Revista Española de Investigación Criminológica

La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio[1]

Manuscrito recibido el 31 de octubre de 2013/Publicado el 18 de diciembre de 2013

Fernando Miró
Universidad de Elche

RESUMEN

El presente estudio tiene como objetivo, además de conocer los niveles de cibervictimización social en relación a la muestra analizada, ofrecer un modelo predictivo que permita en última instancia establecer estrategias de prevención basadas en evidencias científicas. Parte de la reconceptualización de la Teoría de las Actividades Cotidianas de Cohen y Felson (1979) y establece la hipótesis de que el usuario, con su actuar cotidiano en el ciberespacio, es un elemento clave en la producción del evento delictivo. Mediante la realización de una encuesta telefónica con el sistema CATI (Computer Assisted Telephone Interviewing) a 500 sujetos entre 18 y 65 años de edad para la recogida de datos y su posterior análisis, se llega a la conclusión de que el ámbito de riesgo de los usuarios viene definido a través de la incorporación de determinados bienes y esferas de su privacidad al ciberespacio, del uso que hacen de Internet y la ausencia de medidas de autoprotección adoptadas.

Palabras clave: Cibercrimen social, cibervictimización, *harassment*, Teoría de las Actividades Cotidianas, Teoría de las Actividades Cotidianas en el Ciberespacio, objetivo adecuado, guardián capaz.

[1] La correspondencia debe enviarse a Fernando Miró Llinares. Universidad Miguel Hernández de Elche, Avda. de la Universidad, s/n, 03201 Elche (Spain). fmiro@umh.es

ABSTRACT

The aim of this research is to examine levels of social cybervictimization in relation to an analyzed sample as well as to provide a predictive model which ultimately allows establishing prevention strategies based on scientific evidences. The research starts from the reconceptualization of the Routine Activity Theory (1979), developed by Cohen and Felson, and establishes the hypothesis that the user and his daily activities in cyberspace are key elements in producing crime event. A sample of 500 people aged between 18 and 65 has been interviewed using the CATI system (Computer-Assisted Telephone Interviewing) in order to collect and analyze data. According to the data survey, the risk area of the user is defined by private goods and spheres he incorporates into cyberspace, the use of Internet and the lack of self-defense strategies.

Keywords: Social cybercrime, cybervictimization, harassment, Routine Activity Theory, Routine Activity Theory in Cyberspace, suitable target, capable guardian.

1. Introducción.

La sustitución del término delincuencia informática por el de cibercriminalidad se debe esencialmente a la voluntad de expresar con tal conceptualización que, independientemente del medio técnico utilizado o del objeto sobre el que se perpetra, hoy los comportamientos criminales se pueden cometer también en otro ámbito de riesgo distinto al espacio físico, el ciberespacio. La evolución de las Tecnologías de la Información y la Comunicación, especialmente en la última década, han convertido Internet en un medio nuevo e indispensable para la comunicación entre las personas y para el desarrollo de variadas vertientes de su vida. Y la obviedad de que este nuevo espacio virtual es estructuralmente diferente al espacio físico, conlleva la, quizás no tan evidente reflexión, de que las interacciones que ahí se producen o cualquier delito que se cometa en él, conllevarán forzosamente unas características distintas. Como he señalado, en un trabajo anterior (Miró, 2011), los caracteres singulares de este nuevo lugar de comunicación transnacional, anónimo y sujeto a revolución permanente, en el que las dimensiones espacio-temporales incrementan las posibilidades de contacto entre potenciales agresores y víctimas, ha hecho del ciberespacio un ámbito de oportunidad delictiva distinto al espacio físico, en el que la víctima adquiere especial relevancia para la explicación y prevención del delito.

La cibercriminalidad social quizás sea, de entre todas las categorías de delitos cometidos en el ciberespacio, la que más evidentemente refleja tanto esa expresividad de la categoría "cualesquiera delitos ejecutados por medio del uso de las TIC "(Wall, 2007), como algunas de las más significativas características de ese nuevo ámbito de oportunidad delictiva que es el ciberespacio, tal y como después se observará. Lo cierto es que hoy Internet ya no constituye únicamente un medio para la intercomunicación de sistemas informáticos con finalidad económica, sino que también lo es para la interacción personal entre usuarios, para la comunicación íntima entre personas o para la cesión voluntaria de esferas de intimidad. Esto se debe especialmente al protagonismo que han adquirido últimamente las redes sociales y demás herramientas de comunicación personal de Internet que, además, y como corolario negativo inevitable, han traído consigo toda una suma de conductas ilícitas relacionadas con tales relaciones sociales o personales que son las que integramos dentro de esa macrocategoría criminológica denominada cibercriminalidad social. En efecto, es la irrupción de la web 2.0, la que ha supuesto la aparición de ciberataques que afectan a bienes personalísimos como el honor, la intimidad, la dignidad, la libertad sexual o similares (Clough, 2010), que en la literatura criminológica, han ido integrándose en categorías de delitos caracterizadas en su nomenclatura por la suma de prefijos del tipo *cyber*, -u *online*,- con términos referidos a fenómenos criminales preexistentes a la era de Internet. Así es como hemos empezado a saber del *online harassment,* el *cyberbullying,* el *cyberstalking,* el *online grooming* y demás denominaciones de conductas que, juntas, conformarían la categoría cibercriminalidad social. Ésta, frente a otras como la cibercriminalidad económica o la política englobaría, pues, todos aquellos ataques ejecutados en el ciberespacio que afectan a las diferentes esferas personales puestas en común en el ámbito de comunicación social que es Internet.

Si bien podríamos decir que hay tantas modalidades de cibercriminalidad social como formas diferentes de ataque a los distintos intereses personales que pueden verse afectados por las relaciones sociales en el ciberespacio, también es posible hacer dos grandes categorizaciones internas dentro de tal macrocategoría.

La primera podría realizarse atendiendo a la víctima del ciberataque, concretamente a su carácter o no de menor. En efecto, dentro de la cibercriminalidad social son especialmente relevantes algunos cibercrímenes relacionados con los

menores como el *cyberbullying* o el *online child grooming*. El *cyberbullying* hace referencia a las formas de agresión entre menores a través de Internet (Marco Marco, 2010; Patchin e Hinduja, 2006) y ha sido definido por Smith *et al.* (2008: 376) como "una acción agresiva e intencional, desarrollada por un grupo o un individuo, usando formas electrónicas de contacto, repetida varias veces a lo largo del tiempo contra una víctima que no puede defenderse fácilmente". Independientemente de las connotaciones de daño psicológico asociadas al fenómeno, el mismo se caracteriza por una multiplicidad de conductas delictivas o ilícitas ejecutadas por un menor sobre otro, generalmente en el ámbito escolar, y consistentes en atormentar, molestar, amenazar, acosar, humillar, avergonzar, etc., (Marco Marco, 2010) utilizando ya no sólo el espacio físico sino el ciberespacio, bien como ámbito único de acoso o bien como extensión del acoso ya ejercido directamente en el ámbito escolar (Miró, 2013). La otra modalidad de cibercrimen social contra menores que más interés y preocupación social ha despertado en los últimos años es el *online child grooming*, consistente en el contacto de un adulto con un menor a través de Internet realizado para seducir (Berson, 2003), lograr confianza con el menor y obtener de él imágenes con contenido sexual y/o, incluso, una cita posterior ya en el ámbito físico (McAlinde, 2006).

Pero no sólo los menores pueden ser víctimas de acoso, sexual o no, en el ciberespacio. Es indudable que el uso de las TIC para la comunicación social es especialmente popular entre los adolescentes, y también lo es que los ciberataques sobre ellos son especialmente llamativos por la especial tutela que estas víctimas merecen, pero las redes sociales también lo son hoy para adultos y jóvenes mayores de 18 años que se ven sometidos a similares formas de hostigamiento a las ejecutadas sobre menores. Así, cuando se hace uso de Internet u otra tecnología de la comunicación para hostigar, perseguir o amenazar a un mayor de 18 años estamos hablando de *cyberstalking* (Basu y Jones, 2007), definido también por Bocij y McFarlane (2002: 12) como "un grupo de comportamientos en los que una persona, grupo de personas u organización, utilizan las tecnologías de la información y de las comunicaciones para acosar a otra persona, grupo de personas o una organización. Estos comportamientos pueden incluir, aunque no están limitados, la transmisión de amenazas y acusaciones falsas, daños a los datos o equipos, robo de identidad, robo de datos, 'monitoreo' informático, la solicitación de sexo y cualquier otra forma de agresión". El

cyberstalking, por tanto, se asemeja al *cyberbullying* en que tales constructos exigen un acoso reiterado, esto es, que las conductas de hostigamiento, las injurias, las calumnias, las amenazas y demás comportamientos, se realicen de forma continuada sobre una misma víctima. Es posible, sin embargo, y de hecho es lo más habitual, que tales modalidades de ciberataque se realicen de forma singular e individualizada sobre una o varias víctimas y no como parte de un hostigamiento continuado. Para referirse a estas conductas que, aun realizadas singularmente, pueden resultar delictivas o ilícitas, la literatura utiliza el término *harassment.* El *harassment* puede ser materializado en acciones como: recibir contacto no deseado (Henson, 2011), publicar información falsa, enviar mensajes injuriosos, amenazantes o abusivos, suplantar la identidad de otro con ánimo ofensivo o ridiculizante, animar a otras personas a acosar, amenazar o insultar a otro, enviar software malicioso para dañar el equipo de una persona concreta, enviar troyanos para controlar su sistema informático, acceder a información confidencial para descubrirla o revelarla, entre otros (Bocij, 2003).

Además de las conductas de *harrassment*, los adultos y jóvenes mayores de edad también pueden ser en el ciberespacio víctimas de ataques con contenido sexual que, de forma imprecisa y apenas relacionada con el concepto jurídico, suelen englobarse dentro del término ciberacoso sexual. Dentro del *sexual harrassment* se incluirían todos los ataques, realizados por medio del uso de las TIC, que atenten contra la libertad sexual de una persona, y entre los que suelen incluirse el envío de mensajes con contenido de carácter sexual, la exposición no deseada a material pornográfico, sentirse obligado a realizar comportamientos de tipo sexual a través de la *webcam*, a enviar fotos íntimas propias, etc. (Barak, 2005).

Pese a que todos ellos son cibercrímenes sociales cometidos en relación con el uso del ciberespacio para la comunicación social entre personas, es evidente la diferencia entre estos últimos ciberdelitos que atentan contra la libertad sexual integrados en el término "ciberacoso sexual" y, por otra parte, los que afectan a otros intereses dignos de protección como la libertad, la dignidad, el honor o la intimidad, y que se incluyen en el concepto de *harassment.* Consecuentemente, estas dos clases de cibercriminalidad social dan lugar a dos clases de cibervictimización social, entendiendo por ésta la derivada de cualesquiera ataques atentatorios contra bienes jurídicos personalísimos, perpetrados en el marco de relaciones sociales delimitado por

el ciberespacio: la victimización por ciberataques sexuales y la victimización por *harassment.* Como se verá después, estas dos categorías han de ser operativizadas como acciones concretas de acoso sexual y no sexual. En cualquier caso, lo relevante de este estudio no está en determinar la incidencia de cada una de las formas concretas de ataque, ni si quiera de la identificación descriptiva de las víctimas, sino de los factores de riesgo asociados a la victimización social, a lo cual dedicamos el siguiente punto.

2. Marco Teórico

2.1. Revisión de los estudios existentes

La literatura que se ha dedicado al análisis de la victimización por cibercriminalidad social, especialmente en el caso de menores,- y muy en particular, en el caso de victimización por *ciberbullying*,- suele centrar el análisis de los factores de riesgo de victimización en caracteres de tipo demográfico y, sobre todo, de personalidad y relación social. Factores como la búsqueda de sensaciones (Peter y Valkenburg, 2006), la satisfacción con la vida (Peter y Valkenburg, 2006), la conducta agresiva (Ybarra y Mitchel, 2007; Mitchell, Wolak, y Finkelhor, 2008), la tendencia a romper las reglas (Ybarra y Mitchel, 2007; Mitchell, Wolak y Finkelhor, 2008), la depresión (Ybarra, 2004; Mitchell, Wolak y Finkelhor, 2008), el abuso de sustancias (Ybarra, Espelage, y Mitchell, 2007; Hinduja y Patchin, 2008), la adicción a Internet (Casas, Del Rey y Ortega-Ruiz, 2013), la discapacidad intelectual (Didden *et al*., 2009), la baja autoestima (Calmaestra, 2011), los sentimientos de venganza (Hinduja y Patchin, 2008), los sentimientos de soledad (Calmaestra, 2011), la percepción del clima escolar (Calmaestra, 2011), o la relación pobre con los progenitores (Ybarra y Mitchell, 2004; Calmaestra, 2011), entre otros, han sido identificados como "de riesgo" de victimización por *cyberbullying*, y siguen protagonizando muchos de los estudios sobre victimización por estos y otros cibercrímenes sociales.

En los últimos tiempos, sin embargo, han surgido otros estudios que han tratado de relacionar la victimización social, y no sólo en el caso de los menores, con otros factores relacionados con las rutinas o actividades cotidianas de las víctimas potenciales de estos crímenes. El paradigma de las actividades cotidianas, suele utilizarse en

criminología para muchos análisis de victimización, pues al fin y al cabo, esta teoría o *approach* del crimen, está especialmente cercana a la teorización sobre la incidencia de la víctima en el evento criminal. Además, la utilización del paradigma de las actividades cotidianas para la determinación de los factores de riesgo en materia de cibercrimen, no conlleva, y esto es necesario aclararlo, negar la incidencia de otros factores personales, como los comentados antes, en la victimización social. Es obvio, que factores relativos a la personalidad podrán determinar claramente el riesgo de victimización según el factor y el delito. Lo mismo podría decirse de los factores demográficos. Respecto a éstos, sin embargo, no hay que obviar que en muchas ocasiones, reflejan diferencias en cuanto a la valoración del riesgo derivadas, más que del propio factor demográfico, de las distintas rutinas o actividades cotidianas asociadas a cada uno de los sectores (Alshalan, 2006;Yucedal, 2010; Pratt, Holtfreter y Reisig, 2010; Miró, 2012).

El primer estudio que utilizó la Teoría de las Actividades Cotidianas (en adelante, TAC) en relación con la victimización por cibercriminalidad social, fue el llevado a cabo por Catherine D. Marcum (2008) con una muestra de 483 estudiantes universitarios de primer año, donde su objetivo era explicar la victimización por la exposición a material sexual explícito, *harassment* y solicitudes sexuales no deseadas, a partir de la teoría de Cohen y Felson (1979). Para ello, Marcum (2008) elabora tres constructos: exposición al delincuente motivado, objetivo adecuado y guardián capaz. Respecto al primer constructo, exposición al delincuente motivado, Marcum (2008: 5) entiende que "hay sitios que están más habitados por delincuentes motivados que otros" y que, por lo tanto, acceder a ellos puede aumentar la probabilidad de ser víctima. Para ello, pregunta a los estudiantes el número de horas relativas al tiempo pasado en Internet (en general, usando el correo electrónico, la mensajería instantánea, el uso de *chat rooms* y usando redes sociales) y el tipo de actividades que suelen realizar (buscar información, jugar, planificar viajes, visitar *website designs*, comprar, socializar con otros y otras actividades). En cuanto al objetivo adecuado, lo operativiza como el grado de privacidad de las cuentas de redes sociales, la información facilitada a otras personas y la información publicada en las redes sociales. Por último, el guardián capaz lo conceptualiza como la cantidad de supervisión experimentada por los encuestados. Esto es, el lugar donde hace uso de Internet (en casa –el salón, la habitación, con los padres o vigilantes, etc.-, en el colegio, en casa de amigos, *coffee shops*, etc.), si tiene

restricciones de uso de Internet y sistemas de control como los bloqueadores de software.

Los resultados muestran que la TAC, tal y como es concretada para su investigación por la autora, puede explicar la victimización por cibercrimen, si bien con ciertos matices. El estudio identifica distintos predictores para las diferentes formas de victimización: para la exposición a material sexual explicito lo serían comprar, pasar horas a la semana en *chats rooms*, facilitar información personal a través de Internet, tener más privilegios en el acceso a Internet por parte de los padres y ser de raza blanca; para el *harassmen*t encuentra que los mayores predictores son usar Internet para socializar, el número de horas a la semana dedicado al correo electrónico, proporcionar información personal y tener el deseo de tener éxito en la escuela; por último, para la victimización consistente en recibir solicitaciones de contacto sexual, serían proporcionar información personal, usar Internet en lugares distintos al hogar, la escuela, en casa de amigos o en un *coffee shop*, y tener privilegios por parte de los padres para el uso de Internet. En cambio, compartir los sentimientos con los amigos y tener respeto por los profesores constituirían factores de protección.

En sentido similar, Holt y Bossler (2009) también realizaron un estudio con 788 universitarios para determinar los predictores del *online harassment* a partir de la TAC. Elaboraron dos constructos similares a los que planteó Marcum (2008), exposición al delincuente motivado y guardián capaz, pero distinguiendo entre el guardián físico, que son los diferentes programas destinados a la protección (antivirus, Spybot, Ad-Aware, *firewall*, *hardware firewall*, Microsoft Update, etc.), y el guardián social, que lo identifican con los amigos con comportamiento antisocial en la Red. En cuanto a la exposición al delincuente motivado, examinan también las horas pasadas en Internet realizando distintas actividades (comprar, jugar, usar el correo electrónico, redes sociales, etc.) e incluyen como novedad la evaluación de la velocidad de conexión a Internet; si el ordenador que se usa con mayor frecuencia es compartido; las horas que se dedican a usar el ordenador para el trabajo, la escuela y el ocio con el fin de comprobar la integración del ordenador en la vida rutinaria; la habilidad informática y el comportamiento desviado por los propios usuarios. Los resultados, de nuevo, son sólo en parte confirmatorios de las hipótesis de partida. De todos los indicadores medidos, solo resultan ser significativos el uso de las salas de chat, comportase de forma desviada

(concretamente, haciendo *hacking*) y tener amigos que realizan también comportamientos desviados. Tras estos resultados concluyeron que no es pasar más tiempo en Internet lo que aumenta el riesgo de ser victimizado, sino lo que se hace durante ese tiempo en el ciberespacio, por ejemplo, acceder a los contextos específicos frecuentados por agresores. Por otro lado, que el constructo guardián físico no resulte ser un indicador de riesgo, los autores lo justifican diciendo que los resultados son lógicos, pues no tienen como fin evitar este tipo de ataques, sino aquéllos relacionados con *software* malicioso. Finalmente, también resulta ser un indicador de riesgo el hecho de ser mujer, que lo identifican como una cualidad para convertirse en un objetivo adecuado.

Más recientemente Marcum, Ricketts y Higgins (2010) han publicado otro estudio usando la misma muestra del estudio de Marcum (2008), pero esta vez dividen la muestra entre hombres y mujeres y realizan los análisis por separado, para comprobar el efecto de las actividades cotidianas en cada uno de los grupos, aunque partiendo de tres hipótesis comunes a los dos: 1. los individuos que más tiempo pasan en Internet son más propensos a ver víctimas; 2. aquéllos que proporcionan más información personal a los contactos en línea son más propensos a ser victimizados; y 3. los adolescentes que usan el software de protección son menos propensos a ser víctimas. Los resultados muestran que los indicadores varían para cada una de las formas de victimización, pero también en función del sexo. A nivel general, la exposición a delincuentes motivados tiene un impacto considerable para la victimización en ambos grupos, especialmente, el uso de salas de chat, de correo electrónicos y de la mensajería instantánea. Las conductas de suministrar información personal, comunicarse con desconocidos y facilitar información personal a otros a través de las redes sociales, entendidas como características del objetivo adecuado, resultaron ser especialmente peligrosas, sobre todo para las mujeres. Respecto a la tutela capaz, como era de esperar, el software de protección no tuvo ningún efecto, pero sí la vigilancia por parte de otra persona mientras se hace uso de Internet y las propias restricciones impuestas por lo padres, tanto para los chicos como para las chicas.

Reyns (2010), por su parte, realizó un estudio con 974 estudiantes universitarios entre 18 y 24 años para determinar los riesgos asociados al *cyberstalking*, entendido éste como la suma de cinco formas de *online harassment* que también analiza por separado

(contacto repetido no deseado, haber sido hostigado (*harassed*) repetidamente, recibir insinuaciones sexuales no deseadas, haber sido amenazado con violencia y el robo de identidad (*identity fraud)).* Incluye los constructos vistos hasta ahora: exposición al delincuente motivado, el cual mide atendiendo al tiempo pasado en Internet y el tipo de actividades realizadas; el objetivo adecuado, atendiendo a los distintos tipos de información que se publican en las redes sociales; el guardián capaz, que lo identifica con la privacidad de las cuentas en redes sociales y blogs, y programas que rastrean los usuarios que acceden a las cuentas de redes sociales; y añade un cuarto elemento, la proximidad, al entender que las personas que frecuentan lugares con agresores tienen más probabilidad de ser victimizados, y que en el estudio se operativiza como agregar a extraños a las redes sociales, número total de amigos agregados y hacer uso de páginas para buscar amigos.

Los resultados relativos a la relación entre la exposición al delincuente y la victimización no fueron consistentes, aunque sí se encontraron relaciones significativas entre el número de veces que se actualiza el sistema operativo y la victimización por recepción de propuestas sexuales no deseadas, así como entre el número de cuentas de usuario y la victimización por contacto no deseado y por *cyberstalking.* Respecto al elemento guardián capaz, los programas que rastrean perfiles resultaron ser un alto predictor para cuatro formas de victimización (el contacto no deseado, las insinuaciones sexuales no deseadas, el hostigamiento y el *cyberstalking*), resultado que el autor atribuye a un "problema de temporalización", en el sentido de que quienes suelen hacer uso de tal software es porque, anteriormente, han sido victimizados. De todos los indicadores medidos en el estudio, el que más incrementa la probabilidad de ser victimizado es la proximidad, en concreto, admitir extraños y hacer uso de webs destinadas a hacer amigos. En cuanto al resto de variables incluidas, el elemento objetivo adecuado no consigue explicar la victimización, pero sí las medidas de comportamiento desviado. Finalmente, en cuanto a las variables sociodemográficas, ser mujer también resultó ser un predictor para el contacto no deseado, el hostigamiento, la solicitud de sexo y para el *cyberstalking.*

Finalmente, Ngo y Paternoster (2011) realizaron un estudio con 295 estudiantes en el que, además de formas de victimización económica, estudiaron la exposición no deseada a material pornográfico, recibir solicitudes sexuales, *harassment* por

desconocidos, *harassment* por conocidos y difamación en línea. De nuevo, estos autores incluyen los tres constructos: exposición al delincuente motivado, objetivo adecuado y guardián capaz. De modo similar a anteriores trabajos, se incluye, dentro del objetivo adecuado, la comunicación con extraños y proporcionar información personal. Respecto al guardián capaz, estos autores distinguen dos, tal y como hacen Holt y Bossler (2009): guardián físico, que identifican con el software de seguridad (antivirus, antiespía y cortafuegos), y guardián social, quizás más cercano a la idea de guardián del objetivo propuesto por Eck (1994), e incluso a la de "autoguardián", pues lo definen como la habilidad en el manejo de los equipos informáticos y como haberse formado sobre los riesgos en Internet, bien asistiendo a cursos o bien autoformándose mediante páginas de Internet. Además de estas variables, incluyeron otras seis a las que denominaron variables control y hacen referencia al sexo, la edad, la raza, el estado civil, la situación laboral y el comportamiento desviado.

Los resultados mostraron, en primer lugar, que el número de horas usando la mensajería instantánea, indicador del constructo delincuente motivado, fue el único predictor de la victimización, aunque exclusivamente del *harassment* realizado por extraños. En segundo lugar, ninguno de los indicadores del objetivo adecuado resultaron buenos predictores de la cibervictimización social. Por último, en cuanto al constructo de tutela capaz, resultaron ser predictores, por una parte, del *harassment* por extraños, tener software de seguridad y, por otra, de la victimización por exposición no deseada a material pornográfico, el hecho de haberse formado acerca de los riesgos de Internet. Llama la atención que se hayan encontrado los mismos predictores que en estudios anteriores, así como que las variables control sean las que mayor peso predictivo presentan. Concretamente, la edad, relacionada inversamente con la victimización, y estar desempleado, resultaron ser los factores de riesgo más fuertes de sufrir *harassment* por parte de extraños. De sufrirlo por parte de una persona conocida y por la exposición a material pornográfico no deseado, el mayor predictor fue el comportamiento desviado.

La recapitulación de las conclusiones de los estudios existentes hasta la fecha, cuyo análisis pormenorizado es imposible aquí, podría ser que la TAC, tal y como ha sido operativizada hasta la fecha por los autores, apenas explica la victimización por cibercriminalidad social en Internet. Todos los estudios muestran la relevancia de algunos ítems construidos a partir de este enfoque, especialmente en lo relativo a que un

mayor uso de las TIC conllevaría una mayor cibervictimización; pero del mismo modo, en todas las investigaciones, alguno de los constructos no funciona para la explicación de la victimización por estas formas de delincuencia. Ya se ha dicho que esto podría explicarse si se acepta, como se debe, que la TAC es sólo un ángulo de visión, pero no el único para explicar la victimización delictiva. Pero, además, quizás la TAC, cuyas especificaciones concretas fueron pensadas para crímenes en el espacio físico, deba ser repensada para su explicación del delito ejecutado en ese nuevo ámbito de intercomunicación personal que es el ciberespacio.

2.2. De las actividades cotidianas a las actividades cotidianas en el ciberespacio: Del VIVA al ISI

Quizás el gran mérito de la TAC sea que implica una amplificación de la visión criminológica en aras de la adopción de más amplias técnicas para la prevención del crimen. La afirmación, cercana a la obviedad, de que el delito se comete en la presencia de un agresor, una víctima y la ausencia de vigilantes que la eviten, conlleva la constatación de que se pueden adoptar estrategias de prevención centradas en la reducción de las víctimas potenciales y en el incremento de los vigilantes, todo en aras de influir en la decisión racional del atacante. El corolario directo de esto no sólo es la prevención situacional, sino también la identificación y desarrollo de los factores relacionados con la cotidianeidad que hacen de alguien o algo un objeto potencialmente más o menos adecuado. En este sentido, Clarke (1999) formula el acrónimo CRAVED como reflejo de que un objetivo es adecuado cuando se puede esconder fácilmente (*concealable*), se puede trasladar con facilidad (*removable*), está disponible (*available*), tiene valor (*valuable*), tiene valor de disfrute (*enjoyable*) y es fácil deshacerse del artículo (*disposable*). Por su parte, Felson (1998) con el acrónimo VIVA entiende que para que un objetivo sea considerado adecuado debe tener valor desde la perspectiva del delincuente (*value*), inercia, visibilidad física y accesibilidad.

También en el ciberespacio el crimen se produce cuando hay un agresor, una víctima y la ausencia de un guardián capaz. Pero, como analicé anteriormente en otros trabajos (Miró 2011 y 2012), la evidente diferencia de estructura física entre el espacio físico y el ciberespacio conlleva cambios significativos en la relación entre los distintos

elementos del crimen y, por tanto, en los elementos configuradores de un objetivo como adecuado en el ciberespacio, frente a los que hacen a un objetivo adecuado en el espacio físico. En otras palabras, las rutinas, la cotidianeidad de las relaciones interpersonales, también existen en el ciberespacio, pero se manifiestan de forma distinta, por lo que es necesario, a la hora de construir las variables predictoras de riesgo de victimización, pensar más en una TAC en el ciberespacio que en una mera traslación de los elementos clásicos de una teoría pensada para la explicación del crimen en el *meatspace.*

Cuando Clarke habla de *conceable o removable* está, obviamente, pensando en objetos físicos que, por características intrínsecas, pueden ser desplazados u ocultados. Los objetos en el ciberespacio también se desplazan u ocultan pero, esto es innegable, el significado y valor de tales acciones es diferente al del espacio físico. Algo similar sucede con el término *inertia* utilizado por Felson como parte del acrónimo VIVA: con él hace referencia al tamaño y al peso del objeto, que funcionan como obstáculos o impedimentos para que el delincuente lo vea como adecuado, y aunque podríamos pensar en equivalencias como el volumen de un servidor para un ataque DoS o como apunta Yar (2005), el tamaño de un fichero para ser descargado, es claro que la mayoría de estos objetos no se suelen diferenciar por estos valores entre sí. Lo mismo sucede cuando habla de accesibilidad, entendida como la habilidad de un agresor para contactar con un objetivo y llevárselo de la escena del crimen. Si tenemos en cuenta que en el ciberespacio las distancias desaparecen, es decir, no hay que recorrer una distancia como se entiende en el espacio físico, todos los bienes introducidos en el ciberespacio son accesibles para los potenciales agresores.

A mi parecer, la TAC puede servir para explicar la victimización en el ciberespacio siempre que se asuman las nuevas características del ámbito de oportunidad criminal en el que van a relacionarse agresores, víctimas, guardianes y gestores y que, por tanto, se construyan las variables de riesgo a partir de los nuevos caracteres de los objetivos adecuados para la victimización en Internet. Y, tal y como desarrollé más ampliamente en otro lugar, los caracteres que hacen a un objeto adecuado para la victimización son el que haya sido introducido en el ciberespacio, su visibilidad que dependerá de la interacción del usuario titular del mismo y, por supuesto, su valor para el agresor motivado (Miró 2011).

El ciberespacio es un ámbito de comunicación paralelo al espacio físico, pero en el que los objetos, bienes y acciones tienen que ser introducidos en él. Mientras que en el espacio físico se está, en el ciberespacio se puede estar o no. Y lo mismo sucede con los bienes y objetos, con la intimidad, con el patrimonio, con el honor. La decisión de acceder o de introducirse en el ciberespacio no siempre es voluntaria. En muchas ocasiones serán las acciones de terceros o acciones involuntarias nuestras, las que conllevarán la introducción de nuestra imagen, de nuestra privacidad, etc. Pero en muchas ocasiones, sí será nuestra propia actividad rutinaria la que determine qué se introduce en el ciberespacio. Y lo que es indudable, de ahí que sea el primer elemento de la victimización en el ciberespacio, es que si los bienes de una persona, ya sean referentes al patrimonio, a la intimidad, a la libertad sexual, etc., no son introducidos en Internet, éstos no estarán disponibles y por tanto, no podrán ser objeto de ataque por parte de un delincuente.

Que los bienes sean introducidos, de forma voluntaria o no, de por sí ya conlleva una exposición de los mismos a un riesgo. Pero sólo serán objetivos adecuados cuando se conviertan en visibles para el agresor. Dice Yar (2005) que el ciberespacio es de carácter público y que por lo tanto, todos los objetivos son en sí visibles a nivel mundial. El que eso sea así es lo que precisamente, conlleva que todos puedan pasar, en principio, desapercibidos para los agresores. Lo serán, pese a haber sido introducidos en el ciberespacio si permanecen "quietos", si no se comunican ni se relacionan con otros, pues es esa comunicación y contacto entre usuarios la propia esencia de Internet. De este modo, podemos decir que aquello que convierte a un objetivo en visible para otros en el ciberespacio es su interacción, o más bien la de su titular, esto es, el establecer comunicación con otros usuarios a través de las múltiples herramientas que ofrece Internet (correo electrónico, chat, foros, mensajería instantánea, redes sociales, etc.) y hacer uso de otros servicios, como comprar, descargar archivos, ver vídeos, realizar movimientos bancarios, etc. A mayor interacción, mayor visibilidad, mayor contacto con múltiples usuarios y por tanto, con potenciales agresores.

Estos dos elementos, introducción e interacción, definen la adecuación de un objetivo en el ciberespacio desde la perspectiva del potencial agresor. También lo hace, lógicamente, el valor que para éste tenga el bien o interés de que se trate. Desde la postura en la que nos estamos basando, sin embargo, consistente en identificar las

actividades cotidianas de la víctima que pueden incrementar el riesgo de victimización en Internet, es evidente que el valor del objeto debería ser descartado. Dependiendo de cada cibercrimen el valor tendrá relevancia o no, y si además tenemos en cuenta que los bienes en el ciberespacio son informacionales y que puede darse la paradoja de que bienes de escaso valor material pueden tener un gran valor para el agresor, parece claro que este elemento no será indicador valioso en el ciberespacio de la adecuación de un bien para ser objeto de cibercrimen.

Por el contrario sí lo será el que el bien esté o no protegido, lo cual en la gran mayoría de los estudios, a mi parecer erróneamente, se incluye como indicador del constructo "guardián capaz". Cuando Cohen y Felson (1979) hablan de guardián capaz hacen referencia a aquél que, con su simple presencia, hace disminuir el riesgo de que se cometa el delito o que, con su ausencia, hace que sea más probable que se lleve a cabo. En el espacio físico, los autores hacen alusión tanto a los vigilantes formales (policía o personal de seguridad) como a cualquier persona que pueda proteger las propiedades propias o ajenas. Más tarde, es el propio Felson (1995) quien hace una reformulación en la que acaba distinguiendo entre el supervisor íntimo, que sería la persona que por medio de la desaprobación del comportamiento del potencial delincuente hace que el delincuente no realice las actividades delictivas, y el gestor del espacio, que es el que tiene la responsabilidad de supervisión sobre determinados espacios. En parte esto ya había sido adelantado por Eck (1994), quien diferenciaba entre los elementos que son necesarios para el delito (delincuente, objetivo y lugar) y los controladores, que son aquéllos que tienen el potencial de prevenirlos y entre los que se encuentran el *handler*, que tiene una relación con el delincuente y cuyo objetivo es alejarlo de los problemas; el *manager* que es el encargado de proteger el lugar; y los guardianes, que tienen como fin concreto la protección del objetivo.

A mi parecer, tanto los guardianes capaces como los *managers*, son elementos esenciales de la futura prevención situacional del cibercrimen (Miró, 2011). De hecho, es clave comprender cómo cambia la oportunidad criminal en el ciberespacio para determinar nuevas obligaciones a los diferentes prestadores de servicios, incluso a los usuarios, para convertirlos en eficaces protectores de terceros frente al cibercrimen. Pero a la hora de identificar los factores relacionados con las actividades cotidianas de la víctima, que van a incidir en su cibervictimización, más que la actuación de

guardianes y de gestores del lugar, lo relevante es la propia actuación de la víctima en su propia protección. Los autores antes mencionados que han tratado de aplicar la TAC a la cibervictimización (Holt y Bossler, 2009; Marcum, Ricketts y Higgins, 2010; Ngo y Paternoster, 2010), han identificado como guardianes capaces a los distintos programas de seguridad (antivirus, antiespías, cortafuegos, etc.), que sirven para evitar múltiples formas de ciberdelito. Sin embargo, estos tipos de hardware son más bien elementos que, para ser funcionalmente aptos, deben haber sido incorporados al propio objeto y, en muchos casos, por el propio sujeto. Se trata de elementos que, por lo tanto, conceptualmente, definen la propia adecuación del objeto y no su tutela externa, por lo que en realidad estaríamos más bien ante elementos o características del objetivo adecuado. A esto es a lo que denominamos "autoprotección" o, para facilitar el acrónimo, directamente en inglés, *self protection*, en cuanto a que un objetivo será más adecuado para el agresor cuando menos protegido esté por la no incorporación de software del tipo "anti virus", pero también por rutinas de riesgo tales como usar virus pirata o no actualizar el sistema operativo.

De esta forma, pasamos del acrónimo VIVA al acrónimo ISI (Introduction, Self-protection, Interaction). La adecuación de un bien u objeto en el ciberespacio dependerá de que haya sido introducido en Internet (lo cual en ocasiones será determinado por las propias acciones de la potencial víctima), de que esté más o menos protegido, y de la interacción del usuario que lo haga accesible y visible a los potenciales agresores motivados.

2.3. Hipótesis

El presente estudio pretende definir un modelo predictivo que, además de dar explicación a este fenómeno, pueda ayudar a determinar el riesgo de victimización de un usuario concreto a partir de las actividades cotidianas que realice en el ciberespacio. Parto, por tanto, de la reconceptualización de la TAC, tal y como he plateado en el apartado anterior, teniendo en consideración los estudios anteriormente citados, que utilizan el constructo de las actividades cotidianas para la victimización social, así como otras investigaciones que parten de tal teoría para analizar otras formas de victimización que afectan al patrimonio de los usuarios (Choi, 2008; Bossler y Holt, 2009; Pratt, Holtfreter y Reisig, 2010; Yucedal, 2010; Ngo y Paternoster, 2011).

En vista, pues, del panorama científico y de la necesidad de ahondar en la determinación de los factores de riesgo de victimización relacionados con las actividades cotidianas pero a partir del prisma del nuevo ámbito de oportunidad criminal que es el ciberespacio, se ha planteado un estudio que tiene como objetivo principal explicar qué actividades cotidianas en el ciberespacio incrementan el riesgo de victimización por estas formas de *cyberharassment*. Con tales fines y a partir de los apoyos empíricos y teóricos comentados y discutidos, son tres las hipótesis de partida para la realización del estudio. La primera de ellas, es la relativa a la introducción de bienes en el ciberespacio, pues como se ha argumentado en el apartado anterior, el hecho de que al ciberespacio se ha de entrar conlleva que sea necesario que los objetivos sean introducidos de manera voluntaria o involuntaria, quedando la hipótesis formulada como: cuanto mayor sea la introducción de objetivos en el ciberespacio, mayor será el riesgo de victimización. La segunda hipótesis planteada parte de la idea de que el usuario define con su interacción en el ciberespacio el grado de visualización de sus objetivos previamente introducidos, es decir, se harán más o menos perceptibles para los agresores en función de la interacción, siendo por tanto su formulación la siguiente: cuanto mayor sea la interacción en el ciberespacio, mayor será el riesgo de victimización. Por último, la tercera hipótesis está relacionada con la idea que la protección en el ciberespacio pasa por la propia protección de la víctima ante los posibles ataques como ya he argumentado antes, quedando así: cuanto menor sea la autoprotección, mayor será el riesgo de victimización.

3. Metodología

3.1. Muestra

La muestra del estudio estuvo formada por 500 participantes españoles mayores de edad, de los cuales 222 (44,4%) resultaron ser hombres y 278 (55,6%) mujeres, con una media de edad de 40,21 años (DT=12,57). Se estableció el mínimo de edad en 18 años con la intención clara de salvar los problemas que presenta obtener datos de menores de edad. Además se situó el límite máximo en 65 años, ya que el porcentaje de usuarios de Internet mayores de 65 años es muy bajo (Instituto Nacional de Estadística, 2011). Para seleccionar los sujetos se llevó a cabo, un muestreo probabilístico estratificado por sexo,

edad y comunidad autónoma. Los criterios de inclusión de los participantes fueron 1) utilizar Internet un mínimo de 8 horas semanales y 2) tener un máximo de 65 años, por la razón anteriormente expuesta (INE, 2011).

3.2. Variables

La variable dependiente "cibervictimización por *online harassment"*, de naturaleza categórica y dicotómica, fue obtenida a partir de las respuestas dadas por los encuestados a seis preguntas de victimización por *online harassment.* Las conductas sufridas que certifican la victimización son: haber recibido contacto repetido de alguien después de haberle pedido que no lo hiciera; haber sido amenazado gravemente; haber sido intimidado con revelar información dañina o con causarle algún mal; haber sido objeto de la publicación sin su consentimiento de información personal; haberse usado su imagen o haberse suplantado su identidad; y haber sido injuriado o haberse vertido acusaciones falsas sobre su persona. Cuando los encuestados respondían afirmativamente a haber sufrido alguna de estas conductas, eran categorizados en la variable dependiente como "víctima". En cambio, aquellos participantes que no sufrieron ninguna de estas conductas fueron categorizados como "no víctima".

Las variables independientes incluidas fueron creadas por medio de la revisión de la TAC en el ciberespacio: "introducción", "interacción" y "autoprotección".

La "introducción" hace referencia a los bienes que una persona traslada, de forma voluntaria o involuntaria, del mundo físico al virtual (ciberespacio). Para su medida, se creó una escala con los siguientes nueve ítems de respuesta dicotómica (Sí, No): tener en el ordenador con el que se conecta a Internet un archivo con contraseñas, fotos personales, fotos íntimas, vídeos personales, información sensible de la empresa, usar datos personales reales para abrir cuentas en redes sociales, facilitar información personal real a través de redes, facilitar información personal real a través de foros y facilitar contraseñas. La puntuación total en la variable se obtiene a partir de la suma de las respuestas en cada uno de los ítems (Sí=1, No=0), pudiendo alcanzar como máximo un valor de 9 puntos.

La variable "interacción" ha sido operativizada en dos variables, distinguiendo entre las actividades propias de comunicación a través del ciberespacio y las relativas a la comunicación con personas desconocidas. Así, se entiende por "interacción personal"

las acciones que realiza una persona dentro del ciberespacio para comunicarse con otras personas que le convierten en un usuario visible o, en otros términos, más conectado con los demás. Se creó una variable numérica a partir de la suma de las respuestas ofrecidas por los usuarios en 9 ítems, teniendo en cuenta que el rango de medida es dicotómico (1=si, 2=0). Los ítems fueron: uso del correo electrónico, salas de chat, mensajería instantánea, redes sociales, foros, hacer videoconferencia, descargar archivos, consumir pornografía y jugar videojuegos *online*. La variable "interacción con extraños" hace referencia a las acciones que lleva a cabo un usuario de Internet para contactar con desconocidos. Esta variable numérica se ha creado a partir de la suma de las respuestas ofrecidas por los encuestados a 5 ítems dicotómicos: usar webs de contacto, contactar con extraños a través de las redes sociales, contactar con extraños a través de la mensajería instantánea, abrir o descargar enlaces o archivos enviados por desconocidos a través del correo electrónico, y abrir o descargar enlaces o archivos enviados por desconocidos a través de la mensajería instantánea.

Finalmente, y en cuanto a la variable "autoprotección", se ha optado por darle una dirección negativa con el fin de ajustar los resultados a la tercera hipótesis planteada. Así, "no autoprotección" son las acciones que no lleva a cabo un usuario de Internet para proteger sus bienes. La variable se creó a partir de la suma de las respuestas obtenidas en 5 ítems dicotómicos: no tener antivirus, usar software pirata, usar la misma contraseña para todo, no cambiar sus contraseñas como mínimo una vez al año y tener las cuentas públicas.

Además de las variables descritas se incluyeron variables sociodemográficas, en concreto, la variable "sexo" referida al género de los encuestados y que fue codificada 1=hombre y 2=mujer, y la edad que fue evaluada en años.

3.3. Instrumentos de análisis

Para el estudio se elaboró una encuesta *ad hoc* en la que, para asegurar la validez de contenido, intervinieron profesionales de distintos ámbitos (juristas, criminólogos y metodólogos) con el fin de desarrollar un instrumento con el mayor rigor posible. La encuesta se componía de cuatro tipos de preguntas. Una pregunta filtro, "¿cuántas horas a la semana pasa conectado a Internet?" con el objetivo de incluir en el estudio sólo a aquellos sujetos que se conectan a Internet al menos 8 horas a la semana; a continuación

se incluyeron tres preguntas sobre características sociodemográficas (sexo, edad y comunidad); después una serie de preguntas sobre actividades cotidianas en Internet; y por último, se incluyeron catorce preguntas sobre cibervictimización económica y social de las que, para el presente artículo, sólo tomaré en consideración las relativas a la victimización social que conforman el *online harassment.* Además, para garantizar el correcto funcionamiento del instrumento, se realizó un pilotaje con 100 sujetos representativos de la muestra total que sirvió para llevar a cabo los análisis pertinentes que confirmaban la idoneidad de las preguntas elaboradas.

Para la recogida de información se contrataron los servicios de una empresa externa (Investgroup), que llevó a cabo la administración telefónica de la encuesta asistida por ordenador mediante el sistema CATI (Computer Assisted Telephone Interviewing), contemplando tanto teléfonos fijos como móviles. Este sistema minimiza los costes del proyecto respecto a otros sistemas de recogida de datos, como la entrevista cara a cara, y los estudios metodológicos han demostrado que, de manera general, las respuestas a preguntas de victimización mediante entrevistas telefónicas son similares a las obtenidas "cara a cara" (Van Dijk y Mayhew, 1992; Lynch y Addington, 2007; Catalano, 2007). La duración de cada administración osciló entre los 8 y los 15 minutos y se llevó a cabo entre el 1 y el 15 de octubre de 2012.

3.4. Técnicas de análisis

Para el análisis de los datos se utilizó el paquete estadístico SPSS v. 19.0. Se llevaron a cabo, en primer lugar, análisis descriptivos de todas las variables consideradas (dependiente, independientes y sociodemográficas), obteniendo la frecuencia y porcentaje para las variables dicotómicas y los estadísticos mínimo, máximo, media, mediana, desviación típica, varianza y el test de Kolmorov-Smirnov para una muestra para todas las variables cuantitativas.

En segundo lugar, se aplicaron análisis bivariados. Se utilizó el estadístico *U* de Mann-Whitney para estudiar la diferencia de las puntuaciones obtenidas en cada una de las variables independientes ("introducción", "interacción personal", "interacción con desconocidos" y "no autoprotección") entre víctimas y no víctimas por *online harassment.*

Para alcanzar los objetivos del estudio, se han llevado a cabo análisis descriptivos de las variables, análisis bivariados y la construcción de un modelo de regresión logística múltiple, al ser los más adecuados para los objetivos propuestos.

4. Resultados

Por lo que respecta a la variable dependiente, los análisis descriptivos muestran, en primer lugar, que un 21% (n=105) de los participantes ha sufrido alguna de las formas concretas de *online harassment.*

Analizando los datos obtenidos de forma concreta, se puede observar cómo la conducta de "publicar información sin el consentimiento de la persona", es la que con mayor frecuencia se repite, encontrándose que un 10,2% (n=51) de los encuestados dice haberlo sufrido al menos una vez. Siguiendo el orden, "haber recibido contacto repetido de alguien cuando se le ha pedido que no lo haga" es la siguiente conducta más sufrida (10%, n=50), seguido de "haber sido amenazado gravemente" (3,2%, n=16), "usar su imagen o suplantar su identidad" (3,2%, n=16), "vertido acusaciones falsas sobre su persona o injuriado" (1,2%, n=6) y "haberse sentido intimidado" (1%, n=5).

Tabla 1. Prevalencia de *online harassment en la muestra*

CIBERVICTIMIZACIÓN *ONLINE HARASSMENT*	**21% (n=105)***
Publicar información sin consentimiento	10,2% (n=51)
Contacto repetido no deseado	10% (n=50)
Amenazas	3,2% (n=16)
Suplantación de identidad	3,2% (n=16)
Injurias	1,2% (n=6)
Intimidar	1% (n=5)

*****El porcentaje de cibervictimización por *online harassment* corresponde al porcentaje de sujetos de la muestra que ha sufrido al menos alguna de las conductas incluidas dentro la categoría. Hay que tener en cuenta, por tanto, que una misma persona puede haber sufrido más de una conducta.

Los análisis descriptivos realizados sobre las variables independientes muestran, tal y como se observa en la Tabla 2, que existe cierta variabilidad en cuanto a la realización de acciones de introducción de información personal en el ciberespacio, ya que las respuestas de los participantes oscilaron entre los valores 0 y 8, con una media de 2,8 (D.T.=1,5). Parece existir una tendencia mayor en cuanto a la realización de acciones para la comunicación con los demás, siendo la media de la variable "interacción personal" de 3,8 (D.T.=1,7). Sin embargo, no existe ningún participante de la muestra que haya respondido afirmativamente a todas y cada una de las conductas incluidas en la variable "interacción con extraños", mostrando los datos, en general, una baja variabilidad, y siendo la media de 1,2 (D.T.=0,6). Finalmente, los resultados de la variable "no autoprotección" indican que una parte de los usuarios de Internet encuestados no lleva a cabo ninguna acción para proteger sus bienes, habiéndose obtenido una puntuación media de 1,6 (D.T.=1,1). En cuanto a los resultados de la prueba K-S para analizar la normalidad de la variable, los mismos muestran que ninguna de las variables se distribuye normalmente, razón por la cual se ha elegido, para el análisis bivariado, utilizar la prueba no paramétrica *U* de Mann-Whitney.

Tabla 2. Variables independientes (descriptivos)

VARIABLES INDEPENDIENTES	n	$\bar{X}$	D.T.	S^2	Mín	Máx	*Z* de K-S (*p*)
Introducción	500	2,8	1,5	2,5	0	8	2,802 (0,000)
Interacción personal	500	3,8	1,7	3,0	0	9	2,562 (0,000)
Interacción con extraños	500	1,2	0,6	0,4	0	4	10,600 (0,000)
No autoprotección	500	1,6	1,1	1,2	0	5	4,148 (0,000)

Los resultados del análisis bivariado que aparecen en la Tabla 3 indican que se encontraron relaciones significativas entre la variable dependiente y tres de las cuatro variables independientes analizadas. Concretamente, son las personas victimizadas las que más objetivos introducen ($U_{M\text{-}W}$= 15803,00; p=0,000), las que más actividades de interacción personal realizan ($U_{M\text{-}W}$= 13973,00; p=0,000) y las que más interactúan con

extraños ($U_{M\text{-}W}$= 15655,00; p=0,000) en comparación a lo que los participantes evaluados como no víctimas realizan, siendo, por lo tanto, más visibles en el ciberespacio que estos últimos. En cambio, no se encontraron diferencias significativas en cuanto a lo que víctimas y no víctimas realizan para proteger sus bienes ($U_{M\text{-}W}$= 18633,00; p=0,097). A pesar de que este último análisis no arroja resultados estadísticamente significativos, la variable "No autoprotección" se propuso como predictora en los análisis de regresión debido a que se trata de un factor fundamental en el modelo teórico propuesto y debido también a que pueden existir patrones de asociación entre las variables cuando se contemplan en conjunto, tal y como ocurre en la realidad, que puedan resultar, a ese nivel, relevantes para la predicción del fenómeno modelizado, por lo que, para poder obtener una descripción completa de la influencia de cada variable sobre la probabilidad de que la persona sea victimizada, se ha considerado oportuno incluir en el modelo todas las variables independientes evaluadas.

Tabla 3. Relación entre las variables independientes con la variable dependiente

VARIABLES INDEPENDIENTES	***U***	***p***
Introducción	15803,00	0,000
Interacción personal	13973,00	0,000
Interacción con extraños	15655,00	0,000
No autoprotección	18633,00	0,097

Finalmente, con el objetivo de determinar el peso de las variables que afectan a la victimización por *online harassment* y establecer un modelo predictivo de victimización, se realizó un análisis de regresión logística múltiple. Dado el carácter exploratorio de los objetivos de esta investigación y la falta de modelos robustos previos que analicen de forma conjunta las variables abordadas en el mismo, se optó por seleccionar un método simultáneo (Introducir) a partir del cual no se prioriza el orden de entrada de las variables, pudiendo analizar así su influencia cuando todas entran a formar parte del modelo a la vez.

Como se puede observar en la Tabla 4, las variables incluidas mejoran significativamente el modelo nulo (χ^2 =50,773; p=0,000) y el estadístico χ^2 de Hosmer-Lemeshow muestra que el modelo ofrece un buen ajuste a los datos (χ^2= 7,692; p= 0,464). Finalmente, el coeficiente de determinación generalizado R^2 de Nagelkerke presenta un valor de 0,15, una vez incluidas en el modelo las cuatro variables predictoras. Partiendo de una probabilidad umbral o de corte de P(Y=1)=0,5, el porcentaje global de clasificación correcta fue del 79,8%, y mejoró el porcentaje de clasificación correcta para víctimas y no víctimas (79,8% y 97,7% respectivamente).

Tabla 4. Modelo

MODELO	
Omnibus	Paso: χ^2= 50,773 (p= 0,000) Bloque: χ^2= 50,773 (p= 0,000) Modelo: χ^2= 50,773 (p= 0,000)
-2LL	463,183
R2 Cox y Snell	0,097
R2 Nagelkerke	0,150
Hosmer y Lemeshow	χ^2= 7,692 (p= 0,464)
Clasificación	Global: 79,8% No víctima: 97,7% Víctima: 79,8%

En la Tabla 5 se puede observar que todas las variables introducidas ("introducción", "interacción personal", "interacción con extraños" y "no autoprotección") tienen un peso significativo en el modelo (p <0,05), de manera que aquellos sujetos que introducen más objetivos en el ciberespacio, se hacen más visibles a través de la interacción con otras personas (conocidos o extraños) y se protegen menos, tienen más probabilidad de ser victimizados. Teniendo en cuenta las *odd ratio*, por cada unidad de aumento en la variable "introducción" hay un 72,3% (OR=2,613) más de probabilidades de ser victimizado por *online harassment*. Del mismo modo, por

cada unidad de aumento de "interacción personal" y de "interacción con extraños", aumenta la probabilidad de ser victimizado en un 63,3% y un 55,04% respectivamente (OR=1,730 y OR=1,224). Finalmente, por cada unidad de aumento de "no autoprotección", la probabilidad de sufrir victimización es de 55,2% (OR=1,232).

Tabla 5. Variables incluidas en la ecuación

							I.C. 95% para EXP(B)		
	B	**E.T.**	**Wald**	**gl**	**Sig.**	**Exp(B)**	**Inferior**	**Superior**	**Probabilidad**
Introducción	0,961	0,333	8,331	1	0,004	2,613	1,361	5,017	72,32%
Interacción personal	0,548	0,224	5,967	1	0,015	1,730	1,114	2,685	63,3%
Interacción con extraños	0,202	0,099	4,165	1	0,041	1,224	1,008	1,486	55,04%
No autoprotección	0,209	0,093	5,078	1	0,024	1,232	1,028	1,478	55,2%
Constante	-2,705	0,365	54,795	1	0,000	0,067			

5. Discusión

La primera consideración de interés sería que el estudio muestra que la cibercriminalidad social es un fenómeno presente en la sociedad española, por lo que sería recomendable realizar un estudio con una muestra representativa para determinar con exactitud la incidencia del fenómeno en la población española. Uno de cada cinco de los usuarios encuestados ha experimentado alguna vez en su vida alguna forma de *online harassment*. Comparando los resultados obtenidos con otros estudios, podemos ver que éstos son próximos a los encontrados por otros autores. Así, Finn (2004) obtuvo valores que oscilaron entre el 10% y el 15%. Estos resultados ligeramente inferiores pueden deberse a que los mismos se obtuvieron en 2004 cuando el uso de Internet no

estaba tan extendido como lo está ahora. Mucho más cercano se encuentra el 18,9% obtenido por Holt y Bossler (2009), el 20,1% de Reyns (2010), el 20,6% obtenido por Yucedal (2010), y entre el 7,6% y el 20,9% obtenido por Ngo y Paternoster (2011).

Esta similitud de resultados de victimización por cibercriminalidad social ya no lo es tanto cuando comparamos con otros estudios los resultados de victimización para las modalidades concretas de *harassment.* En el caso de las amenazas, los porcentajes son bastante inferiores a los obtenidos por Bocij (2003), entre un 40% y un 49% frente a un 3,2%. Más cercano a éste, aunque igualmente superior, es el 4,4% obtenido por Reyns (2010). Lo mismo sucede para las injurias, donde Bocij (2003) obtiene un 24,4% y Ngo y Paternoster (2011) un 7,6% frente a un 1% en el presente estudio; para la suplantación de identidad, un 9% obtenido por Bocij (2003) en comparación al 3,2% obtenido; y el contacto repetido no deseado, donde Reyns (2010) obtiene un 23,3% frente a un 10%.

Que estos últimos resultados hayan sido tan dispares puede deberse a dos motivos. El primero de ellos, y quizás el que más peso tenga, sea debido deba a las diferencias metodológicas empleadas en los estudios, concretamente a la manera de medir la victimización. Para este estudio se han escogido conductas de *harassment* de especial entidad, y se han dejado de lado otras que, pudiendo causar molestia o perturbación a la víctima, no la convierten propiamente en tal a nuestro parecer. Es obvio, en todo caso, que todo esto se subsanaría si existieran tanto definiciones operativas como instrumentos de medida estandarizados, que permitieran la comparación directa de los resultados ya no sólo a nivel internacional, sino a nivel estatal. El segundo motivo de esta disparidad podría relacionarse con la muestra: la mayoría de los estudios emplean muestras de jóvenes universitarios mientras que en nuestro lo es la población adulta de 18 a 65 años. Hay autores, como Bossler y Holt (2009) que entienden que los jóvenes de por sí son un blanco atractivo, y hay otros como Alshalan, (2006), Yucedal (2010) y Pratt *et al.* (2010), que entendemos (Miró, 2012) que si bien la edad no determina el riesgo sino que lo hacen las actividades cotidianas asociadas a las mismas, es cierto que habrá mayor victimización por el mayor uso y exposición al ciberespacio, lo cual es más usual en jóvenes. El objetivo de nuestro estudio, de todos modos, era precisamente confirmar esta hipótesis, y por eso creemos que es preferible que el análisis abarque a toda la población adulta. Es evidente, en todo

caso, que son necesarios más estudios de este tipo y que, en particular, sería deseable una investigación similar pero realizada sobre una población de 13 a 18 años en la que, además, se les preguntara a los menores sobre sus actividades cotidianas en el ciberespacio. Analizando los resultados de tal investigación y los de ésta, y cruzando en la comparativa el tipo de uso de Internet, podríamos tener una imagen más clara tanto de la prevalencia de cibervictimización social como de las razones a las que ésta es debida.

En cuanto a la parte más relevante del estudio, la del modelo, podemos afirmar con claridad que los resultados confirman las hipótesis inicialmente planteadas. A mayor introducción de objetos e intereses en el ciberespacio, mayor interacción con usuarios conocidos y desconocidos, y menor autoprotección, mayor probabilidad de sufrir victimización. Las consecuencias que tiene esto a la hora de definir estrategias de prevención pueden ser ingentes y no todas abarcables aquí, pero trataré de reflexionar sobre algunas de ellas a partir de la constatación de los resultados del modelo en relación con cada variable.

En cuanto a la variable "introducción", ha resultado ser el mayor predictor para la victimización por *online harassment*, aumentando la probabilidad de sufrir victimización en un 72,3%. Por tanto, a mayor victimización mayor será la probabilidad de ser víctima de alguna forma de *online harassment*. Esto concuerda con la idea de que si el objetivo no ha sido introducido en el ciberespacio, el mismo no podrá ser objeto de ataque.

De cara a la prevención victimal, será importante advertir a los usuarios de los riesgos que conlleva la introducción de bienes personales en el ciberespacio. Proporcionar información personal a través de las distintas herramientas de comunicación personal que provee Internet supone un riesgo como ya habían señalado estudios anteriores (Marcum, 2008; Marcum *et al*., 2010), por lo que cabrían propuestas interesantes como la que plantea Agustina (en prensa), sobre la conveniencia de crear políticas destinadas a cambiar la cultura actual sobre el modo de compartir la intimidad con terceros. Otro de los riesgos, de los que quizás no son tan conscientes los usuarios, es que en el momento en que conectamos nuestros equipos informáticos a Internet, ya sean ordenador, *tablets* o *smartphones*, toda la información contenida en ellos pasa a estar disponible para *hackers* y otras personas desconocidas en el ciberespacio. Estos riesgos pueden ser evitados con gestos tan sencillos como guardar esa información en

discos duros externos. Por último, y en relación con el uso de datos personales para abrir cuentas en redes sociales o cuentas de correo, además de las precauciones que pueden adoptar los usuarios, sería necesario integrar en el proceso de prevención a los guardianes capaces o, más bien, a los gestores de espacios. Al fin y al cabo, el usuario no hace más que cumplimentar una información solicitada por el proveedor de servicios y es él el que, posteriormente, la hace pública o no. Teniendo en cuenta la relación existente entre esta variable y la victimización habrá que reflexionar, quizás por medio de futuros estudios más centrados en estas consideraciones, sobre el cambio de las políticas de los prestadores de esta clase de servicios en el sentido de obligarles a adoptar medidas de seguridad más estrictas o para que no sea necesario aportar tantos datos personales para hacer uso de ellas.

Ha quedado también demostrada la segunda hipótesis que planteaba acerca de que a mayor interacción, mayor será la probabilidad de sufrir *online harassment.* Al igual que los resultados obtenidos en estudios anteriores, la interacción con extraños aumenta el riesgo de victimización en un 55% (Marcum *et al.*, 2010; Reyns, 2010). Sin embargo, el contacto con extraños lo conceptualizan de forma distinta a la empleada en el presente trabajo. Marcum *et al.* (2010) entienden que el hecho de contactar con extraños supone un elemento más del objetivo adecuado, cuestión distinta a la planteada por Reyns (2010), quien entiende que agregar extraños a las redes sociales y hacer uso de páginas web destinadas a hacer amigos son un elemento de proximidad al delincuente motivado. En este sentido, el elemento proximidad podría ser discutido en tanto en cuanto en el ciberespacio las distancias desaparecen (Yar, 2005; Miró 2011) y por lo tanto, todos los delincuentes tienen la misma distancia (d=0) con respecto a las potenciales víctimas. El hecho de interaccionar, lo que va a determinar es la visibilidad de las potenciales víctimas para los agresores motivados. Lo mismo sería válido para el constructo interacción personal que otros autores han denominado exposición al delincuente motivado (Choi, 2008; Marcum, 2008; Holt y Bossler, 2009; Bossler y Holt, 2009; Marcum *et al.*, 2010; Ngo y Paternoster, 2011; Reyns *et al.*, 2011). En este sentido, y siguiendo la idea planteada por Yucedal (2010: 43), por el mero hecho de acceder al ciberespacio ya existe una exposición al delincuente motivado, al igual que sucede en el mundo físico. Lo relevante de la exposición al delincuente motivado viene determinado por la accesibilidad y la visibilidad (Cohen et al., 1981: p.507), entendida

ésta última por Cohen *et al.* (1981) como que el delincuente sabe de la existencia del blanco potencial. Con estos resultados se demuestra también que, además del tipo de actividad de interacción que se realiza en el ciberespacio, también es importante la cantidad de actividades distintas, de modo que los sujetos que más actividades de interacción realizan tienen una mayor probabilidad de sufrir alguna de las conductas de *online harassment* evaluadas.

Finalmente, la tercera variable incluida, la autoprotección, también ha resultado ser significativa, de manera que a menos acciones de protección adoptadas, mayor será el riesgo de sufrir *online harassment.* Pese a las contradicciones encontradas en los estudios referentes al uso de programas de protección, conforme a los resultados de nuestro estudio no tener antivirus y demás conductas de no autoprotección han resultado ser un elemento de riesgo al igual que en el estudio de Choi (2008) y a diferencia de lo que opinan Holt y Bossler (2009). Es cierto que estos programas están diseñados para frenar ataques de software malicioso, pero hay ataques de *harassment* que requieren de un uso de estos programas para un ataque inicial. Pensemos, por ejemplo, en el uso de troyanos para acceder a los sistemas informáticos que permite obtener información, como fotos íntimas, con las que después se puedan realizar chantajes. Las conclusiones son claras en cuanto a las estrategias de prevención: resulta necesario educar a los usuarios en el uso de programas de protección, así como advertir de los riesgos asociados al uso de software pirata, sobre la necesidad de cerrar el acceso a las cuentas de las redes sociales y respecto a lo oportuno que resulta hacer una buena gestión de las contraseñas, no usando la misma para todo y cambiándola con frecuencia. Aunque estas reflexiones ya se han hecho en otras ocasiones, casi siempre se asocian al riesgo de victimización por *hacking* o similares ciberataques, y es importante informar de que también incrementan el riesgo de sufrir *harassment.*

6. Conclusiones

6.1 Síntesis de resultados

La afirmación de que el ciberespacio es un ámbito distinto al espacio físico busca, en última instancia, la comprensión de cuáles son las claves de la conducta criminal en

Internet en aras de su mejor prevención. El presente estudio ofrece algunas de ellas. Además de aportar datos relativos a la prevalencia sobre cibervictimización por *online harassment*, viene a apoyar la tesis planteada de que la víctima es elemento clave en la producción del evento delictivo particularmente en Internet, ya que determina su propio ámbito de riesgo al incorporar determinados bienes al ciberespacio, al interaccionar con otros y particularmente con desconocidos, y al no utilizar todas las posibles medidas de autoprotección. Derivado de esto, surge la necesidad de, además de adoptar las medidas antes propuestas en cuanto a las políticas de seguridad en Internet, destinar recursos para educar a los usuarios en los riesgos derivados de determinadas actividades. Pero, sobre todo, y dadas las limitaciones del estudio aquí publicado, lo más necesario es seguir investigando en esta materia por lo menos en algunas de las direcciones que expresaré a continuación.

6.2. Limitaciones del estudio y propuestas de futuro

En primer lugar es necesario seguir realizando evaluaciones periódicas que nos permitan conocer mejor el fenómeno y más si tenemos en cuenta que las TIC están en permanente evolución. En la medida que el cibercrimen está mediatizado por el uso cotidiano de las TIC, éste también irá cambiando, lo cual es obvio especialmente si tenemos en cuenta que no hemos llegado a las cuotas máximas de expansión del uso de tales tecnologías.

En segundo lugar, sería interesante evaluar si los resultados obtenidos se extienden a otras formas de victimización, como por ejemplo, las relacionadas con el patrimonio que también han demostrado tener una incidencia significativa en la población española, cuya prevalencia se sitúa en torno al 87% de la población adulta (Miró, 2013). De forma pormenorizada, la infección por alguna forma de *malware* se sitúa en el 72,8%, siendo un 24,4% el porcentaje de pérdida efectiva de patrimonio por esta causa. Además, el 45% de la población española reconoce haber recibido correos proponiéndoles algún tipo de favor o negocio económico sospechoso de ser engañoso y un 43,6% manifiesta haber recibido algún correo cuya identidad del remitente era falsa. En menor medida, aunque sus efectos pueden tener un alcance mayor, un 9,4% ha sufrido algún tipo de fraude mediante la realización de compras o el uso de cuentas

bancarias en Internet (Miró y García, 2012) y, por lo tanto, son datos más que suficientes, para destinar otros recursos a su evaluación.

En tercer y último lugar, es necesario ampliar la muestra e incluir en ella a aquellos sujetos para los que el ciberespacio ha sido y es un elemento fundamental en su educación y en el tiempo de ocio, los nativos digitales (Prensky, 2001). Es conveniente evaluar como la familiarización natural con las TIC se relaciona con los procesos de victimización, sobre todo si tenemos en cuenta que pese a su facilidad para manejarse por la Red por haber crecido y desarrollado la mayor parte de su vida en Internet, no han sido educados en el uso de las tecnologías y por lo tanto, desconocen las claves esenciales para prevenir determinadas amenazas que además, y por la inexistencia de distancia en este nuevo medio de intercomunicación social, puede proceder de cualquier lugar.

Agradecimientos

Aunque son muchas las personas que me han ayudado a hacer posible este trabajo, debo hacer mención a una de ellas especialmente. Natalia García Guilabert, ha sido la persona que, con su saber y su dedicación, ha hecho realmente posible que yo entrara por primera vez en la investigación empírica, que pudiera operativizar los objetivos científicos de forma metodológica adecuada, y que eso se plasmara en un estudio del que ella es también responsable. Tampoco debo olvidar ni a mi mujer, Esther, que fue la primera que me explicó ya hace mucho la diferencia entre una variable dependiente e independiente, ni a Rebeca Bautista. Ella y Natalia me corrigen y explican con paciencia y tesón las claves de técnicas complejas y aún extrañas para mí.

Financiación

El presente artículo ha sido realizado en el marco del Proyecto de Investigación financiado por el Ministerio de Economía y Competitividad, DER2011-26054, titulado "Cibercriminalidad: detección de déficits en su prevención jurídica y determinación de los riesgos de victimización para una mejor prevención situacional criminológica".

7. Referencias

Agustina, J. R. (2013). Victimización en el ciberespacio. Consideraciones victimológicas y victimodogmáticas en el uso de las TIC. En prensa.

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey*, Mississipi: Mississippi State University.

Arndt, S., Turvey, C. y Andreasen, N. C. (1999). Correlating and predicting psychiatric symptom ratings: Spearman's r versus Kendall's tau correlation. *Journal of Psychiatric Research*, 33 (2): 97-104.

Barak, A. (2005). Sexual Harassment on the Internet. *Social Science Computer Review*, 23 (1): 77-92.

Basu, S. y Jones, R. (2007). Regulating cyberstalking. *Journal of Information, Law and Technology*, 2 (1).

Berson, I. R. (2003). Grooming cybervictims: The psychosocial effects of online exploitation for youth. *Journal of School Violence*, 2 (10): 5-18.

Bocij, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. *First Monday*, 8 (10).

Bocij, P. y McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, 139, 31-38.

Bossler, A. y Holt, T. (2009). On-line activities, guardianship, and malware infection: an examination of routine activities theory. *International Journal of Cyber Criminology*, 3 (1): 400-420.

Calmaestra Villén, J (2011). *Cyberbullying: prevalencia y características de un nuevo tipo de bullying indirecto*, Tesis doctoral, Servicio de Publicaciones de la Universidad de Córdoba, Córdoba.

Casas, J.A., Del Rey, R. y Ortega-Ruiz, R. (2013). Bullying and Cyberbullying: convergent and divergent predictor variables. *Computers in Human Behavior*, 29 (3), pp. 580-587.

Catalano, S.M. (2007). "Methodological change in the NCVS and the effect on convergence", en J. Lynch & L. Addington (Eds), *Understanding crime statistics*. Cambridge: Cambridge University Press.

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

Clarke, R. V. (1999). *Hot products: understanding, anticipating and reducing demand for stolen goods*. Paper no 112, London: Police Research Series, British home Office Research Publications.

Clough, J. (2010). *Principles of Cybercrime*, Cambridge: Cambridge University Press,.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: an exposition and test of a formal theory. *American Sociological Review*, 46 (5), 505-524.

Cohen, L. y Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44: 588-608.

Didden, R. *et al.* (2009). Cyberbullying among students with intellectual and developmental disability in special education settings. *Developmental Neurorehabilitation*, 12 (3): 146-151.

Eck, J.E. (1994). *Drug markets and drug places: a case-control study of the spatial structure of illicit drug dealing*, Ph.D. dissertation, College Park, MD: University of Maryland.

Felson, M. (1995). "Those who discourage crime", en J.E. Eck & D. Weisburd (Eds.), *Crime prevention studies: Vol 4. Crime and Place*, Criminal Justice Press, Monsey, NY.

Felson, M. (1998). *Crime and everyday life*, 2nd edition, Thousand Oaks, CA: PineForge Press.

Finn, J. (2004). A survey of Onile Harassment at a University Campus. *Journal of Interpersonal Violence*, 19 (4): 468-483.

Henson, B. (2011). *Fear of Crime Online: Examining the Effects of Online Victimization and Perceived Risk on Fear of Cyberstalking Victimization.* Tesis doctoral.

Hinduja, S. and Patchin, J. (2008). Cyberbullying: an exploratory analysis of factors related to offending and victimization, *Deviant Behavior*, 29 (2):129-156.

Holt, T. y Bossler, A. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30 (1): 1-25.

Instituto Nacional de Estadística (2011). Perfil sociodemográfico de los internautas. Análisis de datos INE 2010, en Internet, en http://www.osimga.org/export/sites/osimga/gl/documentos/d/20110905_perfil_sociodemo_2010.pdf.

Lynch, J.P. & Addington, L.A. (Eds) (2007). *Understanding crime statistics; revisiting the divergence of the NCVS and UCR*. Cambridge: Cambridge University Press,.

Marco Marco, J.J. (2010): "Menores, ciberacoso y derechos de la personalidad", en García González, J. (Coord.): *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet.* Valencia: Tirant lo Blanch,.

Marcum, C. (2008). Identifying potential factors of adolescent online victimization for high school seniors, *International Journal of Cyber Criminology*, 2 (2): 346-367.

Marcum, C.; Ricketts, M. and Higgins, G. (2010) Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory, *Criminal justice review*, 35 (4): 412-437.

McAlinden, A. M. (2006) " 'Setting'Em Up': Personal, Familial and Institutional Grooming in the Sexual Abuse of Children. *Social & Legal Studies*, 15 (3): 339-362.

Miró, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen". *Revista electrónica de Ciencia Penal y Criminología, 13-07.*

Miró, F. (2012) *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Miró, F. (2013). Derecho penal, *cyberbullying* y otras formas de acoso (no sexual) en el ciberespacio (en prensa).

Miró, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing, *Revista Electrónica de Ciencia Penal y Criminología* (en prensa).

Miró, F. y García, N. (2012). "Encuesta Nacional de victimización en el ciberespacio", presentada en la conferencia *La victimización en el ciberespacio,* impartida en el *IX Congreso Español de Criminología*, Girona, 2012.

Mitchell, K. Wolak, J., Finkelhor D. (2008). Mitchell, K. J., Wolak, J., & Finkelhor, D. (2008). Are blogs putting youth at risk for online sexual solicitation or harassment? *Child Abuse & Neglect*, 32 (2): 277-294.

Ngo, F. y Paternoster, R. (2011). CybercrimeVictimization: Anexamination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 5 (1): 773-793.

Patchin, J. W. e Hinduja, S (2006). Bullies move beyond the schoolyard a preliminary look at cyberbullying. *Youth violence and juvenile justice*, 4 (2): 148-169.

Peter, J. and Valkenburg, P. (2006). Adolescents' exposure to sexually explicit material on the internet. *Communication Research*, 33 (2): 178-204.

Pratt, T. C., Holtfreter, K., y Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47 (3): 267-296.

Prensky, M. (2001) Digital Natives, Digital Immigrants. *On the Horizon,* 9 (5): 1-6.

Reyns, B. (2010) *Being Pusued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective*. Tesis doctoral.

Reyns, B., Henson, B. y Fisher, B. (2011). Being Pursued Online Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal justice and behavior*, 38 (11): 1149-1169.

Silva L. C. (1995). *Excursión a la regresión logística en ciencias de la salud*, Madrid: Díaz de Santos.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., y Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49 (4): 376-385.

Van Dijk, J.J.M. y Mayhew, P. (1992). *Criminal victimisation in the industrialised world. Key findings of the 1989 and 1992 International Crime Surveys*. La Haya: Ministerio de Justicia, Holanda.

Wall, D. (2007). *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge.

Yar, M. (2005). The Novelty of 'Cybercrime'An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 4 (2): 407-427.

Ybarra, M. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *CyberPsychology & Behavior*, 7 (2): 247-57.

Ybarra, M. y Michell, K. (2004). Youth engaging in online harassment: Associations with caregiver–child relationships, Internet use, and personal characteristics. *Journal of adolescence*, 27 (3): 319-336.

Ybarra, M. y Mitchell, K. (2007). Prevalence and frequency of Internet harassment instigation: Implications for adolescent health. *Journal of Adolescent Health*, 41 (2): 189-195.

Ybarra, M., Espelage, D. Y Michell, K. (2007). The co-occurrence of internet harassment and unwanted sexual solicitation victimization and perpetration: Associations with psychosocial indicators. *Journal of Adolescent Health*, 41 (6): 31-41.

Yucedal, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories*. Tesis recuperada de http://etd.ohiolink.edu/view.cgi/YUCEDAL%20BEHZAT.pdf?kent1279290984.

Fernando Miró Llinares es profesor Titular de Derecho penal y Director del Centro Crímina para el Estudio y Prevención de la Delincuencia de la Universidad Miguel Hernández de Elche.