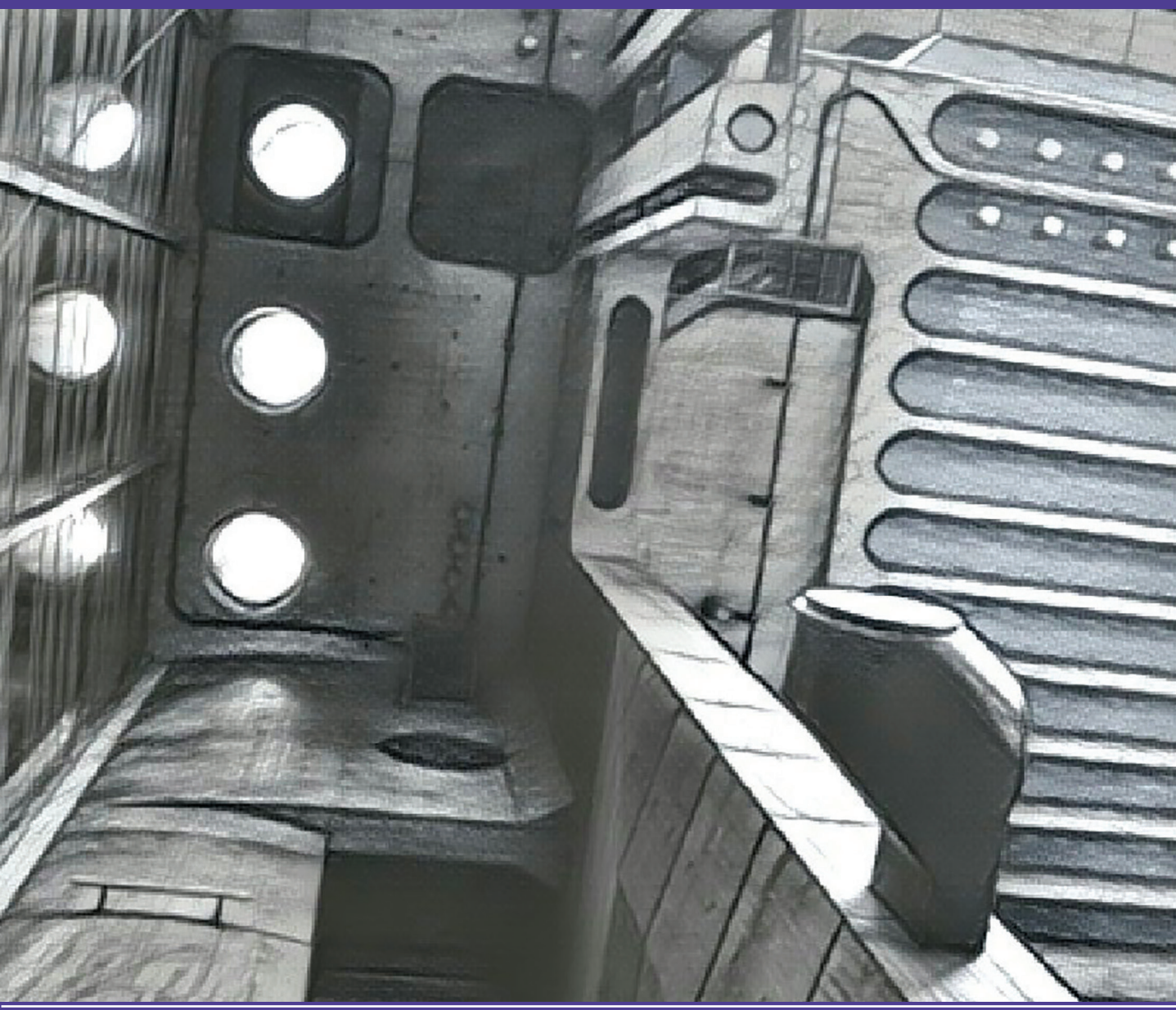
ISSN: 1390-4299
1390-3691

No. 20

URVIO

Revista Latinoamericana de Estudios de Seguridad



Ciberseguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
FLACSO Sede Ecuador • Junio 2017

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

URVIO está incluida en los siguientes índices, bases de datos y catálogos:

- Emerging Sources Citation Index (ESCI). Índice del Master Journal List de Thomson Reuters.
- ERIH PLUS, European Reference Index for the Humanities and the Social Sciences. Índice de referencias.
- JournalTOCS. Base de datos.
- Directory of Research Journals Indexing (DRJI). Directorio.
- Actualidad Iberoamericana. Índice internacional de revistas.
- CLASE, Citas Latinoamericanas en Ciencias Sociales y Humanidades. Base de datos bibliográfica.
- Directorio LATINDEX, Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal.
- DIALNET, Universidad de La Rioja. Plataforma de recursos y servicios documentales.
- EBSCO. Base de datos de investigación.
- FLACSO-ANDES, Centro digital de vanguardia para la investigación en ciencias sociales - Región Andina y América Latina - FLACSO, Ecuador. Plataforma y repositorio.
- REDIB, Red Iberoamericana de Innovación y Conocimiento Científico. Plataforma.
- MIAR (Matriz de Información para el Análisis de Revistas). Base de datos.
- LatAm Studies. Estudios Latinoamericanos. Base de datos.
- Google académico. Buscador especializado en documentación académica y científica.

FLACSO ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

URVIO, **Revista Latinoamericana de Estudios de Seguridad**
Número 19, diciembre de 2016
Quito - Ecuador

ISSN 1390-4299 (en línea) y 1390-3691

URVIO, Revista Latinoamericana de Estudios de Seguridad, es una publicación electrónica semestral de FLACSO, sede Ecuador, fundada en el año 2007. La revista constituye un espacio para la reflexión crítica, el debate, la actualización de conocimientos, la investigación y la consulta sobre temas vinculados con la seguridad, el delito organizado, la inteligencia y las políticas públicas sobre seguridad en la región.

Disponible en:
http://revistas.flacsoandes.edu.ec/index.php/URVIO
http://www.flacsoandes.org/urvio/principal.php?idtipocontenido=13

El Comité Editorial de URVIO decidirá la publicación o no de los trabajos recibidos, sobre los cuales no se comprometerá a mantener correspondencia. Los artículos serán sometidos a la evaluación de expertos mediante el sistema de doble ciego. Las opiniones y comentarios expuestos en los trabajos son de responsabilidad estricta de sus autoras y autores, y no reflejan la línea de pensamiento de FLACSO, sede Ecuador. Los artículos publicados en URVIO son propiedad exclusiva de FLACSO, sede Ecuador. Se autoriza la reproducción total o parcial de los contenidos siempre que se cite como fuente a URVIO, Revista Latinoamericana de Estudios de Seguridad.

Envío de artículos
revistaurvio@flacso.org.ec

FLACSO, sede Ecuador
Casilla: 17-11-06362
Dirección: Calle Pradera E7-174 y Av. Diego de Almagro. Quito, Ecuador
www.flacso.edu.ec
Telf.: (593-2) 294 6800 Fax: (593-2) 294 6803

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

Tema central

Misceláneo

Entrevista

Reseñas

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

Central topic

Miscellaneous

Interview

Books reviews

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2583

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 63-79
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Actividades rutinarias y cibervictimización en Venezuela

Routine activities and cyber-victimization in Venezuela

Juan Antonio Rodríguez[1], Jesús Oduber[2] y Endira Mora[3]

Fecha de recepción: 14 de febrero de 2017
Fecha de aceptación: 3 de abril de 2017

Resumen

El ciberdelito ha aumentado significativamente a nivel mundial en estas últimas décadas. En tal sentido, la investigación sobre este fenómeno en Venezuela ha sido escasa, específicamente en lo que respecta a los factores asociados con la victimización en línea. En consecuencia, este estudio busca promover el análisis de los condicionantes del delito y la victimización en línea en la región. Para ello, se investiga un conjunto de variables derivadas de la *Teoría de las actividades rutinarias*. El propósito es observar su relación con la victimización por *hackeo* y acoso *online* en una muestra de 308 sujetos. Este estudio halló un grupo de variables que pueden estar relacionadas con la probabilidad de victimización cibernética, las cuales serán discutidas en términos empíricos, teóricos y prácticos.

Palabras clave: victimización; *hacking*; acoso en línea; actividades rutinarias; Venezuela.

Abstract

Cybercrime has significantly increased worldwide in the last decades. There has been very little research done regarding cybercrimes in Venezuela in comparison to other places, more specifically in regards to the factors related to online victimization. Thus, this study aims to encourage the analysis on the factors of crime and online victimization in the region. Therefore, a group of variables derived from the routine activity theory (Cohen and Felson 1979), is analyzed. The purpose is to observe its relation to hacking and online harassment in a sample of 308 individuals. This study found a group of variables that could be related to the likelihood of cyber victimization, which will be discussed in empirical, theoretical and practical terms.

Keywords: victimization; hacking; online harassment; routine activity; Venezuela.

1 Criminólogo y Doctor en Psicología Social por la Universidad de Santiago de Compostela (España). Profesor asociado y ex-director de la Escuela de Criminología de la Universidad de Los Andes (Venezuela). Investigador (adscrito al GIC y CENIPEC) acreditado por el ONCTI y el CDCHTA-ULA (Venezuela). Correo: jarodrig@ula.ve.

2 Criminólogo y abogado. Docente e investigador de la Escuela de Criminología de la Universidad de Los Andes (Venezuela). Correo: jesusoduber@hotmail.com.

3 Criminóloga, abogada y MSc. en Orientación de la Conducta. Maestrante de Derecho Procesal Penal y de Gestión Empresarial. Consultora jurídica e investigadora en Derecho Informático del CENDITEL. Correo: endiramorarojas@gmail.com.

Introducción

En las dos últimas décadas, el uso de internet se ha incrementado de manera sostenida en Latinoamérica. Cifras de la Comisión Económica para América Latina y el Caribe (CEPAL) señalan que el porcentaje de usuarios creció casi un 11% de forma interanual en el periodo 2000-2015 (CEPAL 2016). Esta Comisión, al igual que otros organismos como el Banco Interamericano de Desarrollo (BID 2016), afirma que alrededor del 55% de la población total de Latinoamérica y el Caribe utilizó en mayor o menor medida internet en el 2015. No hay duda de que las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un medio fundamental tanto para el desarrollo de actividades comerciales y económicas como para el crecimiento de relaciones sociales en la región. Sin embargo, este mismo desarrollo tecnológico también ha subvertido la seguridad favoreciendo el aumento de nuevas oportunidades para la comisión de viejos delitos (pero ahora basados en modernos sistemas de información y comunicación) y la eclosión de formas muy novedosas de transgresión inmanentes al ciberespacio.

Los informes de organismos internacionales y empresas vinculadas a la seguridad informática reseñan un importante incremento de ataques cibernéticos contra personas físicas, corporaciones y gobiernos de Latinoamérica y el Caribe en el último quinquenio (BID 2016; ESET 2016; Kaspersky 2016; OEA 2013; Symantec 2014a), lo que significa para las finanzas de la zona cerca de 90.000 millones de dólares anuales (BID 2016). Los ciberdelitos con mayor ocurrencia (o al menos los más destacados en los informes de entidades públicas y privadas) son el acceso ilegal a datos (*hacking*) y la violación de la privacidad o confidencialidad, los cuales se encuentran muy relacionados a ataques con *malware* (ESET 2016; OEA 2013; Symantec 2014a).

Al respecto, Kaspersky Lab registró más de 398 millones de ciberataques con *malware* en América Latina durante los años 2015 y 2016, facilitados en parte por la navegación, la descarga de archivos y el ingreso a correos electrónicos fraudulentos o con adjuntos contaminados (Kaspersky 2016). En este sentido, el *crimeware* es otro caso característico de la ciberdelincuencia local. Los *hackers,* apoyados en técnicas como el *spamming* o *pharming,* buscan robar identidades, credenciales y datos financieros para ingresar en cuentas de banco *online* y substraer los fondos disponibles o para interceptar información de tarjetas de crédito y venderla en el mercado. Este tipo de amenazas bancarias basadas en navegadores son usuales en Latinoamérica, pero también han surgido nuevas modalidades como el ataque a dispositivos móviles para interceptar los mensajes de texto (SMS) enviados del banco a la víctima o los ataques con *malware* dirigido a cajeros automáticos (Symantec 2014a).

En Venezuela, las actividades ilegales vinculadas al ciberespacio presentan un patrón muy similar al resto de los países de América Latina y el Caribe. La empresa Symantec (2014b) destaca que el 4,2% de los ataques cibernéticos de la región ocurrieron desde este país en el 2013. Simultáneamente, Venezuela tuvo una tasa de infección por *malware* del 23.13% del total de computadoras analizadas por PandaLabs en ese mismo año (Symantec 2014a). Y además, se ubicó entre los 10 países de esta parte del continente más afectados por el *spear phishing* al sufrir el 5% del total de ataques registrados para Latinoamérica y el Caribe. En el caso concreto de las empresas, el laboratorio de investigación de ESET (2016)

conoció y desmanteló una campaña de propagación e infección de *malware* denominada *Operación Liberpy* en el año 2015. Esta *botnet* se dedicaba expresamente al robo de información de los usuarios. Este mismo reporte señala que 13% de las empresas en Venezuela fueron víctimas de *phishing* en ese mismo periodo.

En vista de este escenario, los organismos gubernamentales de Venezuela y del resto de América Latina han buscado fórmulas para contrarrestar la ciberdelincuencia, lográndose avances sustantivos en el mejoramiento de las capacidades tecnológicas, las políticas de prevención y, en especial, la sanción de leyes contra este tipo de delito[4] (Symantec 2014a; BID 2016). Ahora bien, estos intentos de prevenir y controlar dicho fenómeno son valiosos, pero para que ello tenga una mayor efectividad hay que conocer qué factores están relacionados al mismo. Sobre la base de lo anterior, se debe precisar que hasta el momento se ha desarrollado muy poca investigación sistemática tanto cuantitativa como cualitativa sobre el ciberdelito en Venezuela y el resto de los países de Latinoamérica. De aquí la imperiosa necesidad de dedicar mayor interés a su definición y clasificación, los niveles de perpetración/victimización, los predictores (individuales y ambientales) asociados a estos y los marcos explicativos plausibles para comprender este objeto de estudio a nivel local.

En este sentido, la presente investigación, por sus características, no tiene como finalidad analizar la prevalencia e incidencia de la victimización cibernética en una población determinada. Más bien constituye un análisis cuantitativo que permite mejorar la comprensión de los factores de riesgo y protección inherentes al uso de las TIC, los cuales pueden hacer a alguien vulnerable (o no) a un delito informático. Tomando en cuenta el apoyo alcanzado para este tipo de análisis, se ha decidido utilizar los conceptos y predictores enmarcados en la *Teoría de las actividades rutinarias* (en adelante TAR) propuesta por Cohen y Felson a finales de los años setenta. Un teoría que según Wikström y Treiber (2016) puede considerarse más como un modelo predictivo con el que se consigue definir dónde y cuándo es más probable que ocurra un delito. Así, el objetivo principal de este estudio es contrastar algunos predictores del *hackeo* y el acoso cibernético (*online harassment*) con la aplicación de medidas derivadas de la TAR en una muestra de estudiantes universitarios de Venezuela.

Cibervictimización y actividades rutinarias: desarrollos teóricos y empíricos

La victimización en línea se ha estudiado fundamentalmente en los países desarrollados en las dos últimas décadas. Con el propósito de recopilar información, evaluarla y, luego, tratar de predecir y explicar los delitos relacionados con las TIC, algunos trabajos se han dedicado a analizar el significado y la naturaleza

4 Venezuela cuenta con un marco legislativo que regula el ámbito informático conformado por la Constitución de la República Bolivariana de Venezuela del año 1999, el Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas del año 2001, la Ley de Interoperabilidad del año 2012, la Ley Orgánica de Telecomunicaciones del año 2014, la Ley de Infogobierno del año 2013 y la Ley Especial contra los Delitos Informáticos del año 2001. Se debe destacar que esta última Ley es la que regula las sanciones penales en la materia. En el ámbito institucional los cuatro organismos encargadas del control de los delitos informáticos en este país son: el Sistema Nacional de Gestión de Incidentes Telemáticos (VenCert), el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), el Centro Nacional de Informática Forense (CENIF) y la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) (BID 2016; Symantec 2014a).

de múltiples formas de ciberdelitos. Al punto que, en un marco de visibles desacuerdos, los expertos en el tema han propuesto diferentes definiciones de lo que puede entenderse por delito informático y creado a partir de ellas algunas tipologías (Gordon y Ford 2006; Wall 2005; Yar 2006). Por ejemplo, Gordon y Ford (2006, 14) definen el delito informático como "cualquier delito que es facilitado o cometido usando una computadora, red, o dispositivo hardware".

Sobre la base de esta definición, clasifican el ciberdelito en *tipo I,* que es básicamente de naturaleza tecnológica y *tipo II,* que tiene un componente humano más acentuado. Son delitos propios de la primera categoría, entre otros, el *phishing*, el *hacking*, el *ransomware,* el robo de identidad, los fraudes bancarios o de comercio *online* mediante información robada y los ataques de denegación de servicio (*DoS* y *DDos*). Por su parte, el acoso en línea (*online harassment, cyberbullying, cyberstalking*), el *gromming*, la pornografía infantil y el ciberterrorismo son ejemplos de la segunda categoría. En el presente estudio se analizan dos ciberdelitos enmarcados en cada una de estas tipologías, ellos son el *hacking* y el acoso en línea (*online harassment*). Ambas formas de victimización han sido analizadas empíricamente en la Criminología de países como Estados Unidos y España a la luz de la TAR pero nunca en algún país de Latinoamérica.

Citado más de 6850 veces en las últimas cuatro décadas (Google Scholar 2017), el artículo de Cohen y Felson (1979) titulado *Social change and crime rate trends: a routine activity approach* introduce las ideas centrales de la TAR. Para Cohen y Felson la probabilidad de que ocurra un delito es el resultado de una ecuación que incluye tres variables interdependientes: un delincuente motivado (capaz de perpetrar un delito), un objetivo/víctima adecuado[5] y un guardián eficaz (cuya presencia disuada el delito y su ausencia lo facilite). Concretamente, estos autores predicen que las oportunidades delictivas se dan cuando convergen estos tres elementos en un momento y lugar determinado. Según este enfoque, sin una oportunidad en estos términos es mucho menos probable que suceda el delito; por ello, la oportunidad constituye la causa principal de la victimización delictiva.

Ahora bien, la noción de actividades rutinarias hace referencia a modos de vida que constituyen patrones regulares en la sociedad, los cuales están relacionados con la familia, el trabajo o el entretenimiento y buscan satisfacer necesidades individuales y colectivas. La TAR sostiene que la organización social moderna, afectada por la evolución tecnológica, determina en cierta medida los estilos de vida, hábitos y actividades diarias de las personas, hasta el punto de que puede tener una influencia en las oportunidades que promueven el delito. La evolución tecnológica y social ha significado un aumento de nuevos espacios de oportunidad delictiva porque incrementa la convergencia de un posible delincuente motivado, un objetivo idóneo y la ausencia de un guardián eficaz (Cohen y Felson 1979).

A simple vista, las TIC son un buen ejemplo de transformación tecnológica que han tenido una incidencia importante en el día a día de la sociedad contemporánea. Por esta razón, no es un error suponer que las oportunidades delictivas en torno a las TIC han aumentado por los cambios de las actividades rutinarias modernas y que las personas actúan en respuesta a estas oportunidades. Probablemente,

5 Un objetivo será más o menos adecuado dependiendo de cómo un delincuente lo perciba en función de su valor, inercia, visibilidad y accesibilidad (Cohen y Felson 1979).

teniendo esto en mente, un número creciente de estudios teórico-empíricos ha analizado los correlatos de la victimización *online* usando como marco de referencia la TAR (Bossler y Holt 2009; Bossler, Holt y May 2013; Choi 2008; Holt y Bossler 2009; Leukfeldt y Yar 2016; Marcum, Higgins y Ricketts 2010; Miró 2013; Ngo y Paternoster 2011; Reyns, Henson y Fisher 2011; Tillyer y Eck 2009; Yar 2005).

Las primeras discusiones teóricas se centraron en si las predicciones y explicaciones formuladas por Cohen y Felson, pensando en rutinas y circunstancias muy particulares del mundo físico, como el momento y lugar, son válidas para analizar la victimización por delitos cibernéticos (Eck y Clarke 2003; Grabosky 2001; McGuaire 2007; Miró 2011; Tillyer y Eck 2009; Yar 2005). En el marco de este debate, varios investigadores se han mostrado más o menos de acuerdo con la adaptación de los conceptos originales de la TAR al ciberespacio (Miró 2011 y Yar 2005). Algunos reconocen conceptual y analíticamente cierta correspondencia entre el contexto físico y el contexto virtual donde se pueden manifestar los tres elementos clave de la teoría (delincuente motivado, objetivo adecuado y ausencia de un guardián capaz). Por ejemplo, para estos investigadores una persona puede ser igualmente un *blanco adecuado* si enseña dinero en una taquilla de pago o si ofrece información en *Facebook* sobre el banco donde lo ahorra y un antivirus puede ser un *guardián* tan *capaz* como el vigilante de seguridad que cuida la tienda donde se vende este tipo de *software*. En definitiva, algunos autores sostienen en apoyo a la TAR que la organización del hecho delictivo es equivalente en escenarios físicos y virtuales y, en consecuencia, la cibervictimización puede ser tratada apropiadamente a la luz de la propuesta de Cohen y Felson (Yar 2005).

A la par de este valioso debate, varios estudios han intentado probar empíricamente la TAR en el contexto cibernético analizando muestras de estudiantes universitarios. Por ejemplo, Choi (2008) encontró a favor de esta teoría que los *estilos de vida en línea* imprudentes (como, por ejemplo, abrir adjuntos y enlaces web enviados por correos electrónicos desconocidos o ingresar en mensajes *pop-up*) aumentan la probabilidad de victimización por infección de virus. Y, al contrario, disponer de un *guardián digital* (programas antivirus, antispyware y firewall), disminuye tal probabilidad. En esta misma dirección, Marcum *et al.* (2010) también hallaron cierta evidencia a favor de las predicciones de Cohen y Felson.

En concreto, algunas prácticas *online* que hacen más probable la exposición a delincuentes motivados (uso de correo electrónico, mensajería instantánea, salas de chat y redes sociales) y la idoneidad del objetivo (información personal compartida en redes sociales) se relacionaron con la victimización por exposición a material sexual, acoso (no sexual) y proposición sexual no deseados. Sin embargo, las medidas de protección tecnológicas (uso de *software* de bloqueo) no evitaron este tipo de victimización; aunque, sí lo hicieron otras tácticas como el monitoreo de terceros y los controles parentales.

Otro grupo de investigaciones han encontrado poco o ningún apoyo empírico a la TAR en este tipo de muestras. En su estudio, por ejemplo, Bossler y Holt (2009) concluyen que las compras u operaciones en banca por internet y la vigilancia eficaz operacionalizada como habilidades informáticas y uso de antivirus no tienen una relación con el robo de datos por infección de *malware*. En otra inves-

tigación publicada ese mismo año, estos autores reportan que el acoso en línea (*harassment*) no tiene ninguna correspondencia con la mayoría de los indicadores de la TAR, especialmente con programas de seguridad y con rutinas como el tiempo conectado a internet, uso de correo electrónico y compras en línea. Reyns *et al.* (2011) analizaron el acoso *online* persistente (*cyberstalking*) y determinaron que los indicadores de exposición en línea no presentaron ninguna asociación significativa con este tipo de ciberdelito.

Solo la variable *agregar a personas desconocidas* se relacionó con este modo de hostigamiento. Con respecto a los indicadores de vigilancia, la medida de rastreo de perfil, al contrario de lo esperado, aumentó el riesgo de victimización. Finalmente, Ngo y Paternoster (2011) analizaron la capacidad predictiva de la TAR en un grupo amplio de formas de victimizaciones *online* (*harassment* por parte de extraños y conocidos, infección por virus, *phishing*, pornografía no deseada, solicitud de sexo y difamación) pero sus resultados tampoco consiguieron brindarle respaldo empírico a la teoría; incluso, en la mayoría de los casos se observaron relaciones en el sentido contrario a las predicciones de Cohen y Felson.[6]

Dado el interés que a nivel internacional han despertado las ideas de Cohen y Felson, se prevé que la TAR puede ser analíticamente útil para predecir la victimización cibernética en nuestra región. Así, la pregunta central que guía este estudio es ¿qué actividades cotidianas de las que se experimentan dentro y fuera de Internet se relacionan con la probabilidad de victimización por *hacking* y por acoso en línea (*online harassment)*? Para dar respuesta a esto, el propósito de esta investigación es hallar, a partir de los conceptos y medidas de la TAR, algunas variables individuales y ambientales asociadas a la cibervictimización. En concreto, se analizará estadísticamente si la exposición a un delincuente motivado, la idoneidad del objetivo/víctima y la falta de vigilancia efectiva tienen correspondencia con el *hacking* y al acoso en línea de universitarios venezolanos. Los resultados obtenidos pueden mejorar el conocimiento sobre los correlatos de la victimización cibernética y sobre la validez de la TAR para la predicción y explicación de este fenómeno.

Método

Participantes

Los datos de la muestra provienen de estudiantes universitarios venezolanos adscritos a la Facultad de Ciencias Jurídicas y Políticas de la Universidad de Los Andes. Esta es una muestra por conveniencia y en total fueron analizados 308 sujetos. En términos generales, el 63% (*N*=193) de la muestra es de sexo femenino y el 37% (*N*=113) masculino. En este grupo hay universitarios entre 17 y 56 años de edad y la media es de 25,94 años (D.T 0,09 años). El 68,2% de los sujetos cuenta con edades comprendidas entre 17 y 26 años, por lo tanto, puede señalarse que la muestra está conformada en su mayoría por estudiantes jóvenes. De este grupo de universitarios, un 17,9% (*N* =55) se encuentran estudiando primer año, 28,6% (*N* =88) segundo año, 16,9% (*N* =52) tercer año, 22,7% (*N*=70) cuarto año y un 13,3% (*N*=41) el quinto año de la carrera.

6 En este estudio solo el uso de mensajería instantánea se relacionó con el acoso en línea en la dirección propuesta por la TAR.

Medidas

Victimización en línea (Variable criterio)

La variable criterio se operacionalizó mediante dos formas de victimización por delitos informáticos.[7] La primera es el *hacking,* que se entiende como el acceso y posterior uso de un dispositivo o sitio de la red con fines nocivos, sin el debido consentimiento del usuario o titular al que pertenece. Esta definición se midió por medio del *hackeo* de correo electrónico y cuentas en redes sociales. La segunda es la cibervictimización por acoso en línea u *online harassment*, que se refiere a actos de hostigamiento en internet (Miró 2013). En esta investigación el acoso en línea se midió con tres ítems: suplantación de identidad, uso de imagen sin autorización y contacto repetido no deseado. Para cada una de las preguntas planteadas se usó un tipo de respuesta dicotómica en la que 0 representa "no" y 1 "sí".

Actividades rutinarias (Variables predictivas)

Las variables predictivas se diseñaron sobre la base de lo propuesto por la TAR (Cohen y Felson 1979) y en algunos de los estudios citados en párrafos anteriores. El *objetivo adecuado en línea* son aquellos comportamientos en el uso de internet que hacen a una persona o cosa un blanco probable para el delito. Este constructo se midió con los siguientes indicadores: 1) ¿Por medio de la mensajería instantánea (*Whatsapp, Line, BlackBerry Messenger*, etc.) tiene contacto con personas que no conoce? 2) ¿Abre o descarga enlaces o archivos enviados por desconocidos a través del correo electrónico? y 3) ¿Facilita información personal real a través de las redes sociales? La respuesta a cada una de estas preguntas fue de tipo binaria (0= no y 1= sí).

La *exposición a un delincuente motivado en línea* se operacionalizó como el conjunto de actividades que hace a un individuo más visible ante un ciberdelincuente cuando se conecta a internet. Los 5 indicadores usados para medir este constructo fueron el número de horas de conexión a internet, el uso de correo electrónico, el uso de redes sociales (*Twitter, Facebook*), la descarga de archivos y el uso de la banca *online.* En el caso del primer indicador se le preguntó al encuestado por la cantidad de horas que se conecta al internet durante una semana típica. Con relación a los otros cuatro indicadores, se consultó al encuestado ¿con qué frecuencia utiliza los siguientes servicios de internet a la semana? La categoría de respuesta se planteó como una escala tipo Likert que va de 0 (nunca) a 4 (siempre). En este caso, para efectos de los análisis multivariante se dicotomizaron las variables uso de correo electrónico, redes sociales y descarga de archivos como 0=poco y 1=mucho. En el caso de la variable uso de la banca *online* la categoría "no" se codificó con 0 y "sí" con 1.

Por último, el *guardián capaz* se operacionalizó como aquellas personas, tácticas individuales y herramientas tecnológicas que pueden evitar un potencial ciberdelito. Así, partiendo de este concepto, se han incluido en este estudio medidas sobre prácticas o hábitos del propio usuario que lo protegen del ciberdelito. Al respecto se preguntó: 1) ¿se conecta a internet desde computadoras de uso público (laboratorios de computación, cibercafés, etc.)?, y 2) ¿nos puede indicar si ha solicitado en alguna ocasión

7 Se decidió analizar estos delitos informáticos tomando como base la Constitución de la República Bolivariana de Venezuela de 1999, el Código Penal (2005) y la Ley Especial contra los Delitos Informáticos de 2001, dado que son conductas y acciones que van en contra de lo establecido en estas normas jurídicas (Venezuela 1999; 2001; 2005).

que borren o cancelen sus datos personales de algún registro en internet? Desde un punto de vista tecnológico, se requirió información sobre los programas de protección instalados en la computadora o dispositivo móvil, en concreto, por *software* antivirus y *antimalware*. Cada una de estas respuestas fue planteada de forma dicotómica. Así, en el caso de la variable relacionada con la conexión en equipos públicos el código 1 representa la presencia de la condición y en el resto de los indicadores se reservó para identificar la ausencia.

Tipo de estudio y procedimiento

Los informes de las empresas de ciberseguridad (Symantec, Kaspersky, ESET, etc.) o de las organizaciones públicas o privadas (OEA, BID, etc.) pueden ser un recurso útil para conocer los niveles de ocurrencia de la ciberdelincuencia en distintos lugares; pero la estadística utilizada es meramente descriptiva. En tales estudios no hay ningún intento de analizar relaciones entre variables que permita comprobar, por ejemplo, bajo qué condiciones una persona es vulnerable al ciberdelito. Es decir, entre muchos otros elementos, estos trabajos prescinden del uso de estadística bivariada y multivariante.

Evidentemente, con un nivel de análisis descriptivo es difícil tener un referente teórico acerca de la cibervictimización, lo que hace necesario plantearse otras estrategias de investigación. Es por ello que se ha decidido llevar a cabo un estudio correlacional, de corte transversal, basado en la encuesta de victimización como método de medición. El diseño de esta encuesta giró en torno a un conjunto de preguntas para recabar información sobre los delitos cibernéticos sufridos por el encuestado y algunas variables de orden teórico como el caso de las actividades cotidianas que se suelen desarrollar cuando se hace uso de las TIC.

En términos operativos, luego del diseño de la encuesta se solicitó el permiso a cada profesor en horas lectivas para su aplicación y así contar con su apoyo en el control del alumnado. Se aplicó el instrumento a un total de 11 secciones, las cuales tenían un número de alumnos que oscilaba entre 15 y 70 sujetos por aula al momento de la actividad. Antes de dar inicio a la aplicación del instrumento, los estudiantes fueron informados del contenido general, extensión, forma de llenado y anonimato del mismo. Se hizo hincapié en que cualquier duda sobre algún punto del contenido podría ser consultada al encuestador. El llenado de la encuesta tomó un tiempo promedio de 25 minutos. Finalmente, se utilizó el paquete estadístico SPSS versión 20 para el vaciado y análisis de los datos.

Estrategia de análisis estadístico

En principio se desarrolló un análisis univariado para examinar las características principales de la muestra. Luego se efectuaron algunas pruebas de X^2 y se calcularon coeficientes de correlación *Phi* para determinar los niveles de independencia y asociación entre las variables predictivas y los indicadores de cibervictimización.[8] Finalmente, se utilizó la regresión lógistica binaria debido a la escala de medida de las variables criterio que en este caso fue nominal con dos valores (dicotómica). De esta manera, se pusieron a prueba cinco modelos de regresión por separado para cada indicador de cibervictimización.

8 Por razones de espacio no se presentan los resultados de los análisis bivariados. Si hay algún interés en ellos pueden solicitárselos a los autores.

Resultados

Estadística descriptiva

Según los resultados de la tabla 1, el 20% de la muestra (*N*= 61) fue víctima del acceso no autorizado a su correo electrónico y el 15% sufrió el *hackeo* de una cuenta de red social como *Twitter, Facebook, Instagram*, etc (*N*= 45). Con respecto al acoso en línea (*online harassment*), el 17% de la muestra (*N*= 52) reportó haber sido víctima de suplantación de identidad, el 20% reveló que usaron su imagen sin autorización (*N*= 60) y un 62% experimentó acoso repetidamente luego de haber prohibido un nuevo contacto (*N*= 184).

Con relación a las actividades rutinarias, el 19% de los universitarios (*N*= 58) trató con desconocidos mediante mensajería instantánea, el 12% abrió vínculos y descargó archivos extraños (*N*= 37) y un 33% proporcionó información personal en Internet (*N*= 98). Los indicadores de exposición en línea señalan que estos jóvenes se conectaron a internet, por término medio, 20,08 horas a la semana. El 68% de la muestra (*N*= 206) utilizó con mucha frecuencia el correo electrónico y las redes sociales y esa misma proporción realizó operaciones financieras en la banca *online*. En cuanto a los hábitos de protección, el 81% mencionó que tiene instalado un software antivirus en sus dispositivos (*N*= 233) y 9% algún programa *antimalware* (*N*= 26). Finalmente, el 52% de la muestra (*N*= 158) reportó haberse conectado a internet en computadoras de sitios públicos y un 42% solicitó varias veces que borraran o cancelaran sus datos personales de algún registro en internet (*N*= 120).

Tabla 1. Estadística descriptiva

	Min-Max	M (DT)
Variable		
Victimización en línea		
Hacking de correo electrónico	0-1	0,20 (0,40)
Hacking de cuenta red social	0-1	0,15 (0,36)
Suplantación de identidad	0-1	0,17 (0,38)
Uso de imagen sin permiso	0-1	0,20 (0,40)
Contacto repetido no deseado	0-1	0,62 (0,49)
Objetivo adecuado en línea		
Comunicación con extraños	0-1	0,19 (0,39)
Abrir/descargar enlaces/ archivos desconocidos	0-1	0,12 (0,32)
Proporcionar información personal	0-1	0,33 (0,47)
Exposición a delincuente motivado en línea		
Número de horas en Internet (Semana)	1-150	20,08 (24,32)
Uso correo electrónico	0-1	0,68 (0,47)
Uso redes sociales	0-1	0,68 (0,47)
Descargar archivos	0-1	0,56 (0,50)
Banca *online*	0-1	0,68 (0,47)
Guardián eficaz (tecnológico y humano)		
Software antivirus	0-1	0,81 (0,39)
Software antimalware	0-1	0,09 (0,28)
Conectarse a Internet en computadoras públicas	0-1	0,52 (0,50)
Solicitar eliminación/ cancelación datos	0-1	0,42 (0,49)
Variables de control		
Sexo (Hombre)	0-1	0,37 (0,48)
Edad	17-56	25,94 (0,09)

Análisis de regresión logística binaria

Hacking

Los resultados de los análisis multivariante basados en la técnica de regresión logística binaria se resumen en la tabla 2. Estos resultados señalan para el Modelo 1 y 2 que la mayoría de las medidas referentes a los tres elementos conceptuales de la TAR no fueron predictores significativos del *hacking.* En concreto, ninguna de las variables que conforman el constructo *objetivo adecuado en línea* tuvo correspondencia con los dos indicadores de acceso no autorizado a correos y cuentas en redes sociales.

Solo una medida de *exposición a un delincuente motivado*, en este caso el uso de banca *online,* mostró una relación estadísticamente significativa con el *hackeo* de correo electrónico pero de forma negativa (Modelo 1). En el caso del constructo *guardián eficaz*, solicitar la eliminación y cancelación de datos en registros de internet (OR=2.41) fue un predictor significativo del *hackeo* de correos electrónicos y esa misma variable (OR=2.35) junto al uso de antimalware (OR=4.55) se relacionaron con el acceso no autorizado a cuentas de redes sociales (Modelo 2). En este caso, no usar *antimalware* aumenta 83% el riesgo de *hackeo* de cuentas en *Twitter, Facebook, Instagram*, etc. Por el contrario, el uso de antivirus presentó un efecto inverso sobre el *hacking* de cuentas de redes sociales (Modelo 2).

Acoso en línea (Online harassment)

De manera muy similar al *hacking*, la Tabla 2 muestra que un gran número de medidas no presentaron una relación significativa con el acoso en línea. Específicamente, en el caso de la dimensión *objetivo adecuado en línea,* abrir o descargar enlaces/archivos desconocidos se relacionó con la probabilidad de ser victimizado por suplantación de identidad pero, en esta oportunidad, con signo negativo. Con respecto a la *exposición a un delincuente motivado,* el número de horas en internet es un predictor significativo del acoso en línea en los Modelos 4 y 5. En el caso de la victimización por uso de imágenes no autorizadas y por contacto reiterado no consentido, el mayor número de horas en internet aumenta 50% el riesgo de acoso.

Usar tanto el correo electrónico como las redes sociales se relacionó negativamente con el contacto reiterado no consentido y la suplantación de identidad. En referencia al concepto de *guardián eficaz* únicamente la variable solicitar la eliminación y cancelación de datos en registros de Internet tuvo una relación significativa (OR=2.41) con el acoso por uso de imágenes personales sin autorización (Modelo 4) y con el acoso por contacto reiterado no deseado (Modelo 5). En el primer caso disminuyó un 72% el riesgo de este tipo de acoso y en el segundo caso lo redujo un 80%. Asimismo, hay que destacar que en los Modelos 3 y 4, conectarse a internet en computadoras públicas presentó una relación negativa con las respectivas variables criterio.

En conjunto, estas medidas parecen predecir mejor el acoso por contacto repetido no deseado (R^2= 28%) que se analizó en el Modelo 5. Además, la variable solicitar la eliminación y cancelación de datos de algún registro en internet parece ser una variable clave en la predicción de los diferentes tipos de cibervictimización, dados los patrones de relación significativa que presentó en casi todos los modelos. Finalmente, las medidas usadas para operacionalizar el constructo *objetivo adecua-*

Tabla 2. Modelos de regresión logística binaria para victimización por *hacking* y *harassment* (N= 308)

	Hacking 1 (Correo electrónico) **MODELO 1**			*Hacking 2* (Cuenta red social) **MODELO 2**			*Harassment 1* (Suplantación de identidad) **MODELO 3**		
Variable	B	Wald	OR	B	Wald	OR	B	Wald	OR
Objetivo adecuado en línea									
Comunicación con extraños (Si=1)	-0.02	0.00	0.97	-0.48	0.88	0.62	-0.29	0.38	0.74
Abrir/descargar enlaces/archivos desconocidos (Si=1)	-0.59	1.08	0.56	0.13	0.04	1.14	-1.06	**3.59***	0.34
Proporcionar información personal (Si=1)	-0.62	2.71	0.54	-0.14	0.11	0.87	-0.39	0.95	0.68
Exposición a delincuente motivado en línea									
Número de horas en Internet (Semana)	-0.00	0.75	0.99	-0.01	0.67	0.99	0.01	1.58	1.01
Uso correo electrónico (Si=1)	-0.88	3.44[a]	0.41	-0.89	2.36	0.41	-1.12	**4.37***	0.33
Uso redes sociales (Si=1)	0.12	0.07	1.12	0.14	0.07	1.15	-1.02	3.09	0.36
Descargar archivos (Si=1)	-0.05	0.02	0.94	0.06	0.02	1.06	0.46	1.06	1.58
Banca *online* (Si=1)	-0.99	**4.23***	0.37	-0.65	1.54	0.52	-0.23	0.27	0.79
Guardián eficaz (tecnológico y humano)									
Software antivirus (No=1)	0.48	0.78	1.61	-0.99	**4.12***	0.37	-0.68	1.96	0.51
Software antimalware (No=1)	0.45	0.51	1.57	1.52	**6.11***	4.55	0.35	0.26	1.41
Conectarse a Internet en computadoras públicas (Si=1)	-0.71	**3.34**[a]	0.49	-0.73	2.62	0.48	-1.22	**7.64****	0.30
Solicitar eliminación/cancelación de datos (No=1)	0.88	**5.50***	2.41	0.86	**4.00***	2.35	0.31	0.59	1.36
Variables de control									
Sexo (Hombre = 1)	0.40	0.84	1.49	0.28	0.34	1.33	0.03	0.00	1.04
Edad	0.01	0.20	1.01	-0.01	0.12	0.99	0.01	0.36	1.02
2 Log-likelihood	192,63			158,43			174,19		
Modelo X^2	25.20* (df=14)			22.87[a] (df=14)			28.01*(df=14)		
Nagelkerke R^2	17%			17%			20%		

Nota: $^*p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$; $^{a}p < 0.06$

do en línea resultaron las más débiles del conjunto. En este caso, prácticamente todos los indicadores no tuvieron correspondencia con ninguna de las variables de cibervictimización analizadas y la única medida que presentó una relación significativa lo hizo con signo negativo. Esto, junto a las escasas y contradictorias relaciones encontradas en el resto de las dimensiones, ofrece un débil apoyo empírico a las hipótesis de Cohen y Felson.

Discusión y conclusiones

El objetivo principal de este estudio (quizá inédito en la región) fue identificar algunos predictores de la victimización cibernética en una muestra de estudiantes universitarios. Para ello, se ha medido un conjunto de indicadores vinculados a los tres conceptos teóricos básicos de la TAR (delincuente motivado, objetivo adecuado y falta de vigilancia eficaz) para

Tabla 2. Continuación...

	Harassment 2 (Uso de imagen sin permiso) **MODELO 4**			*Harassment 3* (Contacto repetido no deseado) **MODELO 5**		
Variable	B	Wald	OR	B	Wald	OR
Objetivo adecuado en línea						
Comunicación con extraños (Si=1)	-0.59	1.74	0.55	-0.54	1.24	0.58
Abrir/descargar enlaces/archivos desconocidos (Si=1)	-0.17	0.10	0.84	-1.07	3.13	0.34
Proporcionar información personal (Si=1)	-0.51	1.92	0.60	-0.43	1.61	0.65
Exposición a delincuente motivado en línea						
Número de horas en Internet (Semana)	0.02	**6.12***	1.02	0.02	**4.06***	1.02
Uso correo electrónico (Si=1)	-0.28	0.45	0.75	-0.77	**4.48***	0.46
Uso redes sociales (Si=1)	0.61	2.07	1.85	-0.77	**4.25***	0.46
Descargar archivos (Si=1)	0.27	0.44	1.30	0.12	0.11	1.12
Banca *online* (Si=1)	-0.72	2.72	0.49	-0.07	0.04	0.93
Guardián eficaz (tecnológico y humano)						
Software antivirus (No=1)	-0.59	1.61	0.56	0.33	0.65	1.39
Software antimalware (No=1)	-0.69	0.90	0.50	-0.48	0.66	0.62
Conectarse a Internet en computadoras públicas (Si=1)	-0.95	**5.89***	0.39	-0.60	3.26	0.55
Solicitar eliminación/cancelación de datos (No=1)	0.97	**7.29****	2.65	1.36	**15.35*****	3.89
Variables de control						
Sexo (Hombre = 1)	-0.08	0.04	0.92	-0.14	0.14	0.87
Edad	0.00	0.00	1.00	-0.00	0.19	0.99
2 Log-likelihood	201,57			245,11		
Modelo X^2	30.44**(df=14)			60.00*** (df=14)		
Nagelkerke R^2	20%			28%		
Nota: $^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$; $^{a}p < 0.06$						

tratar de responder a la pregunta: ¿qué actividades cotidianas de las que se experimentan dentro y fuera de Internet se relacionan con la probabilidad de cibervictimización? A continuación se discuten algunos resultados en el marco de esta interrogante.

Un rasgo muy notorio de estos resultados es que gran parte de las medidas analizadas no estaban relacionadas significativamente con las diferentes formas de cibervictimización. Además, el patrón de predicción y la fuerza de las pocas relaciones significativas encontradas variaban según el tipo de variable criterio analizada. El *guardián eficaz* mostró tener el efecto más fuerte y estable sobre las distintas formas de victimización cibernética, en especial sobre las de acoso en línea.

En este caso, al menos una de las medidas de este concepto se relacionó significativamente con casi todos los modos de victimización.

La *exposición a un delincuente motivado* presentó un patrón de predicción más modesto e inestable. En este caso, ninguna de las medidas utilizadas predijo el *hacking* de cuentas de redes sociales. El efecto más débil sobre la cibervictimización lo mostró el *objetivo adecuado en línea* cuyos indicadores, casi en su totalidad, no se relacionaron significativamente con las cinco variables criterio observadas. Enseguida se discuten con más detalle algunos elementos de este patrón de resultados.

En primer término, solo se hallaron tres medidas estadísticamente relacionadas con algunos de los cinco indicadores de cibervictimización conforme a las expectativas de la TAR. Concretamente, los universitarios que pasaron más tiempo en internet (lo cual debe aumentar la probabilidad de *exposición a un delincuente motivado en línea*) fueron más propensos a ser victimizados por acoso *online*. Estos resultados van en el mismo sentido de los reportados por Holt y Bossler (2009) y Ngo y Paternoster (2011) y contrarios a los obtenidos por Reyns *et al.* (2011). Las otras dos variables incluidas en la dimensión *guardián eficaz* son el uso de software antimalware (que actuó como factor de protección del *hackeo* a cuentas de redes sociales) y la solicitud de eliminación de datos en registros de Internet (la cual disminuyó el riesgo tanto de *hacking* como de *online harassment*).

En relación con esto, el efecto del *antimalware* se corresponde con lo reportado en otras investigaciones y demuestra que el uso del mismo reduce la posibilidad de que existan en el dispositivo electrónico programas maliciosos destinados a conseguir claves y datos personales. Aun cuando el efecto del *antimalware* sobre el *hacking* ha sido poco estudiado en muestras de universitarios, este hallazgo confirma su relevancia e, incluso, como lo mencionan Ngo y Paternoster (2011), lo importante de medir de manera separada los distintos indicadores de protección tecnológica (antivirus, antimalware, *firewall*) y no de forma compuesta.

Sumado a esto, el hecho de que la fuerza del efecto y el tipo de factores de riesgo/protección varíen según el indicador de victimización observado, permite especular que los correlatos y las causas de la cibervictimización pueden ser diferentes dependiendo de la naturaleza del delito que se pretenda predecir. Por ejemplo, el *hacking* que es un delito (*tipo I*) *centrado* en la computadora tal vez responda mejor a variables de carácter tecnológico (programas *antimalware*) y el acoso en línea que es un delito (*tipo II*) *asistido* por las TIC se relacione principalmente con variables de interacción social (v. gr. uso de redes sociales). Quizás este tipo de hallazgos contradice a la TAR como posible teoría *general* y sugiere el uso de enfoques específicos o tipologías para predecir y explicar mejor diversas formas de cibervictimización.

En segundo lugar, casi todos los indicadores de la dimensión *objetivo adecuado en línea* no resultaron predictores significativos de la cibervictimización. Si bien esto se logra explicar por la manera en cómo se operacionalizó este concepto en el presente estudio, también es posible que existan otro tipo de efectos que, dados los objetivos de partida, no fueron evaluados como, por ejemplo, los de mediación. Es decir, la relación que se observó en los análisis bivariados entre los indicadores del *objetivo adecuado* y la cibervictimización, puede estar influenciada por alguno de los otros conceptos de la TAR (delincuente motivado y/o guardián eficaz). De no existir tal efecto mediador, el comportamiento estadístico de las medidas de este concepto que, cabe señalar, en otras investigaciones han mostrado tener una relación significativa con la cibervictimización (Choi 2008; Marcum

et al. 2010; Reyns *et al.* 2011), puede refutar la capacidad de la TAR para predecir y explicar la victimización en el mundo virtual.

En tercer lugar, se observaron algunas relaciones estadísticamente significativas contrarias a las predicciones de las TAR. Este es el caso, por ejemplo, de abrir/descargar enlaces/archivos desconocidos, usar correo electrónico y redes sociales, conectarse a internet en computadoras públicas y disponer de antivirus. Esta última variable, en concreto, presentó una relación que está en sintonía con los hallazgos reportados por Ngo y Paternoster (2011). Una lectura somera de estas relaciones haría suponer que, por ejemplo, no usar correos electrónicos o tener instalado un antivirus contribuye a estas formas de cibervictimización. Sin embargo, este tipo de relaciones con signo contrario a las expectativas de la TAR puede ser consecuencia de la naturaleza transversal de los datos. Es decir, puesto que en este estudio no se controló el orden temporal de las relaciones es plausible sostener que una persona que ha sido víctima de ciberdelito decide, posteriormente, restringir su ingreso a páginas extrañas, limitar el uso de redes sociales y correos electrónicos o instalar un antivirus.

Queda claro que estos resultados en conjunto ofrecen, provisionalmente, poco apoyo a la aplicabilidad de la TAR para la compresión de la cibervictimización. Pero, cabe señalar que los mismos pueden tener alguna utilidad en términos preventivos. En principio, la TAR determina qué condiciones son casi siempre necesarias para aumentar la probabilidad de delito y sostiene que la ausencia de cualquiera de los tres elementos es una condición suficiente para evitar que ocurra la victimización. En este estudio se observó una mejor capacidad predictiva del elemento *guardián eficaz* en el que, concretamente, *usar programas antimalware* y *solicitar la eliminación de información personal en la red* disminuyen el riesgo de cibervictimización. Los hallazgos aquí presentados confirman la importancia del propio usuario para un control efectivo. Quien utiliza los servicios de las TIC parece desempeñar un rol básico en la cibervictimización al definir qué dispositivos tecnológicos de vigilancia (*antimalware*) y estrategias de protección no electrónicas lo convierten en un autoguardián (eficaz) de su seguridad informática.

Estos hallazgos permiten llegar a la misma conclusión de Choi (2008) con respecto a que la vigilancia efectiva puede ser el elemento fundamental de la TAR e, inclusive, por el que hay que interesarse más de cara a la prevención situacional. Si las hipótesis de Cohen y Felson son válidas, tal vez garantizando la sola presencia de este elemento situacional se consiga desestimular la decisión de cometer delitos por parte de un sujeto motivado. Dado el aparente alcance que tiene el *guardián eficaz*, las políticas y campañas de disminución de la cibervictimización (desplegadas tanto por entidades públicas como privadas) deben ir orientadas a estimular la educación y habilidades de los usuarios para una adecuada autoprotección que les permita modificar el ámbito de oportunidades delictivas en el ciberespacio.

Para concluir, aun cuando estos resultados hacen un modesto aporte a la investigación sobre la cibervictimización, hay varias limitaciones que se deben considerar. Una de las más importantes es, precisamente, la transversalidad de los datos. Sería importante en futuras investigaciones contar con datos longitudinales para desentrañar las relaciones causales entre las variables de estudio, especialmente para poder identificar si el uso de medidas de protección como el antivirus se da antes o

después de un episodio de cibervictimización. Otra limitación fue la naturaleza de la muestra que, en esta ocasión, se limitó al ámbito universitario. En este caso, analizar en futuros estudios muestras representativas de otras poblaciones permitirá mejorar la generalización de los resultados. Finalmente, la tercera limitación de esta investigación tiene que ver con la validez de los indicadores escogidos.

Sería útil en próximas investigaciones utilizar otro tipo de medidas para operacionalizar los conceptos básicos de la TAR. Incluso, se pueden probar otras técnicas de recolección de información como la metodología de viñetas basada en encuestas factoriales (Wikström, Oberwittler, Treiber y Hardie 2012, como ejemplo de este método en Criminología). Esta técnica consiste en presentarle al encuestado una situación o escenario hipotético inspirado en la vida real y evaluar las decisiones en situaciones concretas cuando se usa Internet. La finalidad de esta metodología es observar la relación de dichas decisiones o valoraciones con las variables teóricas de base y, desde luego, con la probabilidad de cibervictimización. Todo esto podría dar como resultado datos más robustos que permitan apoyar o rechazar la aplicabilidad de esta teoría criminológica para el estudio de la ciberdelincuencia y, por consiguiente, el diseño de métodos más precisos para su prevención y control.

Bibliografía

BID (Banco Interamericano de Desarrollo). 2016. *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016.* Washington: Observatorio de la Ciberseguridad en América Latina y el Caribe.

Bossler, Adam, y Thomas Holt. 2009. "Online activities, guardianship, and malware infection: An examination of Routine Activities Theory". *International Journal of Cyber Criminology* 1: 400-420.

Bossler, Adam, Thomas Holt y David May. 2013. "Predicting online harassment victimization among a juvenile population". *Youth & Society* 44 (4): 500-523.

CEPAL (Comisión Económica para América Latina y el Caribe). 2016. "Estado de la banda ancha en América Latina y el Caribe 2016. Santiago de Chile: Naciones Unidas", http://www.cepal.org/es/publicaciones/40528-estado-la-banda-ancha-america-latina-caribe-2016.

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

Cohen, Lawrense y Marcus Felson. 1979. "Social change and crime rate trends: A routine activity approach". *American Sociological Review* 44: 588-608.

Eck, John y Ronald Clarke. 2003. "Classifying common police problems: A Routine activity approach". *Crime Prevention Studies* 16: 7-39.

ESET. 2011. "Aumenta el hacktivismo en América Latina", http://www.eset-la.com/centro-prensa/articulo/2011/aumenta-hacktivismo-america-latina/2572.

_____. 2016. "ESET Security Report. Latinoamérica 2016", http://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf.

Gordon, Sarah y Richard Ford. 2006. "On the definitions and classification of cybercrime". *J. Comput. Virol* 2 (1): 13-20.

Grabosky, Peter. 2001. "Virtual criminality: old wine in new bottles?". *Social and legal studies* 10 (2): 243-249.

Holt, Thomas y Adam Bossler. 2009. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization". *Deviant Behavior* 30 (1): 1–25.

Kaspersky. 2016. "Internautas en América Latina sufren 12 ataques de malware por segundo", http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/2016/internautas-en-america-latina-sufren-doce-ataques-de-malware-por-segunda-revela-kaspersky-lab.

Leukfeldt, Eric y Majid Yar. 2016. "Applying Routine Activity Theory to Cibercrime: A Theoretical and Empirical Analysis". *Deviant Behavior* 37 (3): 263-280.

Marcum, Catherine, George Higgins y Melissa Ricketts. 2010. "Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory". *Deviant Behavior* 31 (5): 381–410.

McGuaire, Michael. 2007. "*Hypercrime: A geometry of virtual harms*". Londres: Routledge.

Miró, Fernando. 2011. "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la Teoría de las actividades cotidianas para la prevención del cibercrimen". *RECPC* 13-07: 1-55.

_____. 2013. "La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio". *Revista española de investigación criminológica* 5 (11): 1-35.

Ngo, Fawn y Raymond Paternoster. 2011. "Cybercrime victimization: An examination of individual and situational level Factors". *International Journal of Cyber Criminology* 5 (1): 773–793.

OEA (Organización de Estados Americanos). 2013. "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos", http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf.

Reyns, Bradford, Billy Henson y Bonnie Fisher. 2011. "Being pursued online. Applying cyberlifestyle-routine activities theory to cyberstalking victimization". *Criminal Justice and Behavior*, 38 (11): 1149–1169.

Symantec. 2014a. "Tendencias de seguridad cibernética en América Latina y el Caribe", https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends.

_____. 2014b. "Latin American + Caribbean 2013 in numbers", http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc-annex.pdf.

Tillyer, Marie y John Eck. 2009. "Routine Activities". En *21st century criminology: A reference handbook,* editado por Mitchell Miller, 279-287. Thousand Oaks: Sage.

Venezuela. 1999. "Constitución de la República Bolivariana de Venezuela". Gaceta Oficial de la República Bolivariana de Venezuela. N° 36860 del 30 de Diciembre de 1999.

_____. 2001. "Ley Especial contra Delitos Informáticos (2001)". Gaceta Oficial de la República Bolivariana de Venezuela. N° 37313 del 30 de Octubre de 2001.

_____. 2005. "Código Penal". Gaceta Oficial de la República Bolivariana de Venezuela. N° 5768E del 13 de Abril de 2005.

Wall, David. 2005. "The Internet as a conduit for criminal activity". In *Information Technology and the Criminal Justice System*, editado por April Pattavina, 77-98. EE.UU: Sage.

Wikström, Per-Olof, Dietrich Oberwittler, Kyle Treiber y Beth Hardie. 2012. *Breaking rules: The social and situational dynamics of young people's urban crime*. Oxford: University Press.

Wikström, Per-Olof, y Kyle Treiber. 2016. "Situational Theory: The Importance of Interactions and Action Mechanisms in the Explanation of Crime". En *The Handbook of Criminological Theory*, editado por Alex Piquero, 415-444. EE.UU: Wiley Blackwell.

Yar, Majid. 2005. "The novelty of cybercrime: An assessment in light of routine activity theory". *European Journal of Criminology* 2 (4): 407-427.

_____. 2006. *Cybercrime and Society*. Londres: Sage.