 31 No. 9, pp. 1719-1743.

Reyns, B. W., Henson, B., Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. ***Journal of Contemporary Criminal Justice***, 32, 148–168.

Reyns, B. W., Henson, B., Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. ***Criminal Justice and Behavior***, 38, 1149–1169.

Rodriguez, J.A., Oduber, J. y Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. URVIO, Revista Latinoamericana de Estudios en Seguridad, No. 20, pp 63-79

Symantec. (2019), "Internet security threat report", disponible en: https://www-west.symantec.com/ content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Subtel 2017

Vakhitova, Z.I., Reynald, D.M. and Townsley, M. (2015), "Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization", ***Journal of Contemporary Criminal Justice***, Vol. 32 No. 2, pp. 169-188.

Van Wilsem, J. (2013b), "Hacking and harassment—do they have something in common? Comparing risk factors for online victimization". ***Journal of Contemporary Criminal Justice***, Vol. 29 No. 4, pp. 437-453.

Wall, D.S. (2007), Cybercrime: ***The Transformation of Crime in the Information Age***, Polity, London.Williams 2015

Yar, M. (2005). The novelty of "cybercrime": an assessment in light of routine activity theory. ***European Journal of Criminology***, 2, 407–427.


CENTRO DE
ESTUDIOS
DEL FUTURO
UNIVERSIDAD DE SANTIAGO DE CHILE