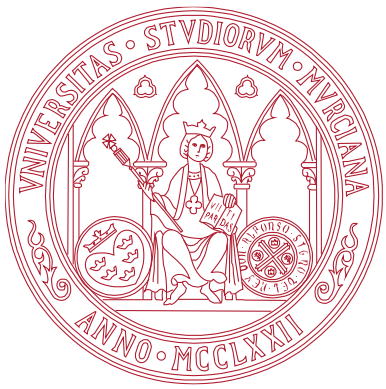


UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio

Dña. Natalia García Guilabert

2014

A mi padre y a mi madre porque sin ellos esto no habría sido posible

A mis hermanas por su amor incondicional

AGRADECIMIENTOS

A la Universidad de Murcia, por apostar de manera decidida por la Criminología y darme la oportunidad de desarrollar la tesis en este ámbito científico.

A los miembros del tribunal, por la amabilidad de asistir al acto de defensa y porque sus sabias aportaciones me ayudarán a encaminar las investigaciones venideras que comienzan con esta tesis doctoral.

Al Instituto Alicantino de Cultura Juan Gil-Albert de la Diputación Provincial de Alicante, por seleccionar este trabajo para las ayudas de Apoyo a la Investigación para la realización de Tesis Doctorales en Ciencias Sociales y Humanidades.

A la Universidad Miguel Hernández, por acogerme y permitirme trabajar en el campo de la investigación que tanto me apasiona.

A mis compañeros del Centro Crímina. A Elena Fernández, José Eugenio Medina, Paco Bernabeu, Zora Esteve, Mar Ruiz, Rebeca Bautista, Tere Díez, Nuria Rodríguez, Araceli Pascual y Javier Castro por sus incesantes ánimos y porque siempre estáis dispuestos a ayudarme en todo lo que necesito.

A mi maestro, el profesor Fernando Miró, por enseñarme a entender y amar la Universidad y, por supuesto, por ofrecerme la oportunidad de aprender de él día a día.

A mis amigos, a todos y cada uno de ellos, por animarme a seguir luchando y comprender mis largas ausencias, especialmente en esta última etapa.

A toda mi familia, pero especialmente a mis padres y a mis hermanas porque les debo todo. Y a Adonai, por acompañarme en este largo y duro camino.

A todos, gracias.

Contenido

PARTE I. MARCO TEÓRICO 11

INTRODUCCIÓN 13

CAPÍTULO I. EL CIBERESPACIO COMO NUEVO ÁMBITO DE COMUNICACIÓN Y OPORTUNIDAD DELICTIVA 23

1. El crimen en el ciberespacio: el cibercrimen 23

2. Sobre la sistematización de las distintas tipologías de cibercrimen 27

3. La cibercriminalidad social: la delincuencia de la web 2.0 38

3.1. Redes sociales y ámbitos de intercomunicación en el ciberespacio como potenciadores de la cibercriminalidad social 38

3.2. Tipos de cibercriminalidad social 41

3.2.1. El ciberacoso sexual, el *grooming* y otras formas de ataque sexual en el ciberespacio 41

3.2.2. *Bullying* y *stalking* como formas de acoso continuado en el ciberespacio 45

3.2.3. Cyberharassment o ataques individualizados de acoso en el ciberespacio 52

3.3. Concepto de cibercriminalidad social y relación con su relevancia jurídica a los efectos de este trabajo 58

4. Caracterización estructural de Internet como nuevo y distinto ámbito de oportunidad 68

CAPÍTULO II. LOS MENORES COMO VÍCTIMAS DEL CIBERACOSO NO SEXUAL 77

1. Menores y cibercrimen en la web 2.0 77

1.1. El uso de los menores de las TIC 77

1.2. Intercomunicación entre menores y cibercriminalidad social 83

2. Análisis de la prevalencia de victimización por ciberacoso no sexual en menores 86

2.1. Prevalencia de victimización por ciberacoso no sexual en menores en España 86

2.2. Prevalencia de victimización por ciberacoso no sexual en otros países 88

2.3. Análisis de las metodologías empleadas 89

3. Factores de riesgo de victimización de ciberacoso no sexual en menores *93*

3.1. El papel de las características demográficas en el ciberacoso 93

3.2. Factores de victimización relacionados con la personalidad 96

3.3. Factores de victimización relacionados con las actividades cotidianas 98

CAPÍTULO III. TEORÍA DE LAS ACTIVIDADES COTIDIANAS EN EL CIBERESPACIO Y VICTIMIZACIÓN POR CIBERACOSO NO SEXUAL 104

1. Teoría de las actividades cotidianas en el marco de las teorías del crimen y la oportunidad *104*

1.1. De las teorías de la criminalidad a las teorías del crimen 104

1.2. La teoría de las actividades cotidianas 116

1.2.1. Teoría de las actividades cotidianas y elementos del crimen 122

2. La aplicación de la teoría de las actividades cotidianas al ciberespacio *130*

2.1. Desarrollos teóricos de la TAC al ciberespacio 130

2.1.1. Nuevas y viejas botellas y criminalidad en el ciberespacio: el enfoque de Peter Grabosky 131

2.1.2. La adaptación de la TAC al ciberespacio por Majid Yar 137

2.1.3. La teoría de las actividades cotidianas en el ciberespacio de Fernando Miró 143

2.2. La aplicación de la teoría de las actividades cotidianas al análisis del riesgo de cibervictimización 150

2.2.1. Estudios de la TAC aplicados a la cibervictimización económica 150

2.2.2. Estudios de la TAC aplicados a la cibervictimización por acoso 164

3. Teoría de las actividades cotidianas y cibervictimización. Toma de posición y replanteamiento funcional de la teoría *184*

3.1. Sentido funcional de la aplicación de la TAC a los estudios de victimización y elementos a medir 184

3.2. TAC y características del objetivo adecuado en el ciberespacio 191

3.2.1. Aplicación del VIVA al ciberespacio 192

3.2.2. Recapitulación 201

4. Interacción e introducción como factores de adecuación del objetivo en el ciberespacio y vigilancia familiar como concreción del elemento guardián capaz 203

PARTE II. ESTUDIO EMPÍRICO 213

CAPÍTULO I. ESTUDIO EMPÍRICO: ANÁLISIS DE LA VICTIMIZACIÓN DE CIBERACOSO CONTINUADO NO SEXUAL EN MENORES DE LA PROVINCIA DE ALICANTE 215

1. Objetivos e hipótesis de partida 216

1.1. Objetivos 216

1. 2. Hipótesis 217

2. Método 219

2.1. Muestra 219

2.2. Procedimiento de selección de la muestra 222

2.3. Variables 223

2.3.1. Variables dependientes 223

2.3.2. Variables independientes 226

2.4. Instrumento 247

2.5. Procedimiento 249

3. Resultados 250

3.1. Análisis descriptivos 250

3.1.1. Análisis descriptivo de los menores víctimas de ciberacoso continuado no sexual de la provincia de Alicante 250

3.1.2. Análisis descriptivos de las actividades cotidianas de los menores de la provincia de Alicante en Internet 254

3.2. Análisis de componentes principales 284

3.2.1. Descripción de las componentes principales 286

3.2.2. Análisis descriptivo de las componentes principales 311

3.2.3. Análisis factorial de las componentes principales 320

3.3. Análisis bivariados 324

3.3.1. Análisis de las conductas de ciberacoso continuado por sexo y edad 324

a. Diferencias por sexo 324

b. Diferencias por edad 335

3.3.2. Análisis de la relación entre las conductas de ciberacoso continuado y las actividades cotidianas de los menores en el ciberespacio 343

3.3.3. Análisis de las variables independientes por sexo y edad 351
3.3.4. Distribución de las variables independientes entre los menores no víctimas de ciberacoso 359
3.3.5. Relación entre las variables independientes 363
4. Modelo predictivo de ciberacoso continuado no sexual de menores 365
4.1. Variables en el modelo 368
4.2. Preparación de la muestra 369
4.3. Entrenamiento de la red 372
4.4. Resultados 373
CAPÍTULO II. DISCUSIÓN, CONCLUSIONES Y PROSPECTIVA 385
1. Discusión 385
1.1. Prevalencia de la cibervictimización 385
1.2. Características demográficas de las víctimas de ciberacoso continuado 397
1.3. Conductas de riesgo de los menores en Internet 400
2. Recapitulación y conclusiones 414
3. Limitaciones y prospectiva 427
Bibliografía 429
Tabla de ilustraciones 471
Índice de tablas 475
ANEXO I. ENCUESTA 479

Parte I. Marco teórico

Introducción

El cibercrimen, como concepto que aúna a toda la criminalidad cometida en el ámbito del ciberespacio, ha adquirido un inusitado protagonismo en los últimos años. Es cierto que no se trata de un fenómeno completamente nuevo, dado que sus primeras manifestaciones surgieron casi al tiempo que Internet comenzaba a dar sus primeros pasos. Sin embargo, ha sido con la popularización de la Red de redes y con su conversión en un nuevo ámbito esencial para la intercomunicación personal, cuando hemos comprendido que más que ante un nuevo tipo de delitos, nos encontramos ante un nuevo tipo de lugar en el que los crímenes se cometen. Una vez más la tecnología modifica los hábitos sociales, hace surgir nuevos intereses, nuevas necesidades, nuevas formas de comunicación social y, también, nuevos crímenes o diferentes concreciones de los mismos.

Una de las aportaciones sobre el estudio del crimen que con más precisión analizó esta intensa relación entre cambio tecnológico, cambio social y criminalidad, fue el seminal artículo de Cohen y Felson "Social Change and Crime Rate Trends: A Routine Activity Approach". Cohen y Felson (1979) plantearon que los cambios tecnológicos y, derivados de ellos, los sociales, modificaban los hábitos y las actividades cotidianas de las personas, lo cual, a su vez, podía incidir en los entornos de oportunidad en los que los crímenes acontecen, como eventos sociales que son. Concretamente, en su ya mítico estudio, Cohen y Felson concluyeron que importantes cambios acontecidos desde el fin de la Segunda Guerra Mundial, paralelamente

a un crecimiento de las condiciones económicas de la gran mayoría y a una mejora significativa de los derechos sociales, podían dar sentido al, conforme a las teorías sociológicas más tradicionales, inexplicable incremento de la delincuencia. La razón es que revoluciones tecnológicas como el automóvil y muchas otras, junto con cambios sociales relacionados con el papel de la mujer en su entorno junto con otros pequeños pero determinantes cambios, habían supuesto un incremento de las oportunidades para el delito, al aumentar el número de objetivos adecuados, al posibilitar el contacto directo entre las personas o sus propiedades y los delincuentes, y al disminuir los guardianes capaces de prevenir el delito. La perspectiva adoptada era, por tanto, aparentemente "macro": el *approach* pretendía explicar una tendencia en la evolución del crimen derivada del cambio tecnológico, pero la teoría iba a ir, como por todos es sabido, más allá.

Lo cierto es que, quizás sin la perspectiva necesaria, la intensidad de los cambios sociales derivados de la inmensa revolución tecnológica acontecida en las últimas tres décadas puede ser incluso superior a la de los años 50 y 60. La web 2.0 ha modificado lo que parecía que iba a ser una herramienta informacional con gran potencial para las transacciones económicas en un nuevo ámbito de relaciones sociales desarrollado paralelamente al físico y cada vez más popularizado en todo el mundo. Bien por el desarrollo vertiginoso que han experimentado las Tecnologías de la Información y la Comunicación (en adelante, TIC), por la facilidad de acceso para personas con apenas conocimientos sobre tecnología, o por el abaratamiento de los sistemas electrónicos, Internet se ha convertido en el medio principal, tanto para las transacciones económicas como para el establecimiento de las relaciones sociales. Si esto es así para las

personas que han sido testigos de la evolución de las TIC y de cómo han impregnado sus vidas, aún lo es más para los que han nacido en la era digital, los llamados "nativos digitales" (Prensky, 2001), que no conciben su vida sin el uso de las TIC. Desde hace unos años, se puede observar cómo los niños -desde que nacen- comienzan su incursión en las TIC. Basta con mirar la oferta de aplicaciones que existe en la actualidad para *tablets* y *smartphones* con juegos destinados a menores entre 0 y 5 años. Son algunos los menores que ya poseen teléfono móvil a los 6 años, pero a los 13 prácticamente lo tienen todos (Bringué y Sábada, 2011). Y a partir de los 10 años hacen uso regular de Internet. Están conectados las 24 horas del día, entre otros motivos porque lo pueden hacer desde cualquier lugar. El Colegio Oficial de Psicólogos de Madrid publicaba recientemente un informe (2014) donde se aseguraba que casi todos los jóvenes nunca apagan sus teléfonos móviles. Y es que, gracias a las redes *wifi,* los servicios de datos y la cantidad de sistemas electrónicos transportables (como el ordenador portátil, el *smartphone* y la *tablet*), se puede acceder a Internet casi desde cualquier espacio físico.

Está claro que, como espacio para la comunicación social, el ciberespacio también se iba a convertir pronto en un ámbito de oportunidad delictiva. El mismo lo fue primero con la aparición de los sistemas informáticos y los intereses económicos y personales relacionados íntimamente con ellos, para algunos pocos delitos cometidos sobre objetos nuevos y también para algunas nuevas conductas que replicaban delitos ya viejos. Pero cuando Internet pasó a ser lo que ahora es, un nuevo lugar en el que las relaciones personales de todo tipo casi pueden replicar a las que se tienen en el espacio físico, los eventos criminales se han ido amplificando, no tanto en número,

como en formas, tantas como posibilidades de relación a través de Internet existen. Esto, como se ha dicho, afecta a todos los estratos sociales, dado que todos usan Internet. Pero si decíamos que los nativos digitales son los que más lo usan como forma de comunicación "inter-pares", es lógico pensar que también a ellos les afecten más estos "nuevos" delitos. La creación de Internet ha supuesto, en este sentido, un nuevo ámbito para la comisión de viejas formas de ataque a las personas en general, y a los menores en particular, como el *bullying,* el *stalking,* el *grooming*, etc. A través del teléfono móvil, el ordenador, la mensajería instantánea, la redes sociales, etc., se puede por ejemplo, humillar, amenazar, acosar, ridiculizar, sin necesidad de una proximidad física. E independientemente de la tipificación expresa o genérica de estas conductas en el Código Penal, la preocupación social por las mismas es cada vez más significativa, dados los efectos dañinos que pueden generar muchas de ellas en aquellas personas que las padecen.

En realidad, todos los cambios sociales que estamos viviendo en la actualidad tendrán consecuencias a nivel "macro" en la evolución de la criminalidad. Será muy interesante, en este sentido, la utilización de la Teoría de las Actividades Cotidianas para analizar, pongamos dentro de 30 años, cómo incidieron todos los cambios tecnológicos y sociales tanto en la evolución de las tasas de la delincuencia física, como en la aparición de esa nueva delincuencia llamada cibercriminalidad. Éste, sin embargo, y pese al título de la tesis que aquí se presenta, no es el objetivo del trabajo. Como se ha dicho al principio, lo que nació como una teoría explicativa de la evolución de la delincuencia a nivel "macro", se fue convirtiendo en un marco teórico o una aproximación explicativa del crimen como evento social a nivel

"micro", conforme al cual el crimen depende de la acción de un delincuente potencial en un lugar con objetivos o víctimas propicias para el delito. Así, con tal planteamiento, se reconocía que el foco del fenómeno criminal puede, y para la prevención también "debe", situarse no sólo en el análisis de las razones por las que un sujeto comete un crimen, sino centrando la visión sobre las condiciones de un objetivo que le hacen, potencialmente, más o menos adecuado para el agresor.

Esta es la perspectiva que, aplicada a la cibercriminalidad, interesa en este trabajo. Independientemente de si las nuevas rutinas de los usuarios de Internet conllevan un incremento o una disminución de la delincuencia, lo que es una realidad es que las TIC han configurado un nuevo tipo de espacio en el que también pueden converger, como avanzó Grabosky (2001), un delincuente potencial, una víctima adecuada en ausencia de un guardián capaz, pero en el que la cotidianeidad es también claramente otra a la del espacio físico. Las investigaciones recientes apuntan a que los nuevos hábitos de comunicación y consumo, es decir, las actividades cotidianas de las personas en el ciberespacio, proporcionan oportunidades para llevar a cabo múltiples formas de cibercriminalidad. Y, dadas las características que configuran el nuevo ámbito, existen grandes y nuevas posibilidades de contacto entre agresores motivados y potenciales víctimas. Esto ha generado nuevos planteamientos sobre cómo los usuarios, con su actuar del día a día, pueden favorecer su victimización al convertirse en objetivos adecuados para el agresor motivado.

En este sentido, el presente trabajo surge con la idea de aportar mayor conocimiento sobre cuáles son las conductas que realizan los

internautas que les sitúan en una posición de riesgo para sufrir ciberacoso no sexual. A partir del *approach* de las "actividades cotidianas", y aprovechando su orientación esencialmente victimológica para tratar de identificar qué hace a alguien más o menos adecuado en el marco de un evento criminal, trataremos de comprender la cotidianeidad en el nuevo espacio y definir variables concretas que determinen la victimización por concretos ciberdelitos.

A partir del planteamiento teórico del que se parte, se han tomado otras dos decisiones respecto al objeto del trabajo que merecen ser comentadas. La primera se refiere a la decisión de centrar el análisis en lo que Miró (2012) ha denominado cibercriminalidad social o personal. Es indiscutible, conforme a todos los estudios empíricos realizados en múltiples y diversos lugares del mundo y sobre los que se hablará posteriormente, que la cibercriminalidad más usual es la realizada con finalidad económica, incluyente tanto de las múltiples formas de fraude como de todos los ciberataques preparatorios (*hacking,* infecciones de *malware* y demás), sin los cuales aquéllas no serían posibles. El interés de analizar qué actividades cotidianas inciden en la victimización de las personas por estos delitos resulta altísimo. Pero también es cierto que el fenómeno más novedoso, que más interés y, quizás algo exagerado, temor suscita en los últimos años es el de la cibercriminalidad relacionada con la web 2.0, con las nuevas formas de intercomunicación entre personas, con las redes sociales, con los sistemas de mensajería instantánea, etc. Precisamente por ello, se ha decidido enfocar el análisis en esta ciberdelincuencia social. La segunda decisión respecto al objeto del trabajo está intensamente relacionada con la primera. Al interesar la cibercriminalidad social, el objeto de estudio debían serlo aquellos

sectores de la población que están protagonizando, claramente, la revolución social derivada de la irrupción de la web 2.0: los adolescentes. Además de ser éste un colectivo que ha sido poco estudiado, especialmente vulnerable y, por ello, particularmente digno de atención; se trata, sobre todo, de un colectivo que hace un elevado uso de las TIC, que ha modificado su cotidianeidad hasta niveles inimaginables hace algunas décadas, cambiando sus usos y la forma de relacionarse entre sí. Si el objetivo final de esta tesis, por tanto, es la comprensión del fenómeno delictivo en Internet, en particular la de la cibercriminalidad social con la voluntad de identificar factores de riesgo dependientes de la cotidianeidad de la propia víctima que incidan en su propia configuración como parte del evento criminal para, a su vez, definir en un futuro mejores estrategias de prevención; los adolescentes eran el objeto adecuado para la investigación.

Para alcanzar tales objetivos, la tesis ha sido estructurada en dos partes. La primera de ellas corresponde a la fundamentación teórica, y se divide en tres capítulos. En el primero se hace un análisis de la cibercriminalidad, de las tipologías existentes y sus clasificaciones, haciendo especial hincapié en la que sufren los menores, y dedicando un apartado al análisis del lugar en el que se cometen los cibercrímenes (el ciberespacio).

El segundo capítulo está centrado en analizar la victimización por ciberacoso no sexual en menores, haciendo una revisión de los resultados más relevantes encontrados hasta el momento en la literatura internacional. Y finalmente, el tercer capítulo está centrado en el estudio de las teorías de las actividades cotidianas en el ciberespacio. Se empieza haciendo un recorrido desde el surgimiento

de las teorías de la oportunidad y por su evolución, para pasar a analizar su aplicación al ciberespacio. A partir de los desarrollos teóricos y prácticos, se realiza un replanteamiento del enfoque de las actividades cotidianas, haciendo énfasis en las características que hacen que un usuario de Internet se convierta en un objetivo potencial para ser atacado por un agresor.

La segunda parte del trabajo está dedicada al estudio empírico y está estructurada en dos capítulos. En el primero, se detallan los objetivos y las hipótesis de investigación planteadas acordes con el desarrollo teórico. También se abordan los aspectos metodológicos del estudio, incluyendo la descripción de la muestra y del procedimiento aplicado para su selección, la definición de las variables evaluadas, el instrumento de medida utilizado y el procedimiento llevado a cabo para obtener los datos de la muestra. A continuación, se exponen los resultados obtenidos en el estudio en el siguiente orden: los datos descriptivos sobre las diferentes formas de victimización y las actividades cotidianas de los menores en el ciberespacio; los datos obtenidos de los análisis bivariados entre las diferentes formas de victimización y las actividades cotidianas; y finalmente, la importancia que tienen las actividades cotidianas en la victimización a partir de la creación de un modelo matemático mediante una red neuronal artificial.

En el segundo capítulo, se expone la discusión de los resultados obtenidos en relación a la hipótesis de partida, las conclusiones que derivan del estudio y las limitaciones encontradas durante el desarrollo, sugiriendo algunas soluciones para mejorar los futuros trabajos que se realicen en este campo. Finalmente, se han adjuntado las referencias

bibliográficas consultadas a lo largo de la realización del trabajo, así como los anexos.

Capítulo I. El ciberespacio como nuevo ámbito de comunicación y oportunidad delictiva

"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology."

(Carl Sagan, 2006)

1. El crimen en el ciberespacio: el cibercrimen

Son muchos los términos que la comunidad científica ha empleado para referirse a la criminalidad relacionada con el uso de las TIC: "delincuencia informática", "*virtual criminality*", "*computer crime*", "*e-crime*", "*crime online*", "*computer-related*", "*high-tech crime*", "*digital crime*", "*Internet crime*", entre otros[1], entre otros. Todos ellos

[1] Así, el término "delincuencia informática" es empleado en la obra de Romeo Casabona (1988) "El poder informático y seguridad jurídica", o en la dirigida por De la Cuesta (2010) "Derecho penal informático". Asimismo, la locución "*virtual criminality*" es utilizada en el trabajo de Grabosky (2001), mientras que

tienen en común que ponen el acento en el papel que juega la tecnología en la comisión de delitos (Clough, 2011), y a pesar de que cada uno de ellos no tienen estrictamente un sentido idéntico, se han venido sustituyendo paulatinamente por el de "cibercrimen" (en inglés *cybercrime*), probablemente, como ha apuntado Miró (2012), porque éste expresa con más precisión la relación con el ámbito nuevo de intercomunicación personal que es Internet.

El término cibercrimen (también, como sinónimo de "cibercriminalidad"[2]) es ampliamente utilizado hoy en día para describir los delitos o daños que resultan de las oportunidades creadas por las tecnologías en red (Wall, 2008). El origen de este término se debe en gran medida a los medios de comunicación (Wall, 2001) y surge de la unión de dos conceptos: "ciberespacio" y "crimen". El término "ciberespacio" (en inglés "*cyberspace*") fue creado por William Gibson en su obra *Neuromancer* en 1984, y significa algo más que la

---

la expresión "*computer crime*" es la utilizada en el estudio de Bregant y Bregant (2014) y en el de Choi (2008). Chiu, Chun y Wang (2009), usan el término "*e-crime*", mientras que Jewkes en su trabajo (2013) emplea la expresión "*crime online*". Grabosky (2007) maneja el término "*computer-related*"; la expresión "*digital crime*" es la utilizada por Taylor (2006); mientras que en su obra con Taylor y Quayle (2003) se inclinó por la locución "*Internet crime*". A esta diversidad de términos empleados, se refiere también Clough (2011).

[2] Explica Miró (2012) que el término cibercriminalidad puede ser usado como sinónimo de cibercrimen. Habrá ocasiones en que ambos términos se refieran a cuestiones distintas, y en este sentido, la locución cibercriminalidad puede ser usada para hacer referencia a la criminalidad cometida en el ciberespacio, es decir, englobando todos los cibercrímenes, mientras que el término cibercrimen, podría ser empleado para situar dentro del fenómeno de la criminalidad un crimen en concreto. Sin embargo, en muchas ocasiones, el término cibercrimen se usa para hacer referencia a todos los comportamientos que reúnen las características tipológicas que conforman el fenómeno y por tanto, es usado como sinónimo de cibercriminalidad.

información digital y la unión entre sistemas informáticos. En palabras de Kuehl (2009) es "el conjunto de un dominio global dentro del entorno de la información cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicación" (p. 29).

Yar (2006) ha definido el cibercrimen como "aquel delito cuya característica esencial es el rol central que las TIC juegan en su comisión" (p.9). En sentido similar, se refiere Jewkes (2006) con este término a "cualquier acto ilegal cometido por medio de (o con asistencia de) sistemas informáticos, redes digitales, Internet y demás TIC" (p. 106). Estas definiciones vienen a incluir tanto los delitos nuevos surgidos a la luz de la creación del ciberespacio y de la aparición de diferentes intereses sociales que también pueden ser dañados o afectados por conductas realizadas en el seno de Internet, como aquellos otros delitos que tienen un referente tradicional y clásico en el espacio físico, pero que ahora también se cometen en este nuevo lugar o ámbito de intercomunicación personal configurado por el uso de las TIC, que es Internet (Miró, 2012). Por otra parte, el término cibercrimen permite recoger en su seno todos los delitos que hasta ahora se conocen realizados en el ciberespacio, así como los que surjan de las diferentes evoluciones de las TIC que aparezcan en el futuro. La cibercriminalidad ha ido mutando y evolucionando de manera paralela a los usuarios del ciberespacio y sus tecnologías asociadas, y lo seguirá haciendo en la medida que evolucione la tecnología y su uso (Clough, 2011, p. 627). Como explica Miró (2012), la primera generación de la cibercriminalidad estaba caracterizada por el uso de los sistemas

informáticos para la comisión de los delitos. Crímenes prototípicos de esta primera era, podrían ser el robo de información, los daños o sabotajes informáticos y otras infracciones en las que se utilizaban las tecnologías de la información esencialmente como objeto de ataque. A ella le siguió una segunda generación, en la que la nota característica era que el delito se cometía a través de Internet, pudiendo citarse como referencia esencial en este sentido, los delitos de distribución de pornografía infantil (Morillas, 2005) o los delitos contra la propiedad intelectual (Miró, 2005), todos los cuales se caracterizaban por el medio de comisión delictiva, y en particular por la nueva dimensión que dichas conductas alcanzaban frente a las formas de ejecución de las mismas en el espacio físico, al perpetrarse ahora en una red transnacional y popularizada con tanta capacidad para dañar intereses sociales y personales, como lo es el ciberespacio.

En realidad, la tercera generación de ciberdelincuencia no parece diferir mucho de la anterior, dado que el elemento que une a todas las modalidades de comportamiento delictivo que integramos dentro del concepto de cibercriminalidad es, básicamente, el medio en el que las mismas se realizan. Pero, de algún modo, el medio ha cambiado, Internet ya no es lo que fue al principio. En la segunda generación de lo que hemos llamado ciberdelincuencia, Internet recién había nacido, y se configuraba como un extraordinario medio para la difusión de información que, básicamente, tenía un valor económico o informacional. Esto sigue siendo así. Pero la web 2.0 ha revolucionado Internet hasta convertirlo en un nuevo ámbito de relaciones sociales y personales inimaginable hace quince o veinte años. Ahora Internet no sólo sirve para difundir información, para transmitirla e intercambiarla, sino que más bien es un lugar en el que se puede estar, en el que

socializar, en el que relacionarse y contactar entre miles de personas. Y esa es la matriz de la tercera generación de ciberdelitos: el ámbito de intercomunicación personal que constituye Internet. Así, y aunque sobre ello se volverá después, delitos prototípicos de esta tercera generación de cibercriminalidad serían las diferentes formas de ciberacoso no sexual, incluyendo el *cyberbullying* o acoso continuado entre menores y en el ámbito escolar, y las diferentes formas de *harassment* o de conductas concretas de acoso individualizado realizadas por medio del uso de las redes sociales y demás herramientas de intercomunicación personal que hay disponibles en la actualidad; y también las variadas modalidades de atentado sexual realizadas a través de Internet, de entre las cuales destaca el *child grooming* o acoso a menores realizado como acto preparatorio inicial previo a un abuso sexual posterior.

2. Sobre la sistematización de las distintas tipologías de cibercrimen

Internet y las TIC están en permanente evolución. Cada día se generan nuevas tecnologías y con ellas también nuevas formas de comportarnos en Internet. Ha cambiado, y seguirá cambiando, la forma de comprar, de realizar transacciones económicas, de estudiar, de comunicar con otras personas, etc. Y ha cambiado también, como no podía ser de otro modo, la forma de cometer crímenes. En la actualidad existen muchas conductas criminales que se pueden llevar a cabo en el

ciberespacio (Morillas Cueva, 2006, 2008), condición que es la esencial y básica que hemos utilizado para que un crimen integre esta macrocategoría denominada cibercriminalidad. La extraordinaria amplitud, pues, del concepto de referencia, y la previsión, totalmente coherente con la evolución cambiante de las TIC, de que sigan surgiendo irremediablemente diferentes tipologías de ciberdelitos, es lo que hace necesario establecer sistemas para la clasificación de las distintas modalidades de conducta criminal en el ciberespacio que las categorice de un modo funcional adecuado, de forma que nos permita bien comprender el fenómeno, bien discriminar sus distintos efectos, o bien definir estrategias diferenciadas de prevención.

Como es por todos sabido, son muchísimas las distintas clasificaciones propuestas para diferenciar entre diferentes tipos de cibercrimen. Podría decirse incluso que cada autor que analiza el fenómeno trata de aportar una o más clasificaciones de cibercriminalidad, diferenciándose del resto de autores que han abordado el delito cometido en Internet. Entre las distintas propuestas que se han realizado, hasta el momento, para ordenar y clasificar los cibercrímenes, se puede distinguir entre aquéllas que lo hacen desde una perspectiva legal, las que atienden a la relevancia que tienen las TIC en la comisión delictiva, y las que se basan en la intencionalidad del agresor. A los efectos de este trabajo, y dado el planteamiento puramente criminológico del mismo, nos interesan especialmente estas dos últimas sistemáticas clasificatorias. Aun así, y en aras de comprender los intereses sociales puestos en riesgo en el ciberespacio, realizaremos un breve repaso por algunas significativas clasificaciones jurídico-legales.

Desde una perspectiva legal, aunque con claras connotaciones fenomenológicas, Furnell (2003) distingue entre los delitos asistidos por el ordenador (*computer-assisted crimes)* y en los que el ordenador es el objetivo (*computer-focused crimes).* Los primeros serían aquéllos que utilizan los sistemas informáticos como herramientas para cometer los delitos, como el blanqueo de capitales, el fraude, el acoso sexual, la pornografía, etc. Los segundos, tienen como objetivo los sistemas informáticos y las redes y como condición esencial que no podrían existir sin la creación de Internet, como por ejemplo, los ataques de *hacking, malware*, denegación de servicios, etc. Esta clasificación propuesta por Furnell (2003), encaja a la perfección dentro de lo que Morillas (2005) categorizó como "postura intermedia" en su macroclasificación sobre las distintas conceptualizaciones de "delincuencia informática", pues distingue entre ordenadores usados para cometer el delito y aquéllos que son empleado como objeto sobre los que recae el mismo.

Distinta es la clasificación elaborada por Wall (2001) donde, también desde una óptica legal, distingue cuatro categorías de cibercrímenes: Frente a una concepción restringida, que englobaría aquellas conductas dirigidas a castigar los atentados sobre el *software* del ordenador y no puedan ser subsumidas por figuras típicas tradicionales por la intangilbilidad de los bienes informáticos; así como frente a una concepción amplia, que entiende como delincuencia informática cualquier comportamiento criminógeno en el que el ordenador esté involucrado.

- *Cyber-trespass*: Hace referencia al acceso no autorizado a sistemas informáticos, donde imperan los derechos

establecidos por el propio titular. Quedarían incluidos en esta categoría el *hacking,* infecciones de *malware,* etc.

- *Cyber-deceptions/thefts*: En esta categoría se incluirían todos los ataques codiciosos y que englobarían diferentes formas de fraude en el ciberespacio, como por ejemplo, los fraudes con tarjetas de crédito.

- *Cyber-pornography/obscenity:* Abarcaría todas las infracciones penales relacionadas con la publicación o comercio con material sexual explícito en el ciberespacio.

- *Cyber-violence:* Incluye dentro de esta categoría todas las actividades individuales o grupales, que tienen como objetivo el daño psicológico o la incitación al daño físico contra otros. Entre ellas, se pueden incluir conductas como la de *cyberstalking, cyberbullying, hate speech, etc.*

En España, aunque no existe propiamente una categoría de delitos informáticos en el Código penal (Olmedo, 2008), sí se han realizado categorizaciones de estos delitos, aunque para una mejor comprensión de las mismas se tiene que tener en cuenta, sin embargo, el momento en el que se realizaron éstas, así como la influencia germánica en el Derecho penal español y, en concreto, la influencia de los trabajos de Ulrich Sieber bajo la conceptualización más tradicional

de "delitos informáticos"[3]. Así, es clásica la distinción que hace Romeo Casabona (1988) entre el fraude informático, las manipulaciones en cajeros automáticos mediante tarjetas provistas de banda magnética, y las agresiones a los sistemas o elementos informáticos, dentro de las cuales incluye el sabotaje informático y las agresiones al soporte material, y la sustracción o copia de bases de datos o de programas, cuyos principales tipos son el espionaje informático y la piratería de programas. En el mismo sentido, González Rus (1999) diferencia las conductas de sabotaje informático, las de acceso ilícito a sistemas informáticos, las de piratería de programas de ordenador (las relativas a la propiedad intelectual) y la utilización ilegítima de sistemas o elementos informáticos.

Otra forma de categorizar los delitos, en la que se ha trabajado ampliamente, es la que atiende al papel que cumplen las TIC en la producción de los cibercrímenes. Así, Clough (2011) propone tres categorías de delitos:

- Delitos en los que el ordenador o la Red es el objetivo, como ocurre, por ejemplo, en el *hacking*, el *malware,* o los ataques de denegación de servicios.

[3] Sieber (1980), incluyó dentro del grupo de delitos informáticos: 1) fraude por manipulación informática o fraude informático; 2) sabotaje informático; 3) acceso no autorizado; 4) sustracción de servicios; 5) delitos económicos tradicionales asistidos por sistemas informáticos y 6) espionaje informático. Más reciente es la clasificación en la que propone distinguir entre: 1. Infracciones a la intimidad; 2. Delitos económicos; 3. Contenidos ilegales y nocivos; y 4. Otros delitos que deriven del uso de la informática (Sieber, 1998).

- Delitos en los que el ordenador es la herramienta empleada para cometer el delito, como sucede en la pornografía infantil, el acoso, el fraude, etc.

- Delitos en los que el uso de los sistemas informáticos es un aspecto incidental de la comisión del delito, pero que pueden ayudar a ofrecer evidencias del mismo, como ocurre en el caso de los mensajes de texto que se recuperan del móvil de una víctima de asesinato.

Respecto a esta última categoría descrita por Clough, otros autores consideran que no debería ser incluida como cibercrimen (Miró, 2012)[4]. Mientras que por su parte, Bregant y Bregant (2014) consideran que a las dos primeras categorías habría que añadir una tercera que hace referencia a la publicación de contenidos ilegales mediante sistemas electrónicos, y que se caracterizaría por la transmisión y difusión de pornografía infantil, la difusión de mensajes de odio racial, la piratería intelectual, etc.

Además de la anteriormente expuesta, (2005) realiza otra clasificación, esta vez desde una perspectiva fenomenológica, en la que distingue tres tipos de cibercrímenes:

[4] Como apunta Miró (2012) "para que estemos ante un cibercrimen no bastará con que se utilicen las TIC para realizar el comportamiento criminal, sino que se exigirá que tal uso tenga que ver con algún elemento esencial del delito" (p. 41).

- *Computer integrity crimes:* Esta categoría englobaría todos aquellos delitos en los que se atenta contra la integridad de una red o de un sistema. Esto es lo que ocurriría en el caso del *hacking*, de la denegación de servicios, del cibervandalismo, etc.

- *Computer related crimes:* Dentro de esta categoría se incluirían todos los delitos que usan la tecnología para engañar a las víctimas con intenciones ilícitas (ciberfraude, *phishing*, etc.)

- *Computer content crimes:* Esta última clase de cibercrímenes, comprendería todos aquellos delitos relacionados con la difusión de contenidos, como la difusión de mensajes de odio racial, de material pornográfico, piratería, etc.

Otra clasificación distinta a las enunciadas y que también está basada en la importancia de las TIC, es la que propone Miró (2012). El autor distingue entre los ataques que sólo se pueden realizar a través de las TIC, los ataques tradicionales que ahora también se pueden realizar a través de las TIC y los ataques que, aun no siendo nuevos, deben ser incluidos en una categoría distinta por la problemática que presenta en su tratamiento. Así, distingue entre:

- Ciberataques puros[5]: En esta categoría se incluyen los delitos que únicamente se pueden cometer en el ciberespacio, y para los que las TIC se han convertido, en un generador de delitos. Esta categoría englobaría delitos como el *hacking,* el *cracking*, el envío de *malware,* el *spam,* los ataques de denegación de servicios, etc.

- Ciberataques réplica: Esta categoría engloba delitos tradicionales que ahora también se cometen en el ciberespacio. Por lo tanto, para este grupo de delitos, el ciberespacio se ha convertido en un lugar nuevo donde llevar a cabo delitos como el fraude, el acoso, el espionaje, etc.

- Ciberataques de contenido: Incluye esta última categoría conductas ilícitas de difusión, o de acceso a información ilícita o socialmente peligrosa, como la pornografía infantil, la difusión de odio racial o la ciberpiratería intelectual, entre otros. En realidad, es una forma concreta de ataques "réplica" pero que merece ser englobada en otra categoría por ser el ciberespacio un sistema que facilita enormemente la difusión de

[5] Similar diferencia realiza Pi (2008), al distinguir entre *pure computer crimes,* para referirse a los delitos cuyo objetivo son los sistemas informáticos y las redes, y *computer-related conventional crimes* para los crímenes que usan los ordenadores y las redes para cometer crímenes convencionales.

contenidos, lo que plantea problemáticas jurídicas especiales.

Finalmente, se distingue una tercera forma de clasificación que ya no atiende a una sistematización legal, ni al papel que juegan las TIC en la producción de actividades ilícitas, sino a la intencionalidad con la que el agresor lleva a cabo los ataques. En este sentido, Miró (2012) distingue entre los que tienen una finalidad económica, lo que tienen una finalidad social y los que tienen una finalidad política.

- Cibercrímenes económicos [6]: En esta categoría se incluyen los delitos cuya finalidad es tener un beneficio patrimonial directo o indirecto. En este sentido, no sólo se incluyen los que directamente afectan al patrimonio de las personas, sino también a los que afectan a otros bienes, como la intimidad, la seguridad de los sistemas, etc., pero cuyo objetivo final es la obtención de un beneficio patrimonial. Así, distingue dos tipos de cibercrímenes económicos, los mediales o instrumentales, y los económicos en sentido estricto.

[6] Otra clasificación interesante para distinguir los cibercrímenes relacionados con el plano económico es la propuesta de Nir Kshetri (2011), quien distingue entre *predatory cybercrimes* y *market-based cybercrimes*. La primera categoría incluye los delitos que dañan o toman los bienes de otra persona, como por ejemplo ocurre en el ciberfraude. Este autor considera que este tipo de delitos, simplemente, redistribuyen la riqueza, frente a los del segundo tipo, que la genera. En esta segunda categoría, se incluirían por ejemplo, las ganancias surgidas de la venta de drogas o de la venta de la información de tarjetas de crédito robadas.

Los primeros, serían todos aquellos ataques que son un paso previo para cometer los segundos, y que -en muchos casos- son necesarios para poder llevarlos a cabo. Sirva el *hacking* como ejemplo de ello, pues permite acceder al sistema informático donde encontrar la información bancaria necesaria para cometer el delito de fraude.

- Cibercrímenes sociales: Esta categoría tiene que ver con la comunicación de las personas a través de Internet, es decir, tiene que ver con la parte "social" del ciberespacio. Y es que el desarrollo de las TIC ha permitido, no sólo un cambio en la comunicación social, sino que también ha abierto la posibilidad de atacar todas las esferas privadas de un usuario de Internet, así como otros ámbitos personales. Por ello, Miró habla de cibercriminalidad social o personal, porque si bien son principalmente, y desde una perspectiva jurídica, intereses personales individuales los que se verían generalmente lesionados al realizarse este tipo de actividades delictivas, el ámbito de comunicación en el que ello se produce, es el de las relaciones sociales. Quedarían incluidas, por tanto, dentro de esta categoría, formas de criminalidad como el *cyberstalking*, el *cyberbullying*, el *online grooming*, etc.

- Cibercrímenes políticos: Esta última categoría englobaría todos los actos ilícitos que tienen que ver con la lucha ideológica o política. Internet es un medio

> poderoso de comunicación y, por lo tanto, puede ser utilizado para la captación ideológica, para atacar a Estados e instituciones, o para la comunicación entre individuos separados geográficamente pero unidos por un mismo fin político o ideológico.

La particularidad de esta forma de clasificación es que permite que un tipo de ataque, que puede realizarse con intenciones distintas, pueda ser clasificado de acuerdo a la intención y no al tipo. Un claro ejemplo se encuentra en el *hacking,* que puede ser clasificado como ataque económico cuando el propósito sea acceder sin autorización a un sistema informático para obtener datos bancarios con los que posteriormente realizar un ciberfraude. Sin embargo, el acceso sin autorización será categorizado como un ataque político cuando la intención sea acceder a los sistemas de un Estado para obtener información o para inutilizar el sistema. Y finalmente, también podrá ser considerado un ciberataque social cuando el propósito del ataque sea vulnerar la privacidad de una persona concreta.

Todas las definiciones propuestas son útiles para sistematizar las diferentes formas de cibercrímenes. De hecho, pueden ser perfectamente compatibles entre sí[7]. Sin embargo, a los efectos del presente trabajo, se va a tener especial consideración a la última forma

[7] Véase el ejemplo que propone Miró (2012), en su trabajo *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, en la página 50, cuando elabora un cuadro uniendo la clasificación atendiendo a la relevancia de la TIC y la intencionalidad del agresor.

de clasificación, pues desde una perspectiva criminológica, hace hincapié en la intención del agresor y en el objetivo. Y dado que el presente trabajo está centrado en unos ataques muy concretos, donde el propósito del que los realiza es dañar, humillar, atormentar, etc. a una persona concreta, parece más acertado adoptar esta última postura. Por último, y sobre todo, debido a que las conductas concretas que se analizan, pueden no tener relevancia desde un punto de vista jurídico, esta es la clasificación que más interesa. Así, las siguientes líneas están destinadas a hacer un análisis detallado de qué se entiende por cibercriminalidad social y qué conductas, desde una perspectiva criminológica, abarca esta categoría.

3. La cibercriminalidad social: la delincuencia de la web 2.0

3.1. Redes sociales y ámbitos de intercomunicación en el ciberespacio como potenciadores de la cibercriminalidad social

Internet en general, y el uso de los teléfonos móviles en particular, son una parte integral de la vida social de las personas. El desarrollo de Internet, y especialmente la creación de herramientas de comunicación como las redes sociales, permite a los individuos estar en contacto con sus amistades veinticuatro horas al día sin necesidad de estar físicamente en el mismo lugar. También permite compartir a tiempo real con otros usuarios situaciones, sentimientos, instantáneas, etc., con facilidad y a un coste muy bajo. Éstas, y otras particularidades,

han hecho que Internet se haya convertido en el medio principal para la comunicación entre las personas. Sin embargo, compartir la vida privada a través de este medio lleva aparejada la exposición a numerosos riesgos que pueden tener un impacto negativo. Y es que todas las esferas personales que pueden ser puestas en peligro en el espacio físico, al relacionarse con los demás, lo están también en el ciberespacio. Y en la medida que las personas vayan desarrollando su vida personal y social en el ciberespacio, también aumentará el número de comportamientos criminales que podrán sufrir.

La cibercriminalidad social, pues, como ha señalado Miró (2012), es la que se produce en el plano de las relaciones personales entre usuarios que utilizan el ciberespacio para comunicarse entre sí, y eso es lo que hace que esa ciberdelincuencia tenga, al mismo tiempo, algunos caracteres "de novedad", y otros "de clasicidad". En efecto, la gran mayoría de los cibercrímenes sociales o personales que se perpetran no son más que, siguiendo la clasificación fenomenológica de Miró (2012), ciberataques réplica, esto es, copias en el ciberespacio de delitos que ya existían anteriormente pero que sólo se ejecutaban en el espacio físico. Las injurias, las calumnias, las amenazas, el acoso sexual y todo un conjunto de conductas que se pueden realizar sin que sea necesaria una cercanía física entre agresor y víctima, también se pueden realizar cuando ésta existe. Lo único que cambia, por tanto, en estos delitos es que ahora se ejecutan a través de Internet. Y eso es lo que les confiere la "novedad". No tanto porque cambie la naturaleza "jurídica" o "etiológica" de estos crímenes, como porque se realizan en un ámbito de oportunidad criminal distinto que requiere, para la prevención de estas conductas, estrategias diferentes que tengan en cuenta la transnacionalidad del fenómeno, la durabilidad de los

ataques en el tiempo, y otros factores que luego se analizarán más pormenorizadamente.

Pero es indiscutible que la inmensa mayoría de estos cibercrímenes sociales siguen siendo lo mismo que sus referentes en el espacio físico: una injuria a través de Internet es una injuria al fin y al cabo. A nadie escapa, en todo caso, que desde una perspectiva criminológica, como eventos sociales que pueden y deben ser prevenidos, su significado y caracteres son distintos.

Incluso algunos cibercrímenes sociales que parecen no tener referente en el mundo físico lo tienen, si bien lo que sucede es que tales conductas no merecían interés al perpetrarse en el ámbito tradicional de ejecución delictiva y, ahora, al ejecutarse en el ciberespacio, sí parecen tenerlo. Es lo que sucede, por ejemplo, con el *child grooming* o con el *cyberstalking*, comportamientos que se daban en el espacio físico pero que han adquirido mayor notoriedad e, incluso, han dado lugar en algunos países a propuestas de tipificación legislativa para la punición de tales conductas cuando se realizan en el ciberespacio. Esto podría dar lugar a una interesante reflexión sobre si es adecuada la tipificación de conductas sólo cuando se perpetran en Internet sin tener en cuenta que en el mundo físico tales conductas siguen existiendo y en algunos casos, pueden conllevar mayor riesgo y, en cambio, siguen el régimen general jurídico. Esta es, en todo caso, una reflexión que excede de los objetivos del presente trabajo.

3.2. Tipos de cibercriminalidad social

3.2.1. El ciberacoso sexual, el *grooming* y otras formas de ataque sexual en el ciberespacio

De todos los ataques que se pueden llevar a cabo en el ciberespacio contra los menores, los que pueden afectar a la indemnidad y la libertad sexual, son los que crean más alarma social. La unión de los prefijos *online* o *cyber* al término *grooming* (*online grooming* o *cybergrooming)* se emplea para hacer referencia a las conductas llevadas a cabo por un adulto en un contexto virtual para ganarse la confianza del menor y acceder a información esencial para la posterior agresión (Salter, 2003). No existe una única definición del término *grooming* e, incluso, se ha llegado a criticar su uso por centrarse en un determinado tipo de contacto sexual con niños (Eneman et al., 2010). Pero en términos generales, *grooming* hace referencia a los métodos usados por los agresores sexuales para establecer una relación de confianza con el menor (Hoff y Koops, 2011). Este término ha sido definido por Craven, Brown y Gilchrist (2006) como "un proceso por el cual una persona prepara a un niño y su entorno para su abuso. Los objetivos específicos incluyen tener acceso al niño, la satisfacción de las necesidades y el mantenimiento del secreto para evitar la divulgación. Este proceso sirve para fortalecer el patrón pauta abusivo del agresor, ya que puede ser usado como un medio para justificar o negar sus actos" (p. 297).

La conducta de *grooming* es, en realidad, un largo proceso, que comienza con la elección por parte del depredador sexual de un lugar que sea atractivo para el menor o adolescente (Choo, 2009), como

chats, redes sociales, etc. Esto, llevado al espacio físico, podría ser equiparado a los lugares que frecuentan los menores como escuelas, parques, centros comerciales, etc. (Davidson et al., 2011); sin embargo, donde se inicia realmente la conducta, es cuando el depredador sexual selecciona a una víctima. Habitualmente, los agresores buscan víctimas más débiles, especialmente aquéllas con vulnerabilidades relacionadas con la incomprensión familiar o social (McAlinden, 2006). Una vez seleccionado el menor objeto de ataque, se acerca a él, fingiendo ser atractivo para el mismo, haciéndole creer que comparten *hobbies* o que entiende su situación. En otras palabras, le presta un interés particular para que se sienta especial y comienza a ganarse su confianza (Choo, 2009), pudiendo de esta forma obtener información comprometida del menor y consiguiendo, por ejemplo, que éste se conecte a la *webcam* y pose medio desnudo, o le mande fotografías comprometidas. Esta información permite al agresor continuar con el acoso mediante la manipulación del menor, o la amenaza de difundir lo obtenido en Internet o a sus contactos personales (Pereda, Abad y Guilera, 2012).

Se trata pues, de un proceso complejo, donde varía el tiempo necesario para la consecución de los fines (McAlinden, 2006), siendo difícil en muchos casos el establecimiento del momento en el que comienza y termina el ataque (Gillespie, 2004), y donde -a menudo- el estilo empleado suele reflejar la personalidad y la conducta del infractor (Whittle et al., 2013). Este proceso se puede aplicar tanto al mundo real como al virtual, aunque en este último varían sustancialmente las técnicas y las herramientas que puede emplear el agresor (Whittle et al., 2013). En este sentido, Internet ha venido a

facilitar el proceso, tanto en términos de ubicación geográfica[8], como en velocidad de contacto y en número de potenciales víctimas (Davidson et al., 2011).

Internet ha cambiado la forma de hacer *grooming*, pero también ha modificado el perfil del sujeto que lo hace (Young, 2005) y de la víctima que lo padece (Wolak et al., 2008), como consecuencia del distinto ámbito en que esta conducta se realiza (Miró, 2012). Y es que en primer lugar, debemos tener en cuenta que el agresor puede acceder a un mayor número de víctimas potenciales, pudiendo además realizar un estudio previo del perfil para seleccionar a las más vulnerables. En segundo lugar, aumenta el número de que potenciales abusadores sexuales lleguen a serlo porque Internet permite -por un lado- difuminar la percepción del riesgo a ser descubierto, y por otro, vencer el aislamiento social. En consecuencia, a diferencia del abusador sexual clásico que suele llevar a cabo sus ataques contra niños como forma de autogratificación (debido a una necesidad de ejercer poder, por dominio, por control, o por rabia, sin ser consciente en ningún momento del daño infligido), el ciberabusador lo es como consecuencia de sus fantasías sexuales, de los desórdenes psicológicos motivados por la necesidad de escapar de la soledad, de la dificultad de las relaciones personales, o de su baja autoestima, pero es totalmente consciente del significado de su conducta y del daño que puede infligir.

[8] Como explica Miró (2011) y se estudiará con detalle más adelante, Internet ha eliminado las barreras físicas de contacto entre los agresores potenciales y el resto de usuarios, aumentando así el número de posibles víctimas.

El perfil de la víctima también cambia, puesto que los ciberagresores ya no buscan menores de doce años, sino que en general, prefieren chicas adolescentes que ya hayan tenido experiencias sexuales y/o estén dispuestas a tenerlas. En el 99% de los casos, las víctimas son menores entre 13 y 17 años, siendo un 48% de éstos, el porcentaje de las agresiones que se llevan a cabo sobre menores de 13 y 14, mientras que el de las agresiones sobre menores de 15 a 17 años asciende a un 51%, quedando el 1% para víctimas de 12 años (Wolak et al., 2008). De cara a la prevención, es necesario comprender que el acoso real comienza previo envío, por parte de la víctima, de información personal a personas desconocidas, actividad que se conoce como *sexting*. En efecto, una de las prácticas que se ha puesto de moda entre los adolescente es el *sexting,* que consiste en la realización de imágenes propias de desnudos completos o de partes desnudas, y su envío a otros (Agustina, 2010). Los datos publicados por la Diputación Provincial de Alicante y el Centro Crímina (Miró, 2014a), informan que esta práctica la realiza el 8,5% de los adolescentes en el caso del envío de fotos, reduciéndose al 2% cuando se trata de vídeos. Los menores ignoran que este tipo de material puede ser difundido de manera muy fácil y ampliamente, de forma que el remitente inicial pierde totalmente el control sobre la difusión de estos contenidos de carácter sexual. Esta práctica[9], junto a otros riesgos como publicar información personal, permite a los agresores estudiar los gustos de los usuarios, entretenimientos, dirección, nombre completo, etc. Y así

[9] Como ha señalado Agustina (2012), la práctica del *sexting* puede aumentar el riesgo de sufrir confusión, vergüenza, delitos privados, difamación, *bullying* o *cyberbullying*, acoso sexual, extorsión, *grooming*, coerción sexual, abuso sexual o violación *offline,* homicidio o suicidio.

seleccionar a la potencial víctima, no sólo para los casos de acoso sexual, sino también para otras formas de delincuencia que afectan a la intimidad, como veremos a continuación (Miró, 2012).

3.2.2. *Bullying* y *stalking* como formas de acoso continuado en el ciberespacio

De todas las formas de agresiones que se pueden realizar contra un menor, probablemente sea el *bullying* la modalidad que más se haya estudiado. El *bullying*, conocido también España como acoso escolar, comenzó a estudiarse en los años setenta , y desde entonces, unidas al desarrollo de las TIC -y en especial a su popularización entre los jóvenes- se han desarrollado nuevas formas de acoso.

Se han elaborado muchas definiciones de *bullying*, pero la que mayor aceptación parece haber tenido es la propuesta por Dann Olweus (1993), quien considera que "un alumno es maltratado o victimizado cuando está expuesto repetidamente y a lo largo del tiempo a acciones negativas de otro o un grupo de estudiantes" (p.98). La aceptación de esta definición puede deberse a que reúne las tres características fundamentales que constituyen el *bullying*: intención de dañar a una persona, ser repetida en el tiempo [10] y existir un desequilibrio de poder real o imaginario entre el agresor (o agresores) y la víctima (Calmaestra, 2011). Pese a que parece existir acuerdo en la

[10] Definen Smith y Sharps (1994) la conducta de *bullying* como el abuso sistemático de poder (p. 2).

comunidad científica sobre estas tres características, también se ha discutido acerca de si se deben incluir otros elementos, como quién debe protagonizar la agresión, qué debe entenderse por "repetido en el tiempo", qué formas de agresión deben incluirse (física, psicológica o verbal), la percepción de la víctima, o los efectos que tenga (Farrington, 1993; Ortega, Del Rey y Mora-Merchán, 2001).

Paralelamente a esta discusión, hemos visto como la popularización de Internet entre los menores ha hecho que también se haya convertido en el vehículo para cometer el daño intencional y repetido [11], conocido con el nombre de *cyberbullying*. Las tres características que conforman el *bullying* tradicional también son las que configuran el *cyberbullying,* pero incluyendo las TIC como característica esencial para su comisión (Wolak et al., 2007). Así, Smith et al. (2008) definen *cyberbullying* como "una acción agresiva e intencional, desarrollada por un grupo o un individuo, usando formas electrónicas de contacto, repetidas veces a lo largo del tiempo contra una víctima que no puede defenderse fácilmente" (p.376).

Es evidente que la diferencia más clara entre el *bullying* y el c*yberbullying* es el medio empleado para llevar a cabo el acoso sistemático. Y es que Internet proporciona diferentes herramientas para llevar a cabo la acción de maltrato, como el correo electrónico, la mensajería instantánea, las redes sociales, el teléfono móvil, etc. Belsey (2005) hace especial hincapié en las herramientas que pueden emplear los menores para realizar el acoso cuando define el *cyberbullying* en

[11] Patchin e Hinduja (2006) definen *cyberbullying* como el daño intencional y repetido, infligido a través del texto electrónico (p. 152).

estos términos: "*Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others*". Pardo Albiach (2010) en cambio, opta por hacer mayor hincapié en las formas concretas de acoso (atormentar, amenazar, acosar, humillar, avergonzar, etc.), afirmando que el *cyberbullying* se da cuando "un niño, adolescente o preadolescente es atormentado, amenazado, acosado, humillado y avergonzado por otra persona desde Internet, mediante medios interactivos, tecnologías digitales y teléfonos" (p.56). Pese a esta diferencia, muchos autores se han planteado si es realmente el *cyberbullying* una extensión del fenómeno tradicional, o -por el contrario- se trata de un fenómeno con entidad propia. En este sentido, Marco (2010) apunta que se trata de las mismas conductas de atormentar, amenazar, humillar, hostigar o molestar, pero a través de medios tecnológicos, como los son Internet, el teléfono móvil, la videoconsola o cualquier otra tecnología de comunicación. Sin embargo, puntualiza este autor, ambos fenómenos responden a causas distintas y por tanto, tienen consecuencias distintas. En sentido similar, Calmaestra (2011) entiende que es una nueva forma de *bullying* que implica el uso de teléfonos móviles, Internet u otras formas de TIC para acosar amenazar o intimidar deliberadamente y que, por lo tanto, debe mantener las mismas características que el *bullying* tradicional (intencionalidad, repetición y desequilibrio de poder), pero añadiendo ciertos matices que ofrecen las tecnologías de las información, como el anonimato y el carácter público de la agresión; pudiéndose cometer en cualquier momento sin

estar limitado físicamente al espacio escolar. En sentido contrario, señalan Pérez Martínez y Ortigosa Blanch (2010) que, a pesar de compartir características con el *bullying,* el *cyberbullying* tiene una autonomía propia, pues atiende a otras causas, se manifiesta de formas muy diversas y sus estrategias de abordamiento y consecuencias también difieren. Una posición diferente a las anteriormente mencionadas, es la de aquéllos que consideran, como Hernández Hernández y Solano Fernández (2007), que realmente existen dos tipos de *cyberbullying*: "aquél que actúa como reforzador de un *bullying* ya emprendido, y aquella forma de acoso entre iguales a través de las TIC y sin que haya antecedentes previos".

Pero no es sólo el *cyberbullying* una de las formas de acoso continuado que se pueden dar en el ciberespacio. También encontramos el *cyberstalking*, cuya diferencia respecto al primero estriba en los protagonistas de la agresión. Así, estaremos ante un caso de *cyberbullying* cuando el autor que lo realice sea un menor (o varios menores) que dirige sus acciones a otro menor, tal y como plantea Marco (2010) al referirse al "acoso psicológico entre iguales"(p.99). En cambio, estaremos ante un caso de *cyberstalking* cuando la agresión se produzca entre adultos (Miró, 2013b).

Precisamente, si atendemos a la definición de *cyberstalking*, observamos que -en la actualidad- se distinguen dos perspectivas: por un lado, las que se refieren al *stalking* pero trasladado al ciberespacio, y por otro, las que lo definen como una suma de actos de *cyberharassment* (Miró, 2012). Dentro del primer grupo, debemos incluir a Basu y Jones (2007), que entienden por *cyberstalking el "*uso de Internet u otra tecnología de la comunicación para hostigar,

perseguir o amenazar a alguien" (p. 13). En sentido similar, Pathé y Mullen (1997) lo definen como aquellos "comportamientos que un individuo inflige a otro repetidas y no deseadas intrusiones o comunicaciones" (p.12). En el segundo grupo encajaría la definición propuesta por Bocij y McFarlane (2002), que lo conciben 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". Son por tanto, comportamientos que pueden incluir –aunque no están limitados sólo a éstos- la transmisión de amenazas y acusaciones falsas, daños a los datos o equipos, robo de identidad, robo de datos, "monitoreo" informático, la solicitud de sexo y cualquier otra forma de agresión. Por otro lado, Henson (2010) lo define como "cualquier tipo de conducta que utiliza dispositivos electrónicos de comunicaciones, a sabiendas y para cometer voluntariamente cualquiera de los siguientes actos en dos o más ocasiones, y sin ningún propósito legítimo: ponerse en contacto o intentar contactar con alguien después de haberle sido pedido por esa persona que cesara en el contacto; acosar, atormentar o atemorizar a alguien; robar o intentar robar la identidad de alguien o información acerca de esa persona para perjudicarle; hacer insinuaciones sexuales no deseadas o injustificadas hacia alguien; y amenazar con causar un daño físico a alguien"(p. 253).

Independientemente de los tipos de definiciones, parece existir un acuerdo en que tanto el *cyberstalking* como el *cyberbullying* son formas concretas de *cyberharassment,* que se diferencian de este último en el elemento continuidad (Cavezza y McEwan, 2014), afirmando estos autores, para el caso concreto del *cyberstalking*, que se diferencia del *cyberharassment* en que continúa durante un período

más prolongado de tiempo. Esto se refleja claramente en el modo en el que se evalúan estas conductas, que generalmente se refieren a acciones concretas de *harassment*. Otro método empleado, aunque con menor frecuencia, es definir previamente en qué consisten estas conductas dando ejemplos concretos y pudiendo responder por frecuencia de aparición en un determinado tiempo. Véase por ejemplo el cuestionario empleado en la Tesis doctoral de Calmaestra (2011). En este sentido, Del Rey, Elipe y Ortega (2012), para el análisis del c*yberbullying,* preguntan en su estudio por tres tipos de conductas: robo de identidad, publicación de imágenes o vídeos en situaciones comprometidas o embarazosas, y abuso indirecto (extender rumores), pudiendo los encuestados contestar con qué frecuencia al mes les ocurría. Del mismo modo, Vandebosch y Van Cleemput (2009) preguntan por acciones concretas: entrar en el buzón del correo electrónico o en las cuentas de mensajería instantánea y cambiar la contraseña, enviar intencionalmente virus, entrar en el ordenador y robar información personal, enviar un número grande de correos a una persona para sobrecargarle el sistema, amenazas o insultar, excluir de un grupo, difundir información privada, entrar en el correo y enviar correos en su nombre, publicar o reenviar un correo con información confidencial y lanzar rumores.

Ejemplos similares de este tipo de estudios, los podemos encontrar en el *cyberstalking*. En este sentido, Henson (2011) utiliza cuatro formas de *cyberharassment* para evaluar el *cyberstalking*, incluyendo como requisito la continuidad: recibir contacto no deseado en más de una ocasión cuando se le ha pedido que no lo hiciera; haber sido hostigado o molestado de forma persistente; haber recibido insinuaciones sexuales no deseadas en más de una ocasión y haber

sido amenazado físicamente más de una vez. Un método similar emplea Reyns (2010), quien considera víctima de *cyberstalking* a aquella persona que haya recibido contacto no deseado, haya sido molestado y hostigado, haya recibido propuestas sexuales no deseadas, o haya sido amenazada, pero todo ello siempre de manera continuada durante un periodo de tiempo.

Estos ejemplos ponen de manifiesto que tanto el *cyberbullying* como el *cyberstalking* pueden adoptar múltiples formas, o lo que es lo mismo, se pueden llevar a cabo mediante la realización de variadas formas de agresión. Dependerá de los protagonistas de la agresión y de la continuidad de ésta, la calificación del comportamiento como *cyberbullying o* como *cyberstalking.* Sin embargo, este último aspecto –la continuidad- que ya planteaba problemas en el espacio físico, aún los presenta más en el ciberespacio. Advertía Olweus (1993) para la modalidad *offline* que, si bien es necesario que el daño sea repetido durante un periodo de tiempo, hay actos en los que -dada la gravedad que entrañan- es suficiente con que la víctima lo haya padecido en una ocasión. Lo mismo podría suceder con el *cyberbullying*, donde una única conducta puede generar efectos negativos graves; no obstante, esta cuestión plantea más dudas en la modalidad *online,* pues el ciberespacio presenta la especial capacidad de hacer perenne lo que en el espacio físico es caduco (Miró, 2011). Así, por ejemplo, el resultado de publicar un comentario o una foto con intención de humillar a una persona puede ser visto en múltiples ocasiones por personas distintas, por lo que un solo acto puede convertirse en una humillación continua (Calmaesta, 2011; Vandebosch y Van Cleemput, 2009). Por ello, será necesario reconsiderar el criterio de repetición en función de cada caso concreto y del tipo de agresión.

3.2.3. Cyberharassment o ataques individualizados de acoso en el ciberespacio

El término *cyberharassment,* sinónimo de *online harassment*, suele emplearse para referirse a actos concretos de acoso en el ciberespacio (Miró, 2012). Esta conducta ha sido definida por Finkelhor et al. (2000) como "las amenazas u otro tipo de comportamiento ofensivo (no sexual) con jóvenes vía *online* o la publicación *online* de información sobre un joven para que otros lo vean" (p.11). La diferencia con el *cyberbullying,* pues, estriba en que con el término *harassment* se hace referencia a las conductas individualizadas de acoso que pueden constituir, o no, parte de un *cyberbullying.* Es por ello que el *online harassment* adopta formas muy variadas, entre las conductas más habituales están las humillaciones frente a otros en la Red, los mensajes amenazantes, la distribución de fotos trucadas, o la suplantación de identidad. Sin embargo, éstas no son las únicas formas de acoso que se pueden ejercer a través de la Red y además, todo apunta a que seguirán expandiéndose en la medida que vayan evolucionando las TIC (Cavezza y McEwan, 2014).

De entre todas las clasificaciones tipológicas en relación con el *harassment* que proponen los autores, podemos distinguir tres clases: aquéllas que hacen distinción en base al medio empleado, las que se refieren expresamente al empleo de las herramientas que proporciona Internet, y las que hacen referencia al tipo de comportamiento (Slonje et al., 2013). Avilés, Irurtia, García-López y Caballo (2011) realizan una propuesta interesante para distinguir los tipos de acoso: aunque

incluyen los casos de *bullying* tradicional, puede servir para clasificar únicamente los ciberataques. Así, distinguen entre agresiones en base a la forma (agresiones que toman formas verbales, de exclusión social, de alto daño psicológico focalizadas en un aspecto concreto como racismo, homofóbico, etc.); en base al fondo (sobre las intenciones de los que actúan y los efectos que producen: exclusión, difamación, humillación, suplantación, chantaje, etc.); y en base al escenario (mensajería instantánea, correo electrónico, páginas web, blogs, redes sociales, etc.).

Las dos iniciales distinciones hacen referencia al medio, aludiendo la primera a un ámbito más general, distinguiendo así entre móvil e Internet; mientras que la segunda hace referencia a la herramienta concreta usada (redes sociales, chat, etc.) Así, podríamos hacer referencia a la mensajería instantánea (por ejemplo, WhatsApp o Line) en el caso del teléfono móvil, y el correo electrónico o las redes sociales en el caso de Internet. No obstante, con la nueva generación de teléfonos móviles que integran todas las aplicaciones de Internet (correo electrónico, redes sociales, etc.), es difícil distinguir entre móvil o Internet para realizar el acoso.

Siguiendo la línea de distinguir las conductas de acoso dependiendo de la herramienta, encontramos la propuesta de Smith et al. (2008), quienes distinguen siete tipos de conductas de acoso: mensajes de texto, acoso telefónico, acoso a través de fotografías/vídeo, acoso a través de correos electrónicos, acoso a través de sesiones de chat, acoso a través de programas de mensajería instantánea y acoso vía páginas web.

Sin embargo, más interesante resulta distinguir los tipos de conductas agresivas a partir de los comportamientos que pueden llevar a cabo los usuarios a través de Internet (por ejemplo: amenazas, insultos, exclusión, etc.). Y es que en realidad, una misma acción dañina se puede realizar a través de diferentes herramientas sin que ello tenga mayor trascendencia con respecto a la conducta. Por ejemplo, una persona puede amenazar a otra a través de la mensajería instantánea o través de correo electrónico, sin que deje de ser la misma acción, pues en ambos casos estamos ante una amenaza. Por tanto, lo importante no será tanto el medio, sino la acción y la repercusión que pueda tener para la persona.

En este sentido, Nocentini et al. (2010) distinguen cuatro tipos de acoso que se pueden realizar a través de las TIC:

- Los comportamientos escritos-verbales (*written-verbal behaviours*), que incluirían llamadas de teléfono, mensajes de texto, correos electrónicos, mensajes instantáneos, chat, blogs, redes sociales, páginas web, etc.
- Comportamientos visuales (*visual behaviors),* como postear, enviar o compartir videos o fotografías comprometidas con otros mediante el teléfono móvil o Internet.
- Exclusión (*exclusion*), que sería el excluir a alguien –de forma intencionada- de un grupo *online*.
- Suplantación *(impersonation),* que sería el caso de robar y revelar información personal, usando el nombre y la cuenta de otra persona.

Otra interesante distinción es la que realizan Vandebosch y Van Cleemput (2009) al señalar conductas de *cyberbullying* directas e indirectas. Las directas son los tipos de conducta en las que la víctima se ve envuelta directamente; distinguiendo dentro de esta categoría -a su vez- otras cuatro: contra la propiedad (lo que podría ser el envío de *malware* para dañar el equipo o un archivo), verbal (que incluye el uso de Internet o el móvil para insultar o amenazar), no verbal (envío de imágenes o ilustraciones obscenas o amenazantes) y social (excluir a una persona de un grupo *online)*. En la segunda categoría, *cyberbullying* indirecto, la víctima no se ve envuelta directamente en la conducta, como sería el caso de hacerse pasar por alguien, expandir cotilleos o rumores, participar votando en una página web que se dedica a difamar a alguien, etc.

Otra clasificación posible, es la que llevan a cabo Kowalski, Limber y Agatston (2010), sobre la base de los tipos de conducta, identificando los ocho siguientes:

- Peleas *online* (*flaming)*: esta categoría hace referencia al intercambio de palabras breve y acalorado entre dos o más personas con un lenguaje hostil y vulgar, que tiene lugar a través de alguna de las nuevas tecnologías. Incluye tanto el intercambio de mensajes privados, como hacerlo en contextos públicos.
- Hostigamiento: se trata de mensajes ofensivos, reiterados y enviados a la persona elegida como blanco por correo electrónico, en foros públicos como salas de

chat y foros de debate; incluyendo también el envío de mensajes de texto al teléfono móvil. Difiere de los insultos porque el hostigamiento es a más largo plazo y más unilateral (incluyendo a uno o más ofensores frente a una única víctima).

- Denigración: es la modalidad que implica descalificar a alguien *online,* difundiendo información despectiva y falsa de una persona, bien a través de una página web o bien vía e-mails, mensajes instantáneos, etc. Esta conducta se puede llevar a cabo por ejemplo, mediante el envío de imágenes crueles o rumores acerca de una persona para dañar su reputación, enviando fotos (alteradas digitalmente) de alguien, etc.
- Suplantación: es usar la cuenta de alguien sin autorización para enviar mensajes que hacen quedar mal a su propietario, o bien le ponen en una situación problemática o en peligro, o bien dañan su reputación.
- Desvelamiento y sonsacamiento: este tipo de conducta implica revelar información comprometida de la víctima a otras personas, enviada de forma espontánea pero privada por la propia víctima, o que ha sido sonsacada a la víctima y después difundida a otras personas.
- Exclusión: supone no dejar participar a una persona en una red social o un grupo *online* específico.
- Ciberpersecución: es la conducta consistente en el envío de comunicaciones electrónicas reiteradas hostigadoras y amenazantes.

- *Happy Slapping*: esta última conducta, que ha sido traducido al español como "paliza feliz" (Goraigordobil, 2011, p.237), consiste en grabar mediante la cámara de los teléfonos móviles imágenes en las que se agrede a una persona y luego son compartidas con amigos o publicadas en algún espacio *online* para que las vean muchas personas.

Esta clasificación viene a completar la propuesta inicialmente por Willard (2007), quien distinguía siete tipos de conductas: flaming*, harassment, denigration, impersonation, outing or trickery, exclusion, cyberstalking.* Por su parte, Buelga et al. (2010) proponen en su estudio las siguientes conductas basadas en la clasificación de Willard: hostigamiento (insultar o ridiculizar, y decir o enviar "cosas guarras"); persecución (obligar a hacer cosas con amenazas o amenazar para meter miedo); denigración (difundir mentiras y rumores falsos); violación de la intimidad (compartir secretos, difundir o manipular fotos de personas (o de la familia) sin permiso, y acceder a las cuentas privadas); exclusión social ("me han llamado/ me han dicho de conectarme y no han contestado"); y suplantación de la identidad (hacerse pasar por alguien para decir o hacer cosas malas en Internet).

A todas estas conductas habría que sumar aquellas otras relacionadas inicialmente con la cibercriminalidad económica, pero que pueden ser entendidas como cibercriminalidad social, si el propósito de quien las ejecuta es molestar, atormentar o acosar. En este sentido, Bocij (2003) incluye en su estudio sobre *cyberstalking*

conductas como animar a otras personas a acosar, amenazar o insultar, suscribirse a servicios para cargar gastos a sus tarjetas, enviar *software* malicioso para dañar el equipo, y enviar troyanos para controlar el sistema informático.

En definitiva, tanto menores como adultos pueden sufrir una amplia gama de ataques en el ciberespacio que pueden afectar al honor, la intimidad, la dignidad, la libertad, la privacidad, o similares. Y, como veremos más adelante, dada la configuración del nuevo espacio, permiten su realización con mayor facilidad.

3.3. Concepto de cibercriminalidad social y relación con su relevancia jurídica a los efectos de este trabajo

El objeto del presente trabajo es la cibercriminalidad, específicamente la cibercriminalidad de tipo social y aún más concretamente, conductas de ciberacoso que podrían entenderse englobadas dentro del cyberharassment. De todas las formas que puede adoptar la cibercriminalidad social, este trabajo sólo abarca la manifestación concreta de algunas (de las muchas) conductas que pueden ser consideradas como ciberacoso. Y no se centra exclusivamente en unas formas concretas de la cibercriminalidad social, sino que además las aborda desde la perspectiva de quien la sufre: la víctima. Sin embargo, el concepto de víctima, no está exento de discusión por parte de la doctrina, por lo que se hace necesario aclarar cuál es la postura que se ha seguido durante el desarrollo del trabajo y, más allá de esto, las razones de la misma. Asimismo, algunas de las conductas que van a ser analizadas en el estudio criminológico que

conforma la principal parte de esta tesis pueden no constituir un "delito", en sentido jurídico. En este sentido, resulta también necesario, explicar cuál es el concepto de cibercrimen que adoptamos y el objeto concreto de la investigación.

Comenzando con la justificación acerca de la postura escogida sobre el concepto de crimen, hemos partido de una perspectiva criminológica. Nadie discute que el delito es uno de los objetos de estudio de la Criminología y, casi con total seguridad, el más importante, pues de él derivan otros objetos de estudio como la víctima o la reacción social frente al mismo. Ya Sutherland, a principios del siglo pasado, definió la Criminología como "el cuerpo de conocimientos sobre el delito como fenómeno social" (p.3). Sin embargo, no es la única definición que ha puesto de manifiesto que el estudio de las causas del delito es la principal actividad de la Criminología (Serrano, 2009), pues en este sentido, García-Pablos (1999) la define como "la ciencia empírica e interdisciplinaria que se ocupa del crimen, del delincuente, de la víctima y del control social del comportamiento desviado". Y por último, otra más reciente, es la propuesta por Garrido, Stangeland y Redondo (2001) quienes la entienden como "ciencia que estudia los comportamientos delictivos y las reacciones sociales frente a ellos" (p. 47).

Sin embargo, a pesar de que existe un acuerdo unánime en que la Criminología se centra en el estudio del delito (o del comportamiento delictivo), no existe tal consenso a la hora de delimitar el alcance del concepto. Aun a riesgo de simplificar en exceso, podría admitirse que hay dos grandes posturas: los que consideran que el concepto de delito debe estar limitado al concepto de delito

normativo, frente a los que consideran que no debe limitarse. Los que apuestan por la primera postura se basan en el principio de legalidad, y por lo tanto, entenderán comportamiento delictivo todas aquellas conductas que estén descritas (tipificadas) en las leyes penales. En otras palabras, las conductas que no estén recogidas en la norma penal no podrán ser consideradas delitos, por muy injustas o dañinas que puedan ser (Serrano, 2009). Asiste razón, probablemente, a quienes defienden esta posición, al señalar ciertos riesgos que podría conllevar esta desconexión entre "crimen" en sentido criminológico y "crimen" en sentido jurídico, pero también se admite que con ello se puede estar restringiendo en exceso el objeto de estudio.

Frente a esta postura, se encuentra la de los que consideran que la noción criminológica del comportamiento delictivo, como constructo más complejo, no debe quedarse sólo en ese puro concepto normativo del delito, sino que ha de dirigir su atención hacia otros elementos no esencialmente delictivos. Así ocurriría, por ejemplo, con las conductas problemáticas o antisociales que puedan ser predictoras de la posterior delincuencia, y los diversos factores biopsicológicos y sociales que puedan ser facilitadores de ella. Explican Garrido y Redondo (2013) que el concepto legal de delito no clarifica qué elementos caracterizan a los comportamientos delictivos, ni por qué deben ser considerados más graves que otros. De hecho, el propio Serrano (2009) reconoce que adoptar de forma estricta la primera postura, podría parecer "insatisfactorio desde un punto de vista científico" (p.69). Y en este sentido, ya apuntaba García-Pablos (2003) que podría adoptarse "una nueva actitud metodológica, flexible, que acentúa la funcionalidad del concepto de "delito", a los efectos de optar a favor de una noción jurídico-formal (penal) o material, según

las finalidades de la investigación criminológica [...] A tenor del mismo, carece de sentido cualquier decisión apriorística que condicione fatalmente –y limite o impida- los propósitos de esta investigación" (p. 101).

A nuestro humilde parecer, es importante asumir la relevancia funcional y práctica que tiene, en la investigación, la determinación del objeto de estudio. Con esto lo que se afirma es que el objetivo de la investigación debe ser absolutamente definitorio del objeto y, a la vez, reconocer que ello no puede conllevar una generalización del mismo a otro tipo de investigaciones. En otras palabras, para decidir cuál es el objeto de crimen adoptado en este estudio, vamos a tomar en consideración los objetivos específicos de esta investigación, lo cual supone que no se pueda generalizar tal definición del objeto a cualquier otro estudio que se realice, por ejemplo, con propósitos distintos.

En este sentido, creemos que es interesante revisar los argumentos que recoge y sintetiza Serrano (2009) por parte de quienes consideran que la Criminología no puede aferrarse a un concepto normativo de delito, y, a la vez, examinar algunas de las razones por las que este mismo autor considera necesario asir su propio concepto de delito al concepto legal. Y esta revisión se realizará teniendo como norte cuales son los objetivos concretos de esta investigación que presento.

Respecto a los argumentos a favor de un concepto no legalista de crimen que aduce Serrano (2009), tres pueden ser perfectamente

empleados a los efectos del trabajo para seguir esta última corriente[12]: "b) el legislador, que es quien legítimamente establece qué conductas son delito, no sigue un criterio satisfactorio desde el punto de vista de la explicación causal del delito, sino que predominan los históricos y de oportunidad. De este modo es difícil que pueda darse una explicación científica general convincente de una materia en la que elementos irracionales y contradicciones tienen una fuerte presencia; c) las leyes penales son irremediablemente vagas e imprecisas, hasta el punto que los jueces y los juristas en general no siempre llegan a acuerdos generalizados sobre su interpretación; y d) las leyes penales son cambiantes: con relativa rapidez se tipifican nuevas conductas, mientras que delitos tradicionales se redefinen o bien dejan de estar castigados"(p. 70). Este último argumento es especialmente importante a los efectos que nos interesan. Si, como señala Morillas Cueva (2006, 2008), el Derecho penal sólo debe encargarse de sancionar las conductas que afecten a los que sean considerados valores esenciales del individuo y de la sociedad en un momento determinado, y

[12] Los otros dos argumentos se desechan porque no aportan relevancia al tema tratado. Estos son "a) No parece asumible que el objeto de estudio de una disciplina venga impuesto desde fuera de la misma, es decir que sea competencia externa la delimitación del mismo. Antes al contrario, lo lógico es que cada disciplina defina ella misma qué va a estudiar y cuál es su contenido y naturaleza; e) Los autores críticos que sostienen que las leyes en general y las penales en particular responden a los intereses de los grupos sociales dominantes –y ello tanto en el momento de su tipificación como, sobre todo, en el más importante y decisivo de su interpretación y aplicación-, y tienen por lo tanto la función de protegerlos; afirman que una concepción legal del delito en el fondo legitima involuntariamente las diferencias sociales y desvía la atención de los comportamientos dañosos más graves para la sociedad en general, como son precisamente algunos de los que llevan a cabo dichos grupos para el mantenimiento de sus intereses y sus posiciones de privilegio" (Serrano, 2009, p. 69 y ss.)

asumimos la rapidez del cambio tecnológico y, unido a él, del social, puede suceder que haya intereses sociales que sean dignos de tutela pero aún no hayan sido incorporados al sistema penal, y sin embargo, merezcan ser objeto de estudio, por ejemplo, para conocer su prevalencia real.

Frente a estos argumentos, y en concreto frente al concepto no unitario de delito de García Pablos, señala Serrano que esta propuesta es legítima pero "corre el riesgo de caer en innumerables investigaciones desconectadas entre sí que en realidad hablen de cuestiones completamente distintas y lleguen, por lo tanto, a conclusiones opuestas, lo cual complicaría y limitaría el progreso de la ciencia".

Pues bien, y como a continuación se expresará, son variadas las razones por las que se ha decidido no asir el concepto de ciberacoso a lo legal y utilizar como variables dependientes conductas de "cibercrimen" que pueden no ser, conforme a nuestro sistema penal, delictivas. Pero la principal de ellas es, precisamente, el riesgo, en el caso de que se utilizara el concepto legal, de realizar una investigación totalmente desconectada de las similares que se están realizando en otras partes del mundo, especialmente en EE.UU. y el mundo anglosajón, y no precisamente por una diferencia del régimen legal, sino porque allí el objeto cibercriminalidad sí está claramente desconectado de la definición legal de crimen. Si eso es un argumento de peso, como con razón entiende Serrano (2009), a favor de una conceptualización u otra, en este caso consideramos que debe jugar a favor de la separación entre el concepto legal y el criminológico, como a continuación se explica.

Como ya se ha avanzado, la pretensión principal de este trabajo no es únicamente obtener los datos de prevalencia de unas determinadas formas de ciberacoso, sino que es –y en aras a la prevención- determinar qué conductas cotidianas de las que realizan las víctimas tienen mayor incidencia en su proceso de victimización. Para ello, se ha empleado una metodología más que aceptada y validada en las investigaciones criminológicas y victimológicas: las encuestas de victimización[13]. Aunque el procedimiento seguido se explica más adelante (parte 2, capítulo 1), es necesario ir adelantando que para el estudio objeto de este trabajo se ha preguntado a las víctimas por unas formas concretas de victimización que la comunidad científica ha identificado como conductas de acoso, y que provocan consecuencias negativas en las personas que las padecen. En este sentido, seguir tal metodología, pero atendiendo a un concepto penal de ciberacoso a menores, nos habría planteado dos problemas, que se expondrán a continuación.

El primero de ellos, surge en relación a una cuestión de comparabilidad. En primer lugar, porque si se atiende únicamente al ordenamiento jurídico español, los resultados obtenidos sólo tendrían valor en este ámbito geográfico. Y en segundo lugar, porque impediría hacer comparaciones con otros estudios realizados hasta la fecha, que han sido modelo de base para el planteamiento de este trabajo.

[13] Para conocer la evolución de las encuestas de victimización y la implicación en el desarrollo del estudio de la criminalidad, se recomienda consultar Luque Reina (2006), Garrido y Redondo (2013), Pereda Beltrán (2013), Aebi y Linde (2010).

El segundo de los problemas vendría originado porque no existe en el vigente Código Penal español un tipo específico que castigue el ciberacoso a menores, por lo que la jurisprudencia ha ido reconduciendo a los distintos tipos penales existentes las diferentes conductas de acoso a menores a través de Internet sobre la base de los diferentes bienes jurídicos que pueden ser dañados o puestos en riesgo por los distintos ciberataques (Miró, 2013b). Este hecho (entre otros) que a continuación se expondrán, hace que sea bastante complicado operativizar variables con precisión jurídica, lo que no significa que sea imposible. Sin embargo, sirva como ejemplo precisamente el acoso a menores a través de los delitos contra la integridad moral, donde habría que incluir algunos elementos -que incluso son discutidos por la doctrina, por poder prescindir de ellos en el caso de que la entidad del ataque sea tal que, pese a realizarse en una ocasión, suponga una suficiente afectación a la integridad moral de la víctima- como la continuidad de la conducta. Se podría preguntar, por tanto, a un menor de doce años: "¿alguien ha realizado de manera continua alguna conducta a través Internet que haya dañado o afectado tu integridad moral?" o "¿se ha visto alguna vez afectada o dañada tu dignidad a causa del comportamiento que ha realizado otra persona a través de Internet?". Desde un punto de vista metodológico sería incorrecto, pues si ya es difícil para la gente lega en Derecho distinguir entre hurto y robo (y por eso muchas encuestas de victimización no distinguen entre estos dos conceptos), aún resulta más difícil introducir términos como integridad moral. En cualquier caso, no se niega que se pueda llegar a elaborar una encuesta que satisfaga este aspecto, pero preferiblemente se debería optar por otro tipo de metodologías, sobre todo de corte cualitativo (como las

entrevistas en profundidad), que permitiesen alcanzar estos objetivos salvando los inconvenientes encontrados. Y de hecho, sería un complemento perfecto para las investigaciones como la que aquí se ha llevado a cabo, cuyos resultados por sí mismos, no sólo son útiles para el diseño de estrategias de prevención, sino que también pueden serlo para la respuesta penal (Tamarit, 2014).

Circunscribirse, por tanto, a un concepto legal de ciberacoso, como único y excluyente, conllevaría dejar de lado cuestiones que sí se deben tener en consideración como su etiología, la fenomenología, la dinámica y la estructura, y, sobre todo, obligaría a cambiar por completo el objeto de la investigación. Por ello en este trabajo, y de forma totalmente aceptada por la comunidad científica, se utiliza un concepto de víctima como el de una persona que puede no haber sufrido un hecho que podría ser constitutivo de un ilícito penal. En este sentido, ha expresado Tamarit (2006) con acierto que "no puede desconocerse la existencia de situaciones que pueden ser definidas en términos de victimización, con la presencia de una víctima y, frecuentemente, de un ofensor perfectamente identificables, y que, pese a su proximidad con lo penal, no pueden ni deben ser concebidas como hechos delictivos. Nos referimos a los fenómenos que tienden a ser descritos en gran medida por los efectos que producen en la víctima, conocidos con términos como *stalking, bullying, mobbing, harassment*" (p. 21).

Y es que el concepto de víctima, como objeto de estudio de la Victimología, tampoco está libre de discusiones doctrinales. Sin querer entrar a valorar cuestiones relacionadas con el alcance del objeto de estudio de la Victimología, pues no tienen relevancia a los efectos del

presente trabajo, es necesario apuntar que también la definición de delito afecta al concepto de víctima. En este sentido, parece que la doctrina mayoritaria también ha apostado por no ceñirse a un concepto normativo de delito. Así, argumenta Tamarit (2006) que "si en el ámbito de la Criminología un destacado sector doctrinal ha defendido la necesidad de reconocer un objeto amplio de la disciplina que comprenda el estudio de la desviación social y comportamientos no delictivos, con mayor razón procede en nuestro ámbito de estudio una apertura a tal clase de fenómenos de victimización" (p. 21). Siguiendo este hilo argumental, afirman Morillas, Patró y Aguilar (2011) que "la mayoría de las conductas que en un futuro serán constitutivas de delito, por cuanto generan un daño a la víctima, antes de su incorporación al Código Penal han sido sometidas a un seguimiento desde un prisma victimológico –incluso criminológico- de acuerdo a la acepción crimen social" (p.34).

A los efectos del presente trabajo, se opta por un concepto de víctima derivado de la Victimología criminal definido como "individuo o grupo de personas que sufre un daño producido por una conducta antisocial, propia o ajena, aunque no sea el detentador del derecho vulnerado" (Morillas et al, 2011, p. 102). En cualquier caso, como pone de manifiesto Morillas et al. (2011) "no existe un concepto unitario de víctima y su definición dependerá, en todo caso, del campo o rama jurídica o social en la que pretenda desenvolverse. Ahí es precisamente donde radica la esencia del concepto victimal, en la destreza que debe manifestar el investigador para optar por una u otra conceptualización según la finalidad perseguida y los objetivos en la investigación" (p.102).

4. Caracterización estructural de Internet como nuevo y distinto ámbito de oportunidad

Los teóricos de la Criminología ambiental como Brantingham y Brantingham (1981), Ekblom (1995) o los creadores de la Teoría de las actividades cotidianas (Cohen y Felson, 1979), establecieron que el lugar en el que ocurren los delitos es determinante para su comisión y, por lo tanto, entenderlo es fundamental para conocer la etiología del delito. Así, para comprender el fenómeno de la cibercriminalidad será necesario analizar el lugar, dado que se da en un ámbito que no es el tradicional espacio físico. En otras palabras, hay que analizar en qué cambia el ciberespacio con respecto al espacio físico, y cómo afecta este hecho al crimen que en él se produce. Las preguntas, por tanto, serían: ¿Cómo es el ciberespacio? ¿En qué se diferencia del espacio físico? ¿Cómo repercuten sus características en los eventos delictivos?

Indica Williams (2007) que el crimen, como cualquier actividad social, es dependiente del espacio y del tiempo. En este sentido, hay que entender que el ciberespacio surge de la interconexión entre los usuarios a través de las TIC. Por ello, cuando se dice que el ciberespacio es un espacio de comunicación (Lévy, 1998), es porque resulta de la actividad social de los usuarios a través de los ordenadores conectados entre sí (Mayans, 2003). Sin embargo, Aguirre Romero (2004), va más allá al señalar que sin la comunicación entre usuarios no existiría la red:

> "El ciberespacio existe solamente como espacio relacional; su realidad se construye a través del intercambio de información; es decir, es espacio y es medio. Una red sin interacción entre sus miembros deja de ser una red; la red existe porque existen relaciones entre sus integrantes" (Aguirre Romero, 2004).

El hecho de que sea necesaria la comunicación para que exista el ciberespacio, marca la primera diferencia con el espacio físico, pues este último existe independientemente de las relaciones que surjan en él. Es decir, dos personas se podrán relacionar en un espacio físico cualquiera y seguirá ahí cuando acabe esa relación (Aguirre, 2004), mientras que "el ciberespacio agota su existencia en cuanto él mismo, sirva para la comunicación entre los sujetos, dado que sin interacción no hay red" (Miró, 2012, p. 146).

Pero si hay algo que cambia sustancialmente entre los dos espacios, es la configuración espacio-temporal. Y es que no existen distancias en el ciberespacio, no se puede hablar de cercanía, proximidad o separación, porque todos los puntos tienen la misma distancia entre sí (Yar, 2005). Lo que sucede en el ciberespacio es que las distancias se reducen y, por consiguiente, el espacio se contrae y, por ello, el término distancia se mide, no sólo en los kilómetros que se tarda en recorrer de un sitio a otro, sino también en el tiempo que se tarda en llegar (Puebla, 1998). En este sentido, dice Puebla que "el tren de alta velocidad y el transporte aéreo producen ciertamente una espectacular compresión del espacio, al reducir las distancias en tiempo" (p. 72). Por tanto, en la medida que el tiempo necesario y el coste se reduce, la distancia es cada vez menor y, en este sentido, las

distancias en el ciberespacio desaparecen porque la comunicación entre dos personas a través de Internet puede ser inmediata, independientemente del lugar físico en el que se encuentren.

Que la distancia deje de ser un obstáculo, tiene como consecuencia la expansión comunicativa (Miró, 2011, 2012), y en este sentido, señala Green (2002) que lo que ocurre en el ciberespacio es que hay una compresión espacio-temporal porque se reduce el tiempo necesario para cubrir una distancia, pero hay un estiramiento en la medida que aumenta el contacto entre la sociedad y por tanto, la eliminación de las barreras físicas acerca a un mismo espacio a todos los usuarios de Internet (Miró, 2011, 2012). En otras palabras, la superación de las limitaciones espacio-temporales impuestas por el espacio físico, permite a las personas interaccionar con todas aquéllas que estén ubicadas dentro de la red global de comunicaciones, "haciendo viable la idea de la aldea global" (Cabero, 1996, p.2).

En cuanto al tiempo, no es su reducción el único cambio provocado por la contracción de las distancias, sino que otra de las particularidades que presenta el ciberespacio en cuanto al tiempo, es que la comunicación entre dos personas puede suceder en dos momentos temporales distintos. Es decir, el emisor puede enviar un mensaje de texto en un momento temporal determinado y ser recibido más tarde por el receptor. En palabras de Cabero (1996) "el tiempo puede ser el mismo y también diferente entre el emisor y el receptor, facilitándose de esta forma la flexibilidad en la comunicación, y permitiendo que las personas para comunicarse no tengan por qué estar en el mismo momento temporal". Incluso, como apunta Miró (2011, 2012), el ciberespacio permite que algo que en el espacio físico

es caduco, sea perenne. Es decir, acciones como la publicación de contenidos, pueden quedar fijadas en el ciberespacio de manera indeterminada y seguir produciendo efectos. No obstante, la compresión del tiempo y del espacio, y la consiguiente expansión comunicativa, lo es tanto para lo positivo como para lo negativo, pues como apunta Landry (2008), produce cibercrímenes y hace que viejos delitos ahora sean más fáciles de cometer.

Sin embargo, no son el tiempo y el espacio las únicas características que diferencias el espacio físico al virtual. Como ha señalado Miró (2011), la configuración del ciberespacio está marcado por otras características extrínsecas, probablemente derivada de las anteriores, que tienen efecto sobre todos los eventos que en él se producen. La primera, y seguramente la más significativa, es su carácter transnacional (Gómez, 2005). El ciberespacio ha supuesto la eliminación de las tradicionales fronteras del espacio físico, permitiendo así que un individuo pueda acceder desde cualquier Estado nacional a una página web alojada en un servidor situado en cualquier otro Estado nacional. Como explica Miró (2011, 2012), esto supone que Internet no pertenece a ningún Estado concreto pero que se puede acceder desde cualquiera de ellos. Lo que supone una expansión sin procedentes de la comunicación, cambiando por completo el concepto de comunidad. Como ha indicado Fonseca (2003), "ese espacio sin espacio (referido al ciberespacio) reconfigura también las nociones del límite. Las comunidades virtuales transcienden no sólo las fronteras nacionales o continentales… Las comunidades virtuales son transterritoriales pero a su vez translingüísticas y transculturales" (p. 16). Afirma Ribeiro (2002) en este sentido, que el ciberespacio es "una especie de universo transnacional,

hiper-postmoderno donde tiempo, espacio, geografía, fronteras, identidades y cultura simulan inexistir o ser irrelevantes".

La transnacionalidad del ciberespacio dificulta el seguimiento y control de la cibercriminalidad. Y es que, en realidad, Internet se configura a partir de la conexión entre sistemas, es decir, es una malla donde ningún nodo tiene el poder de aislar a otro no-nodo, por lo que la inutilización de uno no impide que Internet siga fluyendo (Alcántara, 2011). Este carácter "no centralizado[14] y distribuido" de Internet, e incluso "deslocalizado" en el sentido de que no está situado en un lugar concreto sino en todos a la vez, (Miró, 2011, 2012), impide que haya una autoridad centralizada que pueda ejercer algún tipo de control o de censura sobre las interacciones que en él se produzcan (Romeo, 2006), o lo que es lo mismo, que no está limitado a las leyes nacionales de un único país (Miró, 2011, 2012).

A su vez, que en el ciberespacio no hayan unidades centralizadas que puedan bloquear las conexiones entre nodos debido a su carácter transnacional y distribuido (Papakonstantinou, 2010), permite a los usuarios navegar libremente sin censuras. Es a esto a lo que se alude cuando se habla de la neutralidad de la Red, a la capacidad de comunicación desde un punto a otro del ciberespacio sin que se vea alterado el contenido (Alcántara, 2011; Suarez, 2013).

[14] Explica Alcántara (2011) que es más adecuado hablar de ciberespacio "distribuido" y no de "descentralizado", porque empleando el segundo término podría significar que hay nodos locales que se unen en una red entre sí.

Por otra parte, son quizás todas estas características mencionadas las que han hecho que el ciberespacio se haya convertido en un lugar para el intercambio, tanto económico como social, pues su uso se ha extendido entre todas las sociedades y el mundo. Su carácter universal y popular lo demuestran los últimos datos recogidos por el Banco Mundial[15], apuntan a que tan sólo hay diez países en el mundo donde el porcentaje de usuarios de Internet sea inferior al 2%. Sin embargo, frente a este grupo encontramos países como Estados Unidos, Canadá o algunos de Europa, donde el porcentaje de población usuaria se eleva al 90%. El aumento de usuarios conlleva la concentración en un mismo espacio no solo el número de potenciales agresores sino también un mayor número de objetivos sobre los que dirigir el ataque.

El uso continuo de Internet y de los sistemas de conexión por gran parte de la población mundial ha hecho (y continua haciendo) que estén en permanente evolución y cambio. Echando la vista atrás se puede observar como las formas de consumo y comunicación de las personas han cambiado y continúan haciéndolo. Así, se pasó de la web 1.0, que era un sitio donde acceder a información, a una web 2.0 en la que los usuarios eran consumidores y productores (al mismo tiempo) del contenido que circula en Internet (por ejemplo, se pasó de las

[15] En el siguiente enlace se pueden consultar el número de usuarios por cada cien habitantes por país http://datos.bancomundial.org/indicador/IT.NET.USER.P2. Consultado por última vez el 5 de junio de 2014.

páginas web a los blogs, y de la enciclopedia *online* a la Wikipedia). En la actualidad, se habla ya de la web 3.0 (también conocido como "Internet de las cosas")[16]: una tercera generación, donde son los ordenadores los que pueden procesar la información, como si la entendieran, e inferir conclusiones a partir de los datos. Esta revolución constante hace necesario que los sistemas de protección también evolucionen al mismo ritmo y que se adopten nuevas estrategias de prevención.

Finalmente, cabe destacar el carácter anonimizado del ciberespacio al permitir que los usuarios naveguen por Internet ocultando su verdadera identidad. Esto es posible gracias a que existen múltiples herramientas para interactuar en las que no es necesario revelar la identidad como los servidores de correo electrónico, las redes sociales, etc. Es cierto que se ha mejorado mucho en la identificación de la IP desde la que un usuario se conecta a Internet, pero la posibilidad de acceder a redes *wifi* abiertas (o públicas) o la creación de redes *botnet*, ponen de manifiesto que se puede averiguar desde dónde se realiza un conducta, pero no quién es el auténtico ejecutor (Miró, 2012). En otras palabras, Internet crea múltiples oportunidades para inventar versiones alternativas de uno mismo y para involucrarse en diferentes formas de interacción (Fonseca, 2003).

En resumen, el ciberespacio es distinto al espacio físico y las características que lo configuran (la contracción del espacio y el

[16] Para conocer más sobre este concepto, se puede consultar la siguiente página web: http://www.ibm.com/smarterplanet/us/en/overview/article/iot_video.html

tiempo, la expansión comunicativa, la transnacionalidad de la comunicación, la incapacidad para que exista un órgano central de control, la facilidad para ocultar la verdadera identidad, su popularización entre las personas, y su permanente estado de evolución) hacen que el delito que en él se cometa, como fenómeno social que es, se vea afectado por él. Por tanto, para la comprensión de cada una de las formas de cibercriminalidad, así como para la elaboración de las estrategias de prevención, deberán tenerse en consideración la configuración de este nuevo ámbito de comunicación.

Capítulo II. Los menores como víctimas del ciberacoso no sexual

> "Internet terminó con la era de la casa como refugio, al igual que la artillería acabó con la del castillo como fortaleza."
>
> (Pease, 2001, p. 24)

1. Menores y cibercrimen en la web 2.0

1.1. El uso de los menores de las TIC

Es evidente que el uso de las TIC ha calado en toda la población, pero especialmente, entre los jóvenes. No se puede negar que, gracias a las facilidades que brinda el ciberespacio, éste se ha convertido en un lugar que invita a ser usado para relacionarse con otras personas y también para conocer más mundo. Probablemente, las virtudes de Internet son las que han hecho que se haya convertido para los jóvenes en el medio para establecer relaciones sociales.

Y es que, observando los datos ofrecidos por el Instituto Nacional de Estadística, las conclusiones son evidentes: la práctica totalidad de los menores en España hacen uso de las redes sociales. Tal y como se muestra en el gráfico, desde el 2003 hasta el 2013 (últimos datos accesibles) el uso de Internet entre los jóvenes españoles de 10 a 15 años ha subido en 40 puntos porcentuales (INE, Base de datos).

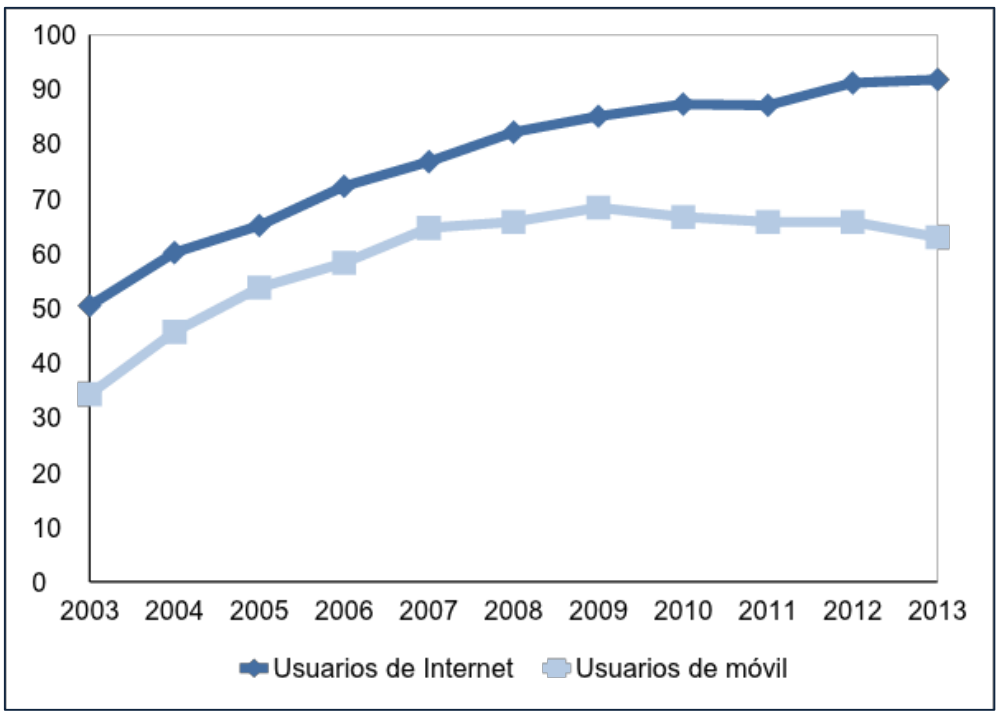


Ilustración 1. Evolución del uso de las TIC en la población española 2003-2013. Elaboración propia a partir de los datos ofrecidos por el INE

Los últimos datos recogidos del Instituto Nacional de Estadística muestran que el 92% de los jóvenes entre 10 y 15 años usa

Internet, mientras que el uso del móvil, no ha experimentado la misma subida que Internet, pero aun así desde el 2003 hasta el 2013 ha pasado de ser usado por el 34,1% al 63%. La amplia diferencia entre el uso de Internet y el uso del móvil puede estar mediatizada por el intervalo de edad manejado. Los resultados del estudio llevado a cabo por Xavier Bringué y Charo Sábada (2011) -con una muestra de 12.919 menores españoles- indican que entre el 20% y el 35% de los niños y niñas de 6 años ya poseen móvil, y que es a partir de los 13 años cuando el porcentaje aumenta hasta 90%.

Analizando los datos ofrecidos por el Instituto Nacional de Estadística para el año 2013, se observa como existe poca variación de uso de Internet por parte de los menores. En este sentido, el 86,6% de los menores de 10 años hacen uso de Internet, aumentando su uso conforme aumenta la edad. De este modo, entre los 16 y 24 años de edad, el porcentaje de usuarios es del 99,6%; es decir, prácticamente todos los españoles hacen uso de Internet.

Con el móvil, la evolución todavía es más clara, situándose a los 10 años el porcentaje en torno al 26%, y aumentando hasta el 90% entre los jóvenes de 15 años. El Instituto Nacional de Estadística no ofrece el dato de uso del móvil en la franja de edad superior a los 15 años, pero seguramente el porcentaje obtendría valores más altos: en torno al 95-99% como han mostrado otros estudios (Bringué y Sábada, 2011). De acuerdo con estos autores, un tercio de los menores obtienen su primer móvil como regalo en ocasiones especiales como Navidad, un cumpleaños o la primera comunión. Así, en el 23% de los casos son los menores quienes lo solicitan, y se les concede, pero

también hay un 19% en el que son sus padres quienes se lo dieron sin solicitud previa.

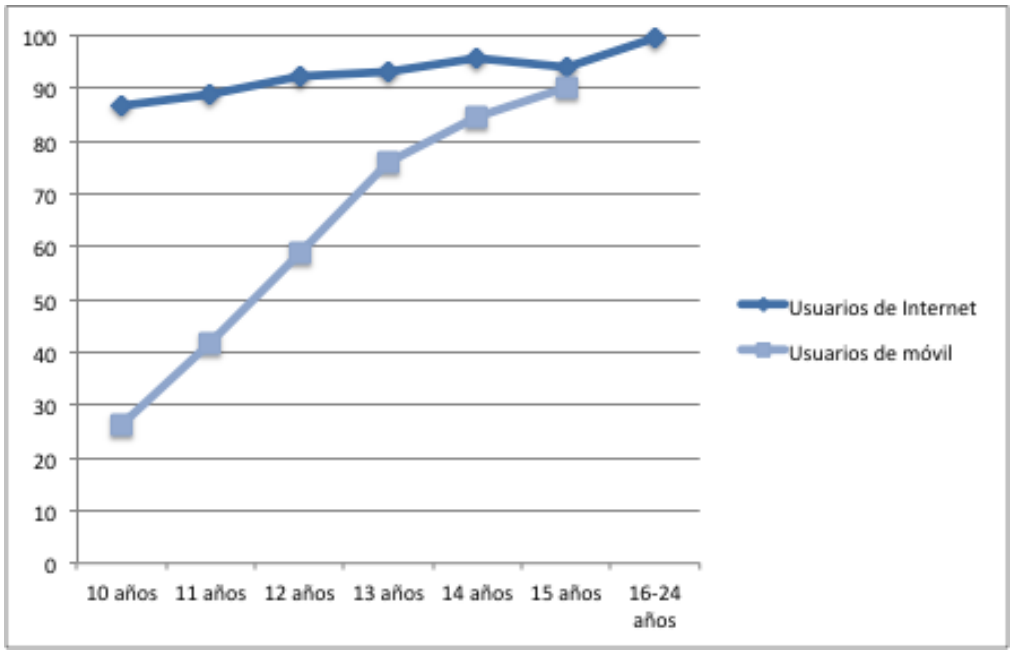


Ilustración 2. Uso de Internet y del móvil por edad. Elaboración propia a partir de los datos del INE (2013)

No cabe duda que Internet es concebido por los menores como una herramienta para establecer relaciones sociales: el principal uso que le dan es establecer comunicación con otras personas. Y es que, como apuntan Bringué y Sábada (2011), Internet permite una comunicación sincrónica, a tiempo real, y con personas o grupos previamente seleccionados. Entre las herramientas de comunicación, las que en mayor medida se usan son las de mensajería instantánea (Bringué y Sábada, 2011), aunque también se hace uso de otras

herramientas, como el correo electrónico y, en menor medida, chats y foros (García, López-de-Ayala y Catalina, 2013).

Pero Internet no es sólo una herramienta de comunicación, sino que también es una herramienta poderosa para el conocimiento, la diversión, compartir información con otras personas, y para el consumo. Los datos en este sentido son claros, el 76% de los menores admite usar Internet para buscar contenidos, y al mismo tiempo les sirve para descargar música, películas y programas informáticos. Similares resultados a los estos son los indicados por García et al. (2013), quienes encontraron que el 48,6% visitaban con mucha frecuencia sitios web de vídeos compartidos, y un 31,6% lo hacía de forma ocasional. La descarga con mucha frecuencia de archivos de música, o de películas o series, estaba en un 37,1%, mientras que el porcentaje de los que lo hacían en ocasiones ascendía a un 33,9%.

A todo lo anteriormente expuesto, debemos sumar el hecho de que Internet permite que podamos compartir con otras personas todo aquello que nos sucede en el mundo físico o, simplemente, aquello que nos parece interesante. Sin entrar a valorar ahora los riesgos asociados a esta práctica, lo cierto es que muchos menores entienden Internet como un lugar donde compartir información. El punto de inflexión en la publicación de los contenidos personales ha llegado con la creación de las redes sociales, pues según el estudio de García et al. (2013), el 75,3% de los jóvenes las usan con mucha frecuencia, y el porcentaje llega hasta el 90% cuando se suma el consumo ocasional. Y es que, como plantean estos autores, "las redes sociales han desbancado al correo electrónico y a la mensajería instantánea" (p. 202) debido a que esa primera herramienta permite, además de chatear o enviar

mensajes, publicar fotos o vídeos y actualizar el estado. En este sentido, hasta un 56% publica toda clase de información (principalmente fotos y vídeos) en redes sociales como Facebook, Tuenti o Instagram (Bringué y Sábada, 2011).

Y si Internet ha conseguido revolucionar la forma de comunicación, también lo ha hecho con la forma en que los menores juegan y se divierten. Se ha pasado de tener que comprar una videoconsola y los juegos para desarrollar esta actividad, a tener disponibles miles de juegos *online* a los que se puede acceder de forma gratuita a través de los ordenadores, *smartphones*, *tablets,* etc. Pero también ha fomentado la socialización, al no ser imprescindible estar en el mismo espacio físico para jugar a un juego con otra persona. De hecho, uno de los principales motivos de que los menores hagan uso de los videojuegos *online* es que les permiten desarrollar espacios y tiempo lúdicos con su propio grupo de amigos, pero también les permite conocer a personas nuevas (Bringué y Sábada, 2011).

Todas estas actividades realizadas por los menores se hacen sin especial supervisión por parte de los padres: aproximadamente el 85% de los menores navegan solos por Internet (Bringué y Sábada, 2011). Los padres aseguran hacer un seguimiento del uso de las tecnologías de sus hijos, pero en la mayoría de los casos éste se restringe simplemente a hacer uso de sistemas de protección. En este sentido, de la encuesta de INTECO (Instituto Nacional de Tecnologías de la Comunicación) se desprende que el 92,5% de los padres consideran que los sistemas y herramientas de protección de seguridad instalados en los ordenadores de sus hijos (que generalmente se limitan al antivirus) son medidas muy efectivas para contrarrestar los riesgos que

provienen de navegar por Internet; llamando la atención, que sólo un 6,4% dude de su efectividad. Y es que lo que especialmente preocupa a los padres y madres es el riesgo de dependencia o uso abusivo de sus hijos de las tecnologías (39,5%), teniendo poca percepción del riesgo de que sus hijos puedan sufrir ataques informáticos intrusivos (13,4%), acoso sexual (9,9%), indeseada interacción con desconocidos (9,2%), timos y fraudes (8,7%), o el acceso a contenidos inadecuados (8,2%). Viendo estos resultados, no es de extrañar que los padres se centren en tomar medidas de tipo físico y técnico, dejando de lado medidas educativas como el diálogo, la advertencia, la formulación de recomendaciones o, simplemente, el adoptar medidas coercitivas como el establecimiento de limitaciones de uso y el control, así como la supervisión de la actividad (INTECO, 2009).

1.2. Intercomunicación entre menores y cibercriminalidad social

Internet ya no es sólo un ámbito para las relaciones económicas o institucionales entre empresas y Estados, sino también, y seguramente en mayor medida, para las relaciones sociales entre las personas. La popularización de las TIC y, en particular, de los denominados *smartphones*, junto a la aparición de las redes sociales, han convertido al mundo digital (el ciberespacio) en el nuevo referente global de las relaciones interpersonales.

Los jóvenes usan las redes sociales para ver vídeos o fotos de amigos (50,1%), o para publicar contenidos interesantes que encuentran en Internet (41%); pero también destinan una parte de ellas, para hacer pública su vida privada: un 55,2% publica vídeos o

fotos personales de manera ocasional, pero un 25,4% lo hace con mucha frecuencia; el 42,6% actualiza periódicamente su perfil, siendo esta práctica más habitual entre las chicas que entre los chicos (García et al., 2013).

A todo ello se suma que las redes sociales permiten a los usuarios crear álbumes de fotografía realizando comentarios sobre las fotos publicadas, y facilitan la interactuación y la comunicación con otros contactos. Además, cada usuario tiene una página personal que contiene información propia, la relación que mantiene con otros contactos y, finalmente, también dispone de juegos online comunitarios (Ontsi, 2011).

Y es que es, probablemente, la facilidad con la que se pueden publicar facetas de la vida personal, donde radica el éxito de las redes sociales, pero esta característica favorece también que se hayan convertido en un lugar óptimo para llevar a cabo delitos contra el honor, la dignidad, la intimidad o la libertad sexual.

Sin ánimo de criminalizar las redes sociales y otras herramientas de comunicación, éstas favorecen sin lugar a dudas la criminalidad, y las claves de porqué puede suceder esto, las resume el director de Pantallas Amigas, Jorge Flores Fernández (2009), en seis puntos:

- En las redes sociales se promueven las relaciones entre personas a través de otras personas, por lo que se pierde el control directo de la referencia, y el criterio de selección o confianza usado se diluye según los nodos se distancian.
- Las redes sociales disponen de demasiadas funciones automáticas que el usuario novato desconoce. Un ejemplo

de ello es que cuando se crea un perfil (salvo que se preste atención para impedirlo) se envía de manera automática una solicitud de invitación a unirse a todas las personas anotadas en el directorio del correo electrónico.

- Existen demasiadas funciones potentes para compartir todo tipo de cosas en Internet, y se desconocen los efectos que tienen *a priori*, como por ejemplo el etiquetado de las fotos, que provoca que puedan estar visibles para múltiples usuarios.
- Los menores desconocen la repercusión y el alcance de lo que publican.
- Las redes sociales guardan información muy precisa, y es tanta la información que contienen, que un usuario puede ser víctima de un rastreo intensivo.
- Las redes sociales presentan al usuario opciones de manera demasiado interesada, lo que suele implicar pérdida de privacidad. Tras la supuesta intención de ayudar y agilizar, ponen muy poco énfasis en que el usuario configure las opciones de privacidad de los datos y, sin embargo, insisten en que complemente su perfil con todo tipo de cuestiones.

En definitiva, es la posibilidad de comunicación entre las personas a través de las distintas herramientas que provee el ciberespacio, unida a las facilidades que éstas presentan para la publicación indiscriminada de la vida personal, lo que hace posible los ataques de tipo personal en el ciberespacio. Y es que como afirma Miró (2012), en relación con las relaciones sociales en el ciberespacio, lo que

es cierto es que "todas las esferas personales que, al relacionarse con los demás, pueden ser puestas en peligro, lo están también en el ciberespacio; y que todas las conductas criminales de ataque a las personas que no requieran una inmediatez física también van a acabar realizándose por medio de Internet" (p.124).

2. Análisis de la prevalencia de victimización por ciberacoso no sexual en menores

2.1. Prevalencia de victimización por ciberacoso no sexual en menores en España

Los estudios realizados hasta la fecha en España muestran discrepancias en cuanto a la prevalencia de victimización: los datos varían desde el 0,4% (Defensor del Pueblo, 2007) al 44,1% (Calvete et al., 2010). Y es que si echamos la vista atrás para hacer un breve repaso a los estudios realizados en España en relación a esta cuestión, el único estudio realizado hasta la fecha con una muestra representativa de la población juvenil española, es el Defensor del Pueblo, que encontró que el 5,5% había sido víctima de *cyberbullying.* De ese conjunto de víctimas, el 5,1% lo había sido de forma esporádica y sólo el 0,4% lo había sufrido de forma muy frecuente. Esta forma de presentar los datos, distinguiendo entre el ciberacoso leve y el severo, es empleada posteriormente por otros autores, cuyos resultados obtenidos son similares. Este es el caso del estudio llevado a cabo por Ortega et al.

(2008), con una muestra de estudiantes cordobeses, encontrando un porcentaje de ciberacoso poco frecuente del 9,3% frente al 1,5% que sufre un ciberacoso frecuente. Por su parte, el Observatorio Estatal de la Convivencia (2008) cifró la prevalencia hasta en un 7% para el acoso poco frecuente y en un 2,1% en el severo. Por último, Avilés (2009) y Calmaestra (2011) encontraron porcentajes similares: cercanos al 5% cuando es una baja frecuencia y en un 0,5% y un 1,2%, respectivamente, cuando se trata de un acoso severo.

Pero la anterior forma de presentar los datos no es la única encontrada: otra práctica habitual es presentar el porcentaje total de victimizados, independientemente de cómo haya sido medido. Esta forma de medición presenta generalmente porcentajes superiores, como puede observarse en el estudio llevado a cabo por la Asociación Protégeles (2010), a partir del cual se indicó que la prevalencia de victimización era del 19%. En ese mismo año, Estévez et al. (2010) encontraron en un estudio realizado en Vizcaya, un 30,1%; y también, Buelga et al., (2010) obtuvieron en una muestra de 2101 estudiantes de la Comunidad Valenciana, un porcentaje del 24% cuando el ciberacoso era realizado a través del móvil, y un 29% cuando era realizado a través de Internet.

Un punto de vista totalmente distinto, es el adoptado por Sureda et al. (2008), que llevan a cabo un estudio con una muestra de estudiantes de las Islas Baleares, que se orientó a buscar la prevalencia en función del tipo de victimización. En este estudio, un 13,4% de la muestra estudiada había sido víctima de difusión de información privada y de rumores, un 11,6% había recibido insultos y amenazas, y

un 8,8% afirmó que imágenes indiscretas o comprometidas de ellos habían sido difundidas.

2.2. Prevalencia de victimización por ciberacoso no sexual en otros países

Esta variedad de resultados en los estudios no sólo sucede en España, sino que también se replica en otros países. En este sentido, Patchin e Hinduja (2012), tras el análisis de diferentes estudios internacionales, determinaron que los porcentajes de prevalencia varían del 6% al 40%, e incluso llegan al 72% si tenemos en cuenta el estudio de Juvonen y Gross (2008).

Haciendo un breve repaso de los estudios llevados a cabo en otros países y comenzando por Estados Unidos, Kowalski y Limber (2007) cifraron la prevalencia en el 11%. Porcentajes más altos encontraron Ybarra et al. (2007), con un 35% de ciberacoso (siendo el 26% un acoso poco severo y el 8% muy severo). Hinduja y Patchin (2008), sin embargo, obtuvieron un porcentaje de cibervictimización por acoso del 32% entre los chicos y un 36% entre las chicas, mientras que Hoff y Mitchell (2009) encontraron un cifra superior, con un 56,1%.

En Canadá, Li (2006) realizó un estudio con 264 estudiantes y determinó un porcentaje de cibervictimización del 25%; y un año más tarde encontraba un porcentaje superior: 28,9% (Li, 2007); mientras que posteriormente, realizó otro estudio con una muestra de China y situó la prevalencia en este país en un 33% (Li, 2008). Años después, en Israel, la prevalencia encontrada fue de un 16,5% (Olenik-Shemesh, 2012). En

Australia, sin embargo, según Price and Dalgleish (2010), la prevalencia varía en función de la edad: el 49% entre los jóvenes de 10 y 12 años, el 52% entre los que tienen 13 y 14 años, y el 29% entre los que tienen 15 y 16 años.

Similares resultados se han encontrado en países europeos. Así, en Grecia, el estudio llevado a cabo por Kapatzia y Sygkollitov (2007) arrojó resultados que variaron desde un 0,9% (cuando el acoso era con una frecuencia de una vez por semana), que se ampliaba a un 14,7% (cuando la frecuencia era de una vez al mes). Sin embargo, en Reino Unido, el porcentaje de cibervictimización por acoso se sitúa en un 22% (Smith et al., 2008); mientras que en Suecia el porcentaje encontrado es inferior al resto de países: 5,3% (Slonje y Smith, 2008). En Holanda se acerca más a los niveles de Reino Unido: 23% (Dehue et al., 2008). En Bélgica, Vandebosch y Van Cleemput (2009) encontraron un porcentaje de victimización del 11%; y por último, en Italia, el porcentaje de victimización encontrado fue de un 10% para los chicos, frente al 15% de las chicas (Brighi et al., 2012).

2.3. Análisis de las metodologías empleadas

Las variaciones encontradas en los resultados podrían deberse a una cuestión cultural, pero lo que parece tener más fuerza, y así han apuntado otros autores, es la diversidad en las diferentes metodologías empleadas (Jackson y Cohen, 2012; Sabella, Patchin y Hinduja, 2013; Tokunaga, 2010; Vandebosch y Van Cleemput, 2009). Son muchos los puntos discordantes entre los estudios que impiden hacer una valoración global y comparar resultados. El primero de ellos es la

definición empleada, que tiene efecto directo sobre el instrumento empleado. Así, se observa que en muchos casos, en los que se emplean cuestionarios creados *ad hoc,* los autores se limitan a preguntar directamente si el sujeto se ha sentido acosado a través de las nuevas tecnologías, como ocurre en el trabajo de Calmaestra (2011), en el que se preguntaba "¿Has sufrido *bullying* a través de Internet en los últimos dos meses?" (p.159). En cambio, otros autores optan por preguntar directamente por formas concretas de acoso, como por ejemplo haber sido insultado o amenazado por medio de Internet o del móvil (Calvete et al., 2010; Juvonen y Gross, 2008; Ybarra et al., 2007). El principal problema es que no siempre se pregunta por las mismas formas de victimización, y a esto, debemos sumarle que hay autores que hacen sólo hincapié en el medio empleado, por lo que encontramos resultados que hacen referencia al móvil, a Internet en general o, de forma concreta, a las herramientas de comunicación que existen (salas de chat, redes sociales, mensajería instantánea, etc.). Y finalmente, derivadas de la definición, encontramos diferencias en si una víctima debe ser entendida como tal cuando sufre una agresión de manera continuada, o tan sólo cuando la ha sufrido una vez.

La segunda gran diferencia viene dada por la delimitación temporal. Algunos estudios se limitan a preguntar a las potenciales víctimas si alguna vez han sufrido alguna forma de victimización, mientras que otros delimitan el acoso a un tiempo concreto que varía desde el último año, hasta los dos últimos meses, o incluso en la última semana.

La tercera gran diferencia es la delimitación del concepto de agresor del acoso. La mayoría de los estudios centrados en la

victimización de menores a través de Internet tienen como objetivo el análisis del *cyberbullying* y, generalmente, los investigadores, al conceptualizar ese tipo de conductas, hacen referencia a que el agresor debe ser un compañero de clase o, al menos, del colegio. Sin embargo, esto no siempre es así. Y precisamente este hecho lo que hace es limitar el conocimiento sobre la victimización que sufren los menores a través de Internet. En este sentido, el Informe publicado por la Diputación Provincial de Alicante y el Centro Crímina (Miró, 2014a) indica claramente que los menores que son victimizados por medio de Internet, además de por sus compañeros de clase o de la escuela, también lo son por parte de personas que han sido conocidas a través de la Red y, especialmente, por conocidos de otros espacios físicos, como son los compañeros de las actividades extraescolares, vecinos, o amigos de otros amigos. Por tanto, ante la decisión de no delimitarse la procedencia del ataque, puede inferirse que los porcentajes de victimización pueden ser superiores.

Los estudios que no han limitado la procedencia del ataque suelen emplear muestras muy amplias abarcando todos los tramos de edad, desde los 16 a los 65 años de edad (Bocij, 2003), aunque la mayoría selecciona muestras universitarias (Finn, 2004; Henson, 2011; Holt y Bossler, 2009; Marcum, 2008; Marcum et al., 2010; Ngo y Paternoster, 2011; Reyns, 2010; Reyns et al., 2011). No es el caso del trabajo de Yucedal (2010), que emplea una muestra que varía de los 12 a los 83 años, y el resultado obtenido por este autor es una prevalencia de ciberacoso a través de la Red del 20,6%.

Finalmente, es necesario apuntar que la fecha en la que se realizó el estudio también puede impedir la posibilidad de hacer

comparaciones, dado que el elemento empleado para realizar la victimización son las TIC, que están en permanente cambio y revolución (Miró, 2012). En este sentido, en la medida en que se vayan mejorando los sistema de comunicación, como así ha pasado con la evolución del SMS a sistemas de mensajería instantánea (como el WhatsApp o el Line) que permiten realizar otras funciones (como el envío gratuito de imágenes o archivos de voz), se ampliarán las posibilidades de crear nueva formas de victimización. Y en la medida en que las TIC se vayan adentrando en nuestras vidas, y especialmente en las de los jóvenes (es decir, cuando su uso se haga todavía más extensivo), será probable que haya una mayor cibervictimización.

En definitiva, se hace claramente necesario establecer una metodología común (Calvete et al., 2010) que permita comparar resultados, comprender mejor los fenómenos, para así poder establecer estrategias de prevención más eficaces.

3. Factores de riesgo de victimización de ciberacoso no sexual en menores

3.1. El papel de las características demográficas en el ciberacoso

Del mismo modo que ocurre con la prevalencia, los autores tampoco se ponen de acuerdo en determinar si el ciberacoso afecta más a los chicos o a las chicas, sin embargo, los resultados encontrados hasta la fecha pueden dividirse en tres grandes grupos. El primero de ellos sería el conformado por aquéllos que han concluido que el género no tiene ningún efecto en el ciberacoso, o lo que es lo mismo, que esta conducta se da en la misma medida tanto en los chicos como en las chicas (Clavete et al., 2010; Finn, 2004; Holt y Bossler, 2009; Jackson y Cohen, 2012; Juvonen y Gross, 2008; Olenik-Shemesh, 2012; Vandebosch y Van Cleemput, 2009; Wigderson y Lynch, 2013; Williams y Guerra, 2007). Un segundo grupo de autores, sería el de aquéllos que han concluido que son los chicos quienes en mayor medida sufren el acoso a través de las TIC, y en esta posición destacan los trabajos tanto de Avilés (2009b), que encontró que el 6% de los chicos son víctimas frente al 5% de las chicas, como Li (2007), que halló diferencias mucho mayores: el porcentaje de chicos víctimas de ciberacoso era del 31,2% frente al 26,3% de las chicas.

Finalmente, el tercer grupo de trabajos concluye que son las chicas quienes tienen más riesgo de ser víctimas de ciberacoso. En este sentido, autores como Calmaestra (2011), Kowalski y Limber (2007) o Smith et al. (2006), determinaron que las chicas son las que en mayor

medida sufren el ciberacoso y, como apuntan Ortega et al. (2008), independientemente de la frecuencia de la aparición. También Wang et al. (2009) determinaron que son las chicas las que más sufren el ciberacoso y, en cambio, son los chicos quienes más lo ejercen. Por su parte, Hoff y Mitchell (2009) aún encontraron diferencias superiores, ya que en su estudio, en el 72,1% de los casos las víctimas eran chicas frente al 27,9% que eran chicos. Determinante también fue el estudio de Li (2007b) en el que halló que el 60% de las víctimas eran mujeres, sin embargo, los resultados no siempre son tan concluyentes: Brighi et al. (2012) encontraron una diferencia de cinco puntos porcentuales entre ambos sexos, y el 15% de las chicas fueron victimizadas frente al 10% de los chicos. Años atrás, en una investigación anterior Ybarra et al. (2006) habían hallado que el 58% de los ciberacosados eran mujeres, mientras que en otra posterior pudieron matizar que éstas lo sufren en mayor medida cuando el acoso ocurre de manera infrecuente (55%), pero también cuando ocurre de manera frecuente (50,8%) (Ybarra et al., 2007). No obstante, debemos matizar que en este último caso, analizando los porcentajes (sobre todo en el caso del acoso severo), el resultado puede ser estadísticamente significativo por el efecto del gran tamaño de la muestra empleado, y no de una realidad efectiva.

Independientemente de esta clasificación general en tres grandes grupos, hay un sector de autores que no se podrían incluir en ninguno de ellos, por entender que en la mayoría de los casos son las chicas las que sufren la victimización, salvo en determinados supuestos donde son los chicos los que más la sufren. En este sentido, Buelga et al. (2010), indican que el ciberacoso es más frecuente en las chicas, salvo para dos conductas, el hostigamiento y la persecución, en las que los chicos son los protagonistas de las victimización. Ybarra et al. (2007)

encontraron resultados similares: las chicas tienen más probabilidades de ser víctimas de ciberacoso de manera puntual, mientras que los chicos las tienen de serlo frecuentemente.

Tradicionalmente, las chicas jóvenes siempre se han visto envueltas en situaciones de violencia de tipo psicológica o verbal, mientras que los chicos suelen protagonizar formas de violencia física o amenazas (Defensor del Pueblo, 2007; Olweus, 2005). Teniendo en cuenta que la criminalidad social que más se suele ejercer a través de los medios electrónico es lanzar insultos o rumores, no es de extrañar que sean las chicas quienes más lo sufren (Miró, 2014a). Esto viene a ser corroborado por algunos de los estudios que han analizado el género de los que amenazan a otros a través de Internet, y que han evidenciado que son los chicos quienes los realizan, pero también quienes los reciben (Buelga et al., 2010).

Y del mismo modo que los autores no se ponen de acuerdo en determinar el género de las víctimas, tampoco existe un acuerdo en la influencia de la edad para ser víctima del ciberacoso. De esta forma, algunos estudios han determinado que los jóvenes con mayor edad tienen más probabilidades de ser víctimas (Kowalski y Limber, 2007; Patchin y Hinduja, 2006), y en sentido similar, Slonje y Smith (2008) encontraron que hay un mayor número de víctimas entre el grupo de los que tienen entre 15 y 18 años, que entre los que tienen de 12 a 15. En cambio, Smith et al., (2008) hallaron que no hay relación entre la edad y la victimización, mientras que Calvete et al., (2010) determinaron que los grupos en los que sucede mayor violencia se encuentra entre los que tienen de 13 a 15 años. Estos resultados coinciden con la mayoría de estudios, que no han encontrado que la

edad sea un factor relevante (Beran y Li, 2007; Didden et al., 2009; Juvoven y Gross, 2008; Katzer et al., 2009; Patchin y Hinduja, 2006; Smith et al., 2008; Varjas, Henrich, y Meyers, 2009; Wolak et al., 2007; Ybarra, 2004). Otros en cambio, sí que han encontrado diferencias (Dehue et al., 2008; Hinduja y Patchin, 2008; Kowalski y Limber, 2007; Slonje y Smith, 2008; Ybarra y Mitchell, 2008; Ybarra et al., 2007). No obstante, son algunos los autores que apuntan que estos resultados incoherentes se deben a los diversos rangos de edad empleados en los estudios (Tokunaga, 2010).

3.2. Factores de victimización relacionados con la personalidad

Algunos autores han tratado de identificar otras variables que pudieran estar relacionadas con la cibervictimización, de manera que pudieran servir para dar explicación o, por lo menos, predecir situaciones de riesgo. En este sentido, además de las variables sociodemográficas, se ha hecho especial hincapié en aquellas relacionadas con la personalidad y las relaciones sociales.

Una de las variables que más se ha estudiado hasta el momento es el sentimiento de soledad (Brighi et al., 2012; Calmaestra, 2011; Olenik-Shemes et al., 2012; Şahin, 2012), perspectiva según la cual, los jóvenes que experimentan soledad (tanto emocional como social) pueden tener más dificultades para el desarrollo de sus relaciones sociales en el espacio físico, por lo que buscarían mantenerlas a través de Internet (especialmente de forma anónima) y ello les llevaría en muchas ocasiones a estar en situaciones de riesgo (Olenik-Shemes et al., 2012). Además de la soledad hay otras variables psicológicas, que

afectan al desarrollo normal de las relaciones y que tienen relación con el ciberacoso, como la depresión (Didden et al, 2009; Mitchell, Wolak y Finkelhor, 2007; Smith et al, 2008; Wang et al., 2011; Wong, Chan y Cheng, 2014; Yang et al., 2013; Ybarra, 2004) y la baja autoestima (Fredstrom, Adams y Gilman, 2011; Calmaestra, 2011; Campfield, 2008; Didden et al., 2009; Wong, Chan y Cheng, 2014). Por su parte, Didden et al (2009), hallaron el interesante dato de que había relación entre la baja inteligencia y el ciberacoso.

El sentimiento de satisfacción con la vida también se ha estudiado como factor relacionado, al entender que un buen nivel de satisfacción se relaciona con el desarrollo positivo y, por contra, un bajo nivel está relacionado con llevar a cabo más conductas de riesgo (Sumter et al., 2012). Asimismo, también se ha relacionado con el abuso de sustancias como el alcohol, la marihuana o inhalantes (Hinduja y Patchin, 2008; Sinclar et al., 2012; Ybarra, Espelage y Mitchell, 2007). Pero también la adicción a Internet, entendida como una necesidad continua de conectarse a ella, que afecta gravemente al estado de ánimo y que contribuye al aislamiento social y a la destrucción de sus relaciones, es otro de los factores que se ha descubierto que tiene relación con el ciberacoso (Casas, Del Rey y Ortega, 2013; Juvonen y Gross, 2008; Vandebosch y Van Cleemput, 2009; Ybarra y Mitchell, 2004a).

Por otro lado, también se ha comprobado la relación del ciberacoso con el apoyo social percibido (Williams y Guerra, 2007), pues los menores que se sienten menos apoyados por sus padres tienen más problemas de ciberacoso (Wang et al., 2009). Y es que la falta de vínculos emocionales (Ybarra, Diener-West y Leaf, 2007) y una

pobre relación paterno-filial (Ybarra y Mitchell, 2004a) tienen efectos negativos, y esto, a su vez, se debe a que los menores no suelen contar a sus padres lo que están sufriendo: tan solo entre el 12,3% y el 21,1% (dependiendo de si se emplea móvil o Internet) le cuenta a sus padres lo que les está pasando, reduciéndose ese porcentaje hasta el 3,6% en el caso de contárselo a los profesores (Ortega et al., 2008).

Sin embargo, hay que tener cautela a la hora de entender estas variables como predictores, pues no siempre se tiene en cuenta la temporalidad de las variables (Ybarra, 2004), no pudiéndose saber si se trata de predictores de la cibervictimización o, por el contrario, si son consecuencias derivadas de ella. Tal y como apuntan Raskauskas y Stolz (2007), el 93% de los que han sido víctimas de ciberacoso, también han desarrollado efectos negativos, y en este sentido, la literatura muestra las variables antes mencionadas como consecuencia de la victimización, como es el caso de la depresión (Kowalsli y Limber, 2013; Turner et al., 2013) y una baja autoestima (Estévez et al., 2010), así como otras como la ansiedad (Kowalski y Limber, 2013; Ybarra et al., 2006), el consumo de sustancias (Mitchell et al., 2007), el neuroticismo (Corcoran et al., 2012), y la ideación suicida (Bauman et al., 2013; Kowalski y Limber, 2013; Turner et al., 2013; Yang et al., 2013).

3.3. Factores de victimización relacionados con las actividades cotidianas

Sin negar el aporte de las variables psicológicas y sociodemográficas a la explicación de la cibervictimización, ha surgido en los últimos años una corriente de autores que tratan de explicar la

victimización a partir de las actividades cotidianas que realizan los menores en el ciberespacio (Bossler y Holt, 2010; Miró, 2013c; Ybarra y Mitchell, 2004a). Estos autores pretenden demostrar, en otras palabras, que aquello que hagan los menores en el ciberespacio determinarán en buena medida su riesgo de cibervictimización (Patchin y Hinduja, 2006). No se trata, y tampoco lo pretende así este trabajo, de considerar que son estas las únicas variables que inciden en la cibervictimización, sino en reconocer que también ellas pueden constituir un interesante foco de atención para, en particular, establecer posteriormente estrategias de prevención.

En este mismo sentido, Wolak, Mitchell y Finkelhor (2007) ya identificaron el mayor uso de Internet como factor de riesgo de la cibervictimización menores, sin embargo, no son los únicos autores que han encontrado una correlación positiva entre el mayor número de horas de uso de Internet y la cibervictimización (Beckman et al., 2013; Casas et al., 2013; Didden et al., 2009; Mishna et al, 2012; Ybarra y Mitchell, 2004a). Así también, Juvonen y Gross (2007) encontraron que este factor aumenta la probabilidad de cibervictimización en un 60% (OR=1,45).

Otros autores, no se han centrado tanto en el tiempo pasado en Internet, sino en el uso concreto de herramientas que proporciona Internet para la comunicación interpersonal. De este modo, y aunque está más asociado a la comunicación profesional, el correo electrónico fue una de las primeras herramientas que se asoció con la cibervictimización de menores (Ybarra y Mitchell, 2004a). También lo han sido el chat (Sengupta y Chaudhuri, 2011; Ybarra y Mitchell, 2004a), el uso de la *webcam* (Juvonen y Gross, 2007), y especialmente las que

han adquirido mayor protagonismo por los jóvenes en los últimos años: el uso de blogs (Mitchell, Wolak y Finkelhor, 2008), la mensajería instantánea (Sengupta y Chaudhuri, 2011) -que según Juvonen y Gross (2007) aumenta la probabilidad en 2,8 veces-, y las redes sociales (Sengupta y Chaudhuri, 2011).

A partir de este punto, es necesario cuestionarse si es el mero uso de las herramientas lo que pone en riesgo a un menor, o es lo que permiten hacer éstas. En este sentido, Mitchell, Wolak y Finkelhor (2008) explican para el caso de los blogs, que son sitios donde los usuarios muestran sus pensamientos e invitan a la retroalimentación de otros usuarios. Pensamientos que se pueden traducir en comentarios desagradables, amenazantes, en definitiva negativos, que pueden afectar a los menores. De forma similar Sengupta y Chaudhuri (2011), en relación con las redes sociales, argumentan que el riesgo no viene determinado por el hecho de tener un perfil, sino porque son potenciales vehículos para que los jóvenes cometan conductas de riesgo (Duncan, 2007). Y es que de acuerdo con Casas et al. (2013) uno de los factores de riesgo de la actividad en el ciberespacio es que se tiene poco control sobre la información personal que se vierte y, probablemente, los menores no sean conscientes de los riesgos derivados de tal acción. Así, los jóvenes priorizan su deseo de popularidad a costa de su privacidad e intercambian de manera continua imágenes, vídeos y otras informaciones personales.

Es precisamente la cesión voluntaria de información personal, uno de los factores que con mayor fuerza inciden en la victimización social (Marcum, 2008; Marcum et al., 2010; Patchin y Hinduja, 2010), pues se vierte todo tipo de información que pone en peligro a los

jóvenes: fotos de sí mismo (Reyns, 2010; Sengupta y Chaudhuri, 2011), el colegio en el que estudian, el número de teléfono (Sengupta y Chaudhuri, 2011), facilitan contraseñas (Mishna et al., 2012; Patchin y Hinduja, 2010; Sengupta y Chaudhuri, 2011), el nombre completo, el estado civil, la orientación sexual, la dirección de correo, intereses y aficiones (Reyns, 2010). Y no sólo se está en riesgo cuando se facilita información personal a otros usuarios publicándola en las redes sociales o a través de otros medios, sino que como ha demostrado Miró (2013c), aunque con población adulta, también hay otra forma de poner a disposición de otros la información personal que supone un riesgo y es guardando información en los sistemas electrónicos con los que navegan por Internet.

Otra de las actividades que permiten las herramientas de comunicación es el contacto (la interacción) con personas desconocidas (extrañas), factor éste que también está altamente relacionada con la victimización social (Marcum et al., 2010; Misha et al., 2012; Mitchell, Wolak y Finkelhor, 2008; Sengupta y Chaudhuri, 2011; Vandebosch y Van Cleemput, 2009), especialmente para los casos en los que la víctima desconoce la identidad del agresor (Wolak, Mitchell y Finkelhor, 2007).

Por otro lado, también se ha estudiado que la víctima más probable es el agresor, y en este sentido Reyns et al. (2011) determinaron que el factor más relevante es el comportamiento desviado *online.* Así, los que contactan con alguien en repetidas ocasiones cuando le han pedido que pare, e incluso acosan o molestan a alguien por Internet, solicitan sexo a alguien que no quiere, amenazan por Internet, descargan música o películas piratas y envían o reciben

imágenes de contenido sexual, tienen más probabilidades de sufrir *cyberharassment*. Concretamente, tienen 6 veces más de probabilidad de que alguien contacte en repetidas ocasiones cuando previamente se le ha pedido que no lo haga, 10 veces más de sufrir acoso *online,* 15 veces más de recibir solicitudes de sexo no deseadas y 14 veces más de sufrir *cyberstalking*.

Este punto se ha estudiado especialmente relacionando el *bullying* tradicional con el *cyberbullying*, explicando que los que usan Internet para acosar a otros tienen mayor probabilidad de acabar siendo víctimas (Vandebosch y Van Cleemput, 2009; Wolak, Mitchell y Finkelhor, 2007). Y no sólo los que agreden a través de Internet, también es un factor de riesgo haber sido agresores en el espacio físico (Misha et al., 2012), así como haber sido víctima (Brighi et al., 2012; Li, 2007; MacDonal y Roberts-Pittman, 2010; Vandebosch y Van Cleemput, 2009; Ybarra y Mitchell, 2004b) y espectadores de *bullying* tradicional (Vandebosch y Van Cleemput, 2009). No es de extrañar, por tanto, que algunos autores sostengan la idea de que el acoso *online* sea una extensión de la intimidación tradicional. Sin embargo, otros autores como Kowalski y Limber (2013), consideran que, a pesar de que hay una relación evidente entre ambos fenómenos porque hay algunos que ven Internet como otro método más para intimidar o para vengarse por haber sido intimidado en la escuela, hay otros que lo ven como un mecanismo para decir y hacer cosas que nunca harían cara a cara.

Finalmente, también se ha considerado relevante por algunos autores el lugar físico en el que se encuentra el menor a la hora de navegar por Internet. Así, los que usan el ordenador en zonas privadas de la casa como la habitación, tienen más riesgo de ser victimizados

que los que lo hacen en espacio públicos (Sengupta y Chaudhuri, 2011) y en otros lugares como la casa de los amigos (Marcum, 2008). También es un factor de victimización el tener mayores privilegios por parte de los padres para el uso de Internet (Marcum, 2008), mientras que la instalación de filtros y otros programas informáticos de control parental no tienen efecto en la exposición de los menores a contenidos nocivos, ni sobre la prevención de la victimización social (Marcum, 2008; Sengupta y Chaudhuri, 2011). Así, como argumentan Holt y Bossler (2009), este tipo de programas no están destinados a evitar estos ataques, sino aquéllos relacionados con el *software* malicioso, por lo que autores como Sengupta y Chaudhuri (2011) consideran que es más útil hablar con los hijos sobre los riesgos a los que se exponen que el uso de dispositivos de monitoreo.

Todos estos resultados obtenidos en las investigaciones confirman la idea de Ybarra y Mitchell (2004a): los menores que hacen uso de Internet para interactuar con otras personas, tienen más riesgo que aquéllos que lo emplean para hacer otras actividades como la descarga de *software.* Por ello, y de acuerdo con Miró (2012), las actividades cotidianas en el ciberespacio son predictores significativos de la victimización, particularmente para el caso de los menores, a lo que se suma que a mayor número de actividades sociales distintas en el ciberespacio, mayor será la probabilidad de sufrir acoso, injurias o cualquier otra actividad similar.

Capítulo III. Teoría de las actividades cotidianas en el ciberespacio y victimización por ciberacoso no sexual

"Antes las distancias eran mayores porque el espacio se mide por el tiempo"

J.L. Borges

1. Teoría de las actividades cotidianas en el marco de las teorías del crimen y la oportunidad

1.1. De las teorías de la criminalidad a las teorías del crimen

La investigación criminológica desde sus inicios, ha mostrado gran interés por el individuo delincuente, así, los científicos se han aproximado al estudio del delito tratando de explicar cuáles han sido los factores que han llevado a la persona a cometer los delitos y desde una perspectiva preventiva, se han centrado en intervenir directamente en las causas de la criminalidad (Medina, 2011). De este modo, las orientaciones psicológicas, han buscado las causas del comportamiento delictivo en ciertos trastornos mentales, en

diferencias sexuales o en la inteligencia; por su parte, desde un punto de vista sociológico, factores como la pobreza, las injusticias sociales, las deficiencias en la socialización o la falta de educación, han sido objeto de investigaciones y relacionados con el delito; finalmente, otros han señalado ciertas razones de carácter biológico como los desencadenantes de la actividad delictiva.

La primera de las orientaciones, la biológica, mira hacia el hombre delincuente tratando de localizar e identificar en alguna parte de su cuerpo y de su funcionamiento orgánico el factor diferencial que pueda explicar la conducta delictiva. Así, se buscan patologías, disfunciones o trastornos somáticos que la puedan provocar. Como consecuencia, las diferentes hipótesis de trabajo llegan a ser tan variadas como disciplinas y especialidades existen en el ámbito de las ciencias: antropológicas (Bertillon, 1909; Goring, 1913; Hooton, 1931), biotipológicas (Di Tullio, 1980; Kretschmer, 1961; Sheldon, 1942), endocrinológicas (Marañón, 1946; Ruiz de Funes, 1929), genéticas (Exner, 1957; Jacobs, 1993), neurobiológicas (Raine, 1993, 2013), bioquímicas (Walsh, 1995), etc. Todas ellas, eminentemente empíricas, lo que provoca, cierta incapacidad para llegar a resultados teóricos más generales que los expresados por la propia especialidad. En definitiva, esa decidida inclinación por la perspectiva biologicista muestra una incuestionable vocación clínica y terapéutica, que potencia la clínica fisiológica, por encima de otras proyecciones y orientaciones de la investigación criminológica.

Por eso precisamente, para algunas corrientes de opinión, y especialmente para ciertos autores, las teorías lombrosianas (Lombroso, 1876) aún conectadas con orientaciones jurídicas

(Garofalo, 1885), o sociológicas (Ferri, 1900), no parecían explicar suficientemente ciertos crímenes aparentemente incoherentes, que obedecían a motivaciones triviales, extrañas y en ocasiones incomprensibles. Y el resto de explicaciones imperantes hasta entonces tampoco parecían ser capaces de desentrañar el misterio de las motivaciones profundas del crimen. Básicamente, porque el determinismo positivista no debe ser interpretado en términos de las afirmaciones científicas irrefutables de una ciencia exacta, sino en los relativos y probabilísticos de una ciencia social (Akers, 1997).

Estas limitaciones trataron de resolverse por medio del nuevo paradigma de las explicaciones psicológicas del crimen, que buscaban, sobre todo, descubrir esos móviles ocultos en los lugares más recónditos de la mente humana, intentando al mismo tiempo, aportar nuevos conocimientos y desarrollar nuevas técnicas de aplicación a la ciencia criminológica. En base a una, muchas veces automática y generalizada percepción, se suele atribuir a menudo a supuestas anomalías mentales el origen de conductas que sólo pueden ser explicadas por una anormalidad mental, para lograr de ese modo eludir la suposición de que alguien "normal" pueda llevar a cabo conductas tan inexplicables como el crimen. El resultado de todo este esquema de pensamiento, en algunos casos casi inevitable, es que se tienden a equiparar las conductas de adecuación a la norma con el equilibrio mental, y de análoga manera, la conducta desviada con la enfermedad mental. Y, dentro de la corriente psicológica, es la Psicopatología, como ciencia que estudia el concepto de cada uno de los diferentes trastornos mentales, así como sus manifestaciones y sintomatología, la que puede profundizar en la interrelación entre las diversas patologías mentales y las acciones delictivas (Maudsley, 1871; Monahan, 1996),

especialmente las que más se suelen asociar a determinadas conductas que no parecen tener otra explicación más que ésta. Lo cual también es el caso de conductas no directamente relacionadas con la enfermedad mental y sí con individuos con trastornos de la personalidad, muchas veces implicados en los delitos más violentos, como puede ser el caso de los cometidos por psicópatas (Cleckley, 1941; Hare, 1970; Kraepelin, 1913).

Las modernas teorías criminológicas de corte psicológico, como es de esperar, ponen el acento en los condicionantes individuales que pueden concurrir en la persona para hacerle inclinarse hacia la conducta delincuente, como la búsqueda de estimulación (Eysenck, 1977), respuesta ante el estrés (Damasio, 1994), el factor sexo/género (Giddens, 1993; Pollak, 1950; Rechea, 2008), los procesos hormonales (Fishbein, 1992), la inteligencia (Chico, 1997; Gardner, 1995; Henggeler, 1989), o la propia personalidad (Eysenck, 1989), entre otras muchos. Pero no por ello obvian totalmente el papel que pueda jugar el ambiente, por lo que también estudian la relación entre la delincuencia y el entorno familiar (Canter, 1983). En esencia, propugnan que toda conducta es el producto de la interacción entre las predisposiciones del sujeto y diferentes elementos que procedentes del exterior que le rodean.

Finalmente, los enfoques de orientación sociológica ponen el acento de sus explicaciones del hecho criminal en factores de tipo social, como anteriormente ya se ha indicado. Y la moderna Criminología Sociológica no se limita a resaltar la importancia del entorno en la aparición de la conducta criminal, sino que además contempla el hecho delictivo como un fenómeno social en toda su

extensión. Este tipo de orientaciones abarcan una variada gama de inclinaciones de tipo muy diverso, que no obstante, tienen en común esa explicación básica referida al entorno social que rodea al individuo.

La característica común de las primeras corrientes ambientalistas de la Criminología era, en general, la inclinación hacia el estudio de la distribución espacial del delincuente (Brantingham y Brantingham, 1981; Park, Burgess y McKenzie, 1925; Shaw, 1929). Aunque también se investigan otros aspectos como, por ejemplo, los diferentes modelos de estudio de la importancia de la distancia física entre víctima y delincuente en relación con el lugar del crimen, o la distribución de la delincuencia juvenil en áreas urbanas (Shaw y McKay, 1942). Por su parte, frente a todo ello, el funcionalismo examina la conducta desviada como fenómeno social; y sin embargo, y esa es una de sus características diferenciales, no sostiene que el origen del delito esté en el posible impacto de determinados factores sociales, ni es una desestructuración del orden social, sino que se deriva más bien, del funcionamiento normal de la vida social, el cual produce delincuentes igual que produce ciudadanos que no lo son. De esa manera, considera que la criminalidad es producto de la propia estructura social (Durkheim, 1894; Merton, 1938), pero, en todo caso, no es un resultado deseable, sino que proviene de una crisis o un desajuste de esa estructura. La conducta delincuencial es, entonces, una respuesta irregular del individuo como una forma normal de adaptación del mismo a esa situación. En ocasiones, teniéndose en cuenta la trascendencia del barrio donde se vive en relación con las posibilidades efectivas de ejercitar el rol criminal (Cloward y Ohlin, 1960). Según la óptica funcionalista, la delincuencia no es más que un fenómeno social que contribuye, en unión de otros, a la estabilidad de la función social,

y el delincuente un factor de regulación de su funcionamiento. Y lo que es patológico no es la criminalidad, sino las alteraciones incontroladas de su estructura y las tasas delincuenciales.

Para las teorías subculturales, el delito no es consecuencia de la desorganización social o de la ausencia normativa (como mantienen las teorías anómicas), sino que surge de una organización social distinta y de unos códigos de valores propios de cada subcultura, distintos de los de la sociedad de referencia (Cloward y Ohlin, 1960; Cohen, 1955; Wolfgang y Ferracuti, 1967). La realidad es que la Escuela Ecológica ya había prestado una cierta atención hacia el fenómeno de las bandas callejeras juveniles de delincuentes (Thrasher, 1927), y los teóricos del enfoque subcultural siguen este camino, pero en vez de estudiar la organización interna de estas bandas, ponen el acento en las condiciones sociales que han podido llegar a provocar su aparición. Por su parte, los defensores de las explicaciones del proceso social afirman que todo individuo, independientemente de la clase social a la que pertenezca, puede llegar a convertirse en delincuente. Aunque, eso sí, hay un mayor número de delincuentes de clase social baja, lo cual sucede porque en éstos se dan en mayor medida una serie de carencias que los inclinan a ello, a veces de forma casi inevitable. Si bien esto no quiere decir que un individuo de clase media, e incluso alta, no pueda llegar a convertirse en delincuente si llegan a concurrir en él procesos de interacción con estancias sociales que resulten determinantes en ese sentido.

Mientras otras escuelas criminológicas intentan responder a la cuestión de cómo se origina el delito, buscando el factor explicativo del porqué puede llegar a cometerse, las del control social por el contrario,

lo que tratan de estudiar no es por qué se delinque, sino qué es lo que impide a los individuos hacerlo (Hirschi, 1969; Reckless, 1970; Reiss, 1959; Glaser, 1978). Podría decirse que lo que presuponen es la desviación y, entonces, lo que hay que revelar es la conformidad hacia las reglas establecidas. A diferencia de las teorías de corte sociocultural, intentan explicar el fenómeno criminal sin atribuirlo esencialmente a los estatus sociales más bajos, ya que sostienen que el debilitamiento del control social puede darse también en las clases sociales más privilegiadas.

Las teorías de aprendizaje social, como variantes del conductismo próximas a las teorías sociológicas del aprendizaje, se basan en que la adquisición de modelos criminales se lleva a cabo por medio de un proceso de aprendizaje evolutivo a través de la observación y la imitación. Se afirma en ellas que el niño no sólo aprende en función de las posibles recompensas o castigos, sino sobre todo de lo que observe en modelos como los padres, los maestros, los amigos, en los medios de comunicación, etc. (Bandura, 1973; Sutherland y Cressey, 1960; Sutherland, 1939) Así, la actividad de aprendizaje vicarial permite que el individuo procese experiencias de otros que puedan servirle de guía de comportamiento. Por otra parte, su capacidad de auto-regulación le confiere también la posibilidad de ejercer control sobre su propia conducta generando auto-refuerzos desencadenados por la interacción del individuo con el ambiente que le rodea.

El enfoque de la teoría del etiquetamiento supuso un cambio de orientación de una Criminología que, hasta entonces, estudiaba preferentemente el comportamiento criminal. Así, el *labelling approach*

lo que defendía era, más que el estudio de la figura del delincuente, el de los procesos por los cuales éste llega a ser definido como tal, y como, en función de ese proceso, reacciona la sociedad ante él (Becker, 1963; Lemert,1951). Otro aspecto que interesa especialmente a los representantes del etiquetamiento, son las consecuencias de ese proceso por el cual un determinado individuo resulta definido como delincuente. La idea básica de la que se parte, es que el individuo se forma una imagen de sí mismo que es el producto de su interacción con los demás, a lo que se suma que sus comportamientos están mediatizados por esa imagen que tiene de sí mismo. Según este proceso, si por determinados motivos la persona es "etiquetada" como delincuente, se considerará a sí mismo como tal y, en consecuencia, actuará como se espera que actúe un criminal.

La Criminología tradicional se fundamenta, aunque indudablemente con sus variaciones caracterizadoras según el caso, en la existencia de un orden social basado en el consenso. Orden en el que juega un papel garantizador fundamental el Derecho y en el que el Estado tiene la función de aplicarlo, anteponiendo los intereses generales de la sociedad a los individuales o los de ciertos grupos. Sin embargo, las denominadas teorías del conflicto parten de una tesis totalmente contraria: no es la integración la que permite mantener el funcionamiento del sistema social, sino aunque parezca paradójico, el que lo consigue es el conflicto (Chambliss, 1975; Dahrendorf, 1959; Quinney, 1972; Taylor, Walton y Young, 1973), y por ello, consideran la existencia de conflictos sociales como algo normal y necesario. Y uno de ellos es el delito, que cumple su función, igual que el resto de conflictos presentes en toda sociedad.

La consecuencia de estos planteamientos teóricos es que la reducción del delito, recordemos que, determinado por las tendencias psicológicas, biológicas o los condicionantes sociales, debe ser afrontada desde la intervención directa en las causas que mueven a los individuos, y ello debe hacerse por medio de programas sociales y de desarrollo económico o a través de la rehabilitación y reinserción (Medina, 2011), dirigidos al delincuente como ser "diferente" desde el punto de vista biológico, social o psicológico.

Sin embargo, en las décadas de los sesenta y sobre todo en los setenta del siglo pasado surgen, fundamentalmente en Estados Unidos de América, Gran Bretaña y Canadá, un número creciente de autores que, cada vez con más vehemencia, manifiestan lo que consideran un evidente fracaso del sistema de Justicia Criminal. Así, la obra de Jane Jacobs *The Death and Life of Great American Cities* (Jacobs, 1961) primero, la de Oscar Newman *Defensible Space: Crime Prevention Through Urban Design* (Newman, 1972) después, o la obra fundamental de Ray Jeffery, *Crime Prevention Through Environmental Design* (Jeffery, 1971), muy especialmente, en su edición de 1977[17], comienzan a poner el énfasis en el estudio del evento criminal, y de manera particular en el ambiente, cambiando así el foco de atención, y dirigiéndolo desde el individuo delincuente, objeto casi único de estudio y que prácticamente marginaba al propio acto criminal, hacia

[17] En esta edición podemos encontrar afirmaciones como ésta: "The only question remaining then is: If the present model is so stupid, why do we resist all attempts to change it?" (Jeffery, 1977, p.11).

el evento delictivo. De entre estos autores, Jeffery se muestra como uno de los más críticos con el estado de cosas al que había llegado la prevención del delito, poniendo de manifiesto el fracaso de los argumentos de la disuasión, y en general del sistema de Justicia Criminal, de la Policía, y de los jueces, para corregir el crimen[18]. En este sentido, y ante el sistema de justicia cruel e inhumano, el autor propone como alternativa, la prevención del delito por medio del diseño de espacios (Jeffery, 1977, p. 10).

Por su parte, Derek Cornish y Ronald Clarke (1986) formulan desde Gran Bretaña, como consecuencia en parte de este cambio de enfoque, la perspectiva de la elección racional del delito, la cual plantea que los infractores con su comportamiento buscan la obtención de un beneficio y toman sus decisiones sobre la base de un juicio, resultado de estimar las oportunidades que tienen para llevar a cabo el delito con éxito, el riesgo de ser detectados y detenidos, y los beneficios que esperan obtener, considerando de este modo que, la conducta delictiva es básicamente instrumental y que está dirigida a satisfacer las necesidades de dinero, búsqueda de sensaciones, sexo, estatus, etc. Este análisis de costes y beneficios es en realidad, un proceso que comprende dos decisiones, la de implicación y la de evento: la primera se refiere a la disposición a llevar a cabo delitos, y en este sentido, el individuo evalúa las diferentes opciones que se le plantean para alcanzar sus objetivos, tanto legales como ilegales, eligiendo

[18] Otro ejemplo de las críticas vertidas por Jeffery hacia el sistema de justicia imperante en la época, es la siguiente: "(…) Deterrence and punishment are failures; treatment and rehabilitation are failures; the criminal justice system is a failure from police to courts to corrections." (Jeffery, 1977, p. 9).

finalmente comenzar a delinquir y continuar haciéndolo o no; mientras que la segunda, se refiere al delito concreto y está influenciada por los factores situacionales, es decir, distingue entre la decisión de cometer un concreto delito en un preciso momento y lugar, de la de iniciar una "carrera delictiva" (Medina, 2011). Por otra parte, que la decisión sea racional, no significa que el delincuente realice un cálculo frío y desapasionado de todas las opciones y consecuencias, ni que sea infalible en sus percepciones y evaluaciones, sino que, al igual que el resto de decisiones del ser humano, está limitada por las numerosas variables que influyen y que pueden ser conocidas o no por el sujeto (Serrano, 2004).

Otra propuesta surgida al abrigo del estudio del crimen como evento que se desarrolla en un ámbito espacio-temporal, es la Teoría del Patrón Delictivo del matrimonio canadiense Paul y Patricia Brantingham (1991). Centrados en la dimensión geoespacial del delito, postulan que los delincuentes cometen sus delitos en aquellos lugares en los que pasan más tiempo, en el hogar, la escuela, el trabajo, los centros de ocio y las rutas que unen esos nodos. Estos son los lugares que mejor conocen por sus actividades diarias y por tanto, es donde localizan las oportunidades para cometer sus delitos, y así, conocidos sus patrones de actividad diaria, podremos entender también los patrones espacio-temporales de la actividad delictiva. De este modo podrán distinguirse los "generadores del delito", es decir, aquellos lugares que atraen al público en general y que se convierten en problemáticos por su capacidad para atraer oportunidades delictivas, como los estadios de fútbol o los centros de ocio, de los "atractores del delito", es decir, los que tienen la capacidad de crear oportunidades

delictivas por sí mismos, como las áreas de prostitución o de venta de drogas.

Estas diferentes aproximaciones al estudio del delito finalmente se agruparon bajo la denominación de "teorías del crimen" (Gottfredson y Hirschi, 1990), frente a las tradicionales "teorías de la criminalidad". Y aunque diferentes, todas ellas, tienen en común dos ideas: en primer lugar, que los delitos no se distribuyen aleatoriamente en el espacio y el tiempo, sino que se concentran en determinados periodos temporales y en ciertos lugares denominados *hot spots* o puntos calientes (Sherman, Gartin y Bueger, 1989), e incluso en determinados objetivos[19]; y en segundo, la oportunidad delictiva, es decir, lo que hace que existan concentraciones espacio-temporales de los delitos es precisamente la existencia de oportunidades en esos momentos y lugares (Medina, 2011).

El creciente número de investigaciones generado en los últimos cuarenta años ha provocado una lógica evolución de los iniciales planteamientos, dando lugar a un robusto cuerpo de conocimientos que ha impulsado hasta tal punto las teorías del crimen, que incluso se ha propuesto por parte de algunos autores la creación de una "ciencia del delito", vaticinado que si la Criminología no cambia para ser más efectiva, será eclipsada por esta nueva corriente (Clarke, 2004). Es en este sentido, el Jill Dando Institute of Security and Crime Science, del University College of London, dirigido por Richard Wortley, el prototipo de esta nueva concepción del estudio del delito. Sin embargo, en

[19] Véase por ejemplo, el análisis de la victimización reiterada en la obra Pease (1998).

España, puede que por ser uno de los países que más tardíamente se ha incorporado a esta nueva forma de estudiar el delito, se ha dedicado escasa atención a este tipo de enfoques criminológicos (Vozmediano y San Juan, 2010).

Sea como fuere, a pesar de las críticas vertidas en contra de desarrollos como la prevención situacional del delito, surgidos de estas teorías, lo cierto es que con su vocación claramente pragmática y menos ambiciosa desde el punto de vista de la construcción teórica, ya que no trata de comprender al individuo como ser complejo, sino el evento delictivo, éstos tienen la virtud de considerar, tal y como Marcus Felson propone en sus "falacias del crimen" (Felson y Boba, 2010), que el delito es generalmente un hecho ordinario, pues puede ser cometido por cualquiera, ya que los criminales no son "los otros", sino que podemos ser cualquiera de nosotros (Medina, 2011), y que además, puede ser evitado por medio del desarrollo de técnicas prácticas, modificando el ambiente y en definitiva, tomando medidas para reducir las oportunidades.

1.2. La teoría de las actividades cotidianas

Es en este contexto de creciente crítica dirigida al sistema de justicia penal, propiciado por una parte, por el cada vez más alarmante aumento de la cifra de la criminalidad y por otra, por los avances en la investigación científica y el desarrollo de las teorías de alcance medio, en el que surge la teoría de las actividades cotidianas, enunciada por Lawrence Cohen y Marcus Felson (1979). Considerada en la actualidad una de las construcciones teóricas más citadas e influyentes en el

ámbito de la Criminología moderna (Miró, 2014b), ha generado, en las últimas cuatro décadas, un enorme volumen de trabajos científicos elaborados sobre la base de sus planteamientos, desde las más variadas metodologías (Spano y Freilich, 2009).

En su seminal artículo, "Social Change and Crime Rate Trends: A Routine Activity Approach", Cohen y Felson (1979) señalaron que paradójicamente, mientras ciertos indicadores de bienestar y condiciones socioeconómicas publicados en la década de los sesenta por la Oficina del Censo Norteamericano, como la pobreza o la baja escolarización (hasta entonces, como se ha visto, consideradas causas de la criminalidad), habían experimentado una considerable mejoría[20], los informes que el FBI publicaba sobre las tasas de la criminalidad en esos mismos años (Uniform Crime Report, FBI, 1975), indicaban que se estaba produciendo un importante aumento de la actividad delictiva[21]. Estos autores trataron de explicar esta contradicción centrándose en las variaciones de los patrones en los que se estructuraban las ocupaciones diarias de las personas. Así, observaron que las actividades cotidianas de los individuos habían experimentado un cambio y que ese cambio, podía ser el responsable del aumento de la criminalidad al proporcionar mayores oportunidades delictivas, especialmente en los delitos de carácter predatorio, tal y como los

[20] La proporción de negros que completaban sus estudios medios en las ciudades aumentó de un 43 por cien en 1960 a un 61 por cien en 1968, el desempleo descendió significativamente entre 1959 y 1967, y los ingresos por familia se incrementaron, reduciéndose el número de familias consideradas pobres, de 11,3 a 8,3 millones

[21] Entre 1960 y 1975 las tasas de robo, robo con fuerza, violaciones y homicidios, se incrementaron un 263%, 164%, 174% y 188%, respectivamente.

definieron Felson y Cohen (1980): aquellos delitos en los que una persona causa daño a otra o a sus propiedades.

Las transformaciones en los patrones de actividad a las que Cohen y Felson se referían, se habían reflejado en distintas encuestas e informes publicados en aquellos años. Entre otros factores, destacaban el mayor protagonismo adquirido por las actividades de las personas desarrolladas fuera del hogar, los cambios experimentados en los bienes de consumo y el modo en que la sociedad realizaba las transacciones. De este modo, la incorporación de la mujer al mercado laboral y su acceso a la educación superior, la prolongación de la duración de las vacaciones, los viajes fuera de la ciudad, o los permanentes desplazamientos de un lugar a otro, por una parte, dejaban los hogares vacíos y sin protección; y por otra, incrementaban los contactos entre los posibles delincuentes y sus objetivos, al coincidir en el lugar en que se concentraban esas actividades cotidianas unos y otros. En cuanto a los bienes de consumo, postularon que los avances tecnológicos habían propiciado el consumo de electrodomésticos y equipos electrónicos cada vez más pequeños, de elevado valor económico y fáciles de transportar y sustraer, lo que los haría muy atractivos. Todo ello, junto con la aparición de cajeros automáticos, el aumento de las transacciones y los pagos y reintegros bancarios, habría provocado un cambio en la circulación de propiedades, que acrecentaría su movilidad y visibilidad. En definitiva, se había producido un incremento de los objetivos adecuados en ausencia de guardianes capaces de darles protección, lo que habría proporcionado un mayor ámbito de oportunidad criminal.

Estas afirmaciones se apoyaban, por ejemplo, en las encuestas de victimización dirigidas por Hindelang (1976), con las que contrastaron que las actividades desarrolladas lejos del hogar presentaban mayores riesgos que las llevadas a cabo en el mismo. En este sentido y dado que no era posible establecer mediante cálculos directos, los cambios en la cantidad de tiempo que las personas se encontraban en su hogar, definieron a partir de la Encuesta de Población (desde 1947), lo que denominaron Household Activity Ratio, cuyo resultado aportaba una estimación de la proporción de hogares americanos más expuestos al riesgo de una victimización personal o sobre una propiedad. También como consecuencia de las encuestas de victimización, Felson advirtió en estudios anteriores que los jóvenes tenían mayores probabilidades de ser víctima del delito, o que los hogares en los que convivían matrimonios o en los que las mujeres no se habían incorporado al trabajo presentaban menor riesgo de ser victimizados que aquellos otros ocupados por personas solteras o en los que las mujeres trabajaban fuera de casa (Medina, 2014).

Los datos así presentados por Cohen y Felson aportaban una visión distinta del fenómeno delictivo ya que, mientras que las variaciones de las tasas delictivas en el espacio ya habían sido estudiadas por autores como Guerry (1993) o Quètelet (2010), en muy pocas ocasiones la investigación había considerado la interdependencia temporal de los delitos con el lugar y las actividades humanas. En sus primeros trabajos, Cohen y Felson centraron su atención en los patrones de actividad humana apoyándose en las enseñanzas de Colquhoun (1800) y muy especialmente de Hawley (1950), para el que la comunidad no es simplemente una unidad territorial, sino una organización simbiótica de actividades humanas

que se desarrollan en un espacio y tiempo (Cohen y Felson, 1979). Así, ritmo, tempo y *timing*, constituían los tres elementos en los que se descomponía la organización del tiempo y que debían ser estudiados para comprender a la sociedad (Clarke y Felson, 1993; Felson y Poulsen, 2003).

Aunque fundamentada en la ecología humana, la teoría de las actividades cotidianas presenta numerosas conexiones y puntos de contacto y ha recibido influencias, de otros enfoques y teorías criminológicas surgidas en la década de los setenta, que como ya hemos visto, respondían a la sensación de fracaso de muchos de los programas de intervención social y de rehabilitación, dirigidos a la reducción de la delincuencia, cuyo origen era la concepción del delincuente como un ser que debía ser tratado desde una orientación médica o psicológica, por sus predisposiciones individuales o patologías. Por el contrario, enfoques como el de la elección racional plantean desde una perspectiva pragmática, la intervención sobre los factores situacionales y las oportunidades delictivas. El origen de esta perspectiva se sitúa, como se ha visto, en los trabajos de Cornish y Clarke (1986) con los que el enfoque de Felson coincide, de un lado, en las bases de las que parte (la decisión racional) y de otro, en la voluntad de situar el acento de la prevención y la explicación del delito no sólo en el criminal, sino también en el ambiente en que actúa.

En este sentido, desde su planteamiento inicial, el enfoque de Cohen y Felson, ha sido coherente con la idea de un delincuente racional que aprovecha sus oportunidades, tanto es así que en ocasiones a la teoría de Cohen y Felson se le denomina "teoría de la oportunidad" (Serrano, 2009). De este modo, tanto para el enfoque de

las actividades cotidianas, como para la perspectiva de la elección racional, el tópico de la oportunidad juega un papel relevante. Uno de los primeros y más decisivos antecedentes del paradigma de la oportunidad (Serrano, 2009), aunque restringido al papel de la víctima, fue la teoría de los estilos de vida de Hindelang (Hindelang, Gottfredson y Garofalo, 1978), cuya idea central es que ciertos estilos de vida favorecen la victimización porque ofrecen más oportunidades para ello. Precisamente en relación con los estudios de Hindelang y sobre todo con la publicación de la teoría de los estilos de vida y la exposición diferencial al delito (Hindelang, Gottfredson y Garofalo, 1978), encontramos ciertos puntos de conexión con la teoría de las actividades cotidianas, aunque entre ambas hay una diferencia de enfoque ya que, mientras que Hindelang, Gottfredson y Garofalo ponen el énfasis en la víctima, Cohen y Felson, acentúan el papel del evento delictivo.

Por su parte, el trabajo publicado en Londres por Mayhew y sus colegas *Crime as opportunity* (Mayhew, Clarke, Sturman, y Hough, 1976) es considerado como otro grandes hitos de las teorías de la oportunidad. A pesar de ser contemporáneo al de Cohen y Felson (1979), debe entenderse el desarrollo de la teoría de las actividades cotidianas independiente del británico, al no existir en aquellos momentos referencias del trabajo realizado al otro lado del Atlántico, como ha señalado Tilley (2009). En este sentido, la teoría de las actividades cotidianas sugiere que el delito puede aumentar o disminuir, sin que se produzca cambio alguno en el número de delincuentes. Por el contrario, el aumento de la disponibilidad de objetivos adecuados o la disminución de la efectividad de los guardianes, o el cambio en las actividades cotidianas de la sociedad,

pueden incrementar la probabilidad de que estos elementos confluyan en el espacio y el tiempo y por tanto aumentar las oportunidades delictivas. Junto a esta, una de las ideas más potentes de la teoría de las actividades cotidianas es precisamente, que las oportunidades no se distribuyen del mismo modo en la sociedad, ni son infinitas. En lugar de ello, hay un limitado número de objetivos disponibles que pueden ser vistos como atractivos por el delincuente (Tillyer y Eck, 2009).

También se relaciona el enfoque de las actividades cotidianas con la propuesta de Brantingham y Brantingham (1991), quienes han puesto de manifiesto, como ya se dijo, con su teoría del patrón delictivo la vinculación espacial existente entre el delito, los objetivos y los patrones de movimiento de los delincuentes cuyas actividades diarias se ubican en lugares y momentos en los que la probabilidad de llevar a cabo actos ilícitos es mayor. Los delincuentes cometen sus delitos cerca de las áreas donde pasan más tiempo (su hogar, trabajo, escuela, tiendas y espacios de ocio) y alrededor de las rutas que los conectan. El conocimiento del espacio que les rodea está determinado por sus actividades realizadas en el pasado y condiciona la ubicación de sus actividades futuras. Si queremos entender los patrones de distribución espacial y temporal del delito, necesitamos, por tanto, entender los patrones de actividad cotidiana y los movimientos de los delincuentes.

1.2.1. Teoría de las actividades cotidianas y elementos del crimen

La teoría de las actividades cotidianas explica el evento delictivo por medio de tres elementos esenciales, que confluyen en el espacio y

el tiempo en el transcurso de las actividades diarias de las personas. Estos tres elementos son: a) un delincuente potencial, esto es, con capacidad para llevar a cabo un delito; b) un objetivo o víctima apropiado para ser objeto del mismo, y por último; c) la ausencia de guardianes capaces de dar protección a objetivos y víctimas (Cohen y Felson, 1979).

El delincuente potencial o más bien probable, podría ser cualquiera con una razón para cometer un delito y con las habilidades apropiadas para hacerlo (Felson y Cohen, 1980), aunque lo más probable es, conforme a los aportes de la teoría criminológica, que sea un joven varón, sin trabajo estable, fracaso escolar, con accidentes de tráfico y que haya sido atendido en urgencias (Gottfredson y Hirschi, 1990). En su primera formulación Cohen y Felson (1979) emplearon el término delincuente motivado, sin embargo, en posteriores trabajos particularmente de Felson (entre otros, Felson y Cohen, 1980; Felson, 1986; Felson y Clarke, 1998; Felson y Boba, 2010) evitaron utilizar el término motivado al referirse al delincuente, ya que para ellos, lo verdaderamente relevante no era la disposición o motivación para cometer el delito, sino los factores físicos que posibilitaban que una persona se viera involucrada en él (Clarke y Felson, 2009). Lo que aportaba este enfoque, en particular, era la expresión de la necesidad para la comprensión del crimen de desviar la atención del criminal (Felson, 1995) dado que era en él exclusivamente en quien se centraba. Ahora bien, el que fuera necesario atender a otros elementos del delito para la comprensión y prevención del mismo (Felson y Clarke, 1998), en ningún momento suponía dejar de lado el "punto de vista" del delincuente (Felson, 2008), dado que, como se verá, la propia definición del objetivo como "adecuado" se hacía a partir de la comprensión de

los propósitos y capacidades del agresor en relación con las características intrínsecas de los posibles objetos del crimen.

El objetivo adecuado, es una persona o propiedad que puede ser amenazada por un delincuente. Felson prefiere el término objetivo al de víctima, puesto que el primero pone de relieve el hecho de que la mayor parte de los delitos están orientados a la obtención de bienes y por tanto, la víctima puede estar ausente del lugar del delito (Felson y Clarke, 1998). La probabilidad de que un objetivo sea más o menos adecuado, está influida por cuatro atributos, descritos desde el punto de vista del infractor, por medio del acrónimo VIVA (valor, inercia, visibilidad y accesibilidad), que definen su nivel de riesgo (Cohen y Felson, 1979; Felson y Clarke, 1998).

- Valor, calculado o simbólico, desde la perspectiva del delincuente.
- Inercia, refiriéndose al tamaño, peso y forma, esto es, los aspectos físicos de la persona o el bien, que funcionan como obstáculos o impedimento para que el delincuente lo vea como adecuado.
- Visibilidad, como exposición de los objetivos a los delincuentes, es decir, el atributo que marca a la persona o el bien para el ataque.
- Accesibilidad, referido al diseño del lugar y la ubicación del objeto que aumenta el riesgo de ataque o lo facilita.

Posteriores desarrollos modificaron el concepto VIVA, descrito ya, aunque sin excesiva profundidad, en el primer trabajo de Cohen y

Felson (1979), el cual podía ser aplicado a cualquier tipo de objetivo ya fuera material o personal. Coherentes con su perspectiva ecológica, los autores se centraron en este primer momento en la relación del objetivo con el espacio y el tiempo, sin prestar demasiada atención a los motivos que llevaron al delincuente a elegir un objetivo u otro y con independencia de si se trataba de un objeto material o no. Una vez desarrollada la teoría y complementada con otras como la "elección racional", suficientemente distanciados de las teorías de la criminalidad y contando ya con un amplio respaldo empírico, ulteriores formulaciones acogieron nuevos conceptos como el de los "hotproducts" de Clarke (1999), centrado específicamente en aquellos objetos más atractivos para los ladrones. Por medio del acrónimo CRAVED, Clarke describe que aquellos productos que son robados con mucha mayor frecuencia que otros porque son *concealable, removable, available, valuable, enjoyable and disposable*.

El tercer y último elemento descrito en la teoría es la ausencia de un guardián capaz, alguien que puede intervenir para detener o impedir un delito (Cohen y Felson, 1979). El guardián capaz de evitar el delito, es aquel con cuya simple presencia no se comete y cuya ausencia lo hace más probable (Felson, 1995). Este elemento comprende a cualquiera que transite por un lugar o tenga como función la vigilancia de personas o propiedades (Felson, 2006), aunque el concepto de guardián no debe restringirse ni confundirse con la policía o los vigilantes de seguridad. Obviamente estos lo son, y de hecho su ausencia es la más habitual en el momento en que se lleva a cabo un delito (Felson, 1986; Felson y Boba, 2010), tal y como puso de manifiesto el clásico experimento de Patrullas Preventivas de Kansas City en el que se puso a prueba la efectividad de las patrullas aleatorias,

constatando que el incremento de los niveles normales de patrullas en un área determinada, no tenía un efecto significativo sobre la actividad delictiva conocida en esa área (Kelling, Pate, Dieckman y Brown, 1974). Por ello también deben considerarse guardianes capaces, y pueden tener incluso más importancia en la prevención, el ocupante de una vivienda, un hermano, un amigo o un transeúnte y en general, cualquier persona que en el desarrollo de sus actividades diarias pueda, con su presencia o con su actividad, protegerse a sí mismo, proteger a otros o proteger las propiedades propias o ajenas.

El concepto de guardián capaz, su ausencia o su presencia, ha sido objeto de actualización prácticamente desde su formulación inicial. Su propia definición ha sido discutida y reformulada tanto por el propio Felson como por otros investigadores. Por ejemplo Hollis-Peel y sus colegas (2011) en una revisión de la literatura relacionada con la figura del guardián en la Teoría de las Actividades Cotidianas, lo han definido como, "el individuo o grupo de individuos, cuya presencia física o simbólica, actúa intencionadamente o no para disuadir de un potencial evento delictivo", pretendiendo incluir de este modo elementos que entienden no quedan suficientemente precisados en el artículo original de Cohen y Felson (1979) ni en otros posteriores. Un ejemplo de ello son los circuitos cerrados de televisión (CCTV), operados por personas cuya presencia en el lugar del evento delictivo no es física (Hollis-Peel, Reynald, van Bavel, Elffers y Welsh, 2011). El propio Felson, en un intento de vincular su teoría con la del control social de Hirschi (1969), hace una reformulación de la figura del guardián, distinguiendo entre el supervisor íntimo y el gestor del espacio (Felson, 1995). El primero puede ser el padre o un amigo que intenta, por medio de la desaprobación del comportamiento del

potencial delincuente, que no lleve a cabo acciones contrarias a las normas. El gestor del espacio, segundo elemento en los que descompone al guardián, se refiere a aquellos individuos que tienen una responsabilidad de supervisión sobre determinados espacios, por ejemplo, porteros, conductores de autobús, etc. De este modo al desarrollar el concepto de guardián tomando los cuatro elementos de la teoría de Hirschi (1969), apego, compromiso, implicación y creencias y resumirlos en uno solo, *cuidador*, y profundizando en la idea de que alguien pueda disuadir a un delincuente por medio de su presencia en un lugar o que una persona desaliente a un posible delincuente por su relación con él, Felson es coherente con la idea de control social e impulsa la noción de que el control constituye un elemento crítico en los cambios en las tendencias de las tasas delictivas (Cohen y Felson, 1979).

Sobre la base de los tres elementos iniciales propuestos por Cohen y Felson (1979); delincuente, objetivo y guardián y la posterior incorporación del supervisor íntimo descrito por el propio Felson (1986), Eck elaboró lo que se conoce como triángulo de la criminalidad, distinguiendo los elementos que son condición necesaria para el delito, de aquellos otros, a los que se refiere como controladores, que tienen el potencial de prevenirlo (Eck, 1994). De este modo, delincuente, objetivo y lugar, situados en el triángulo interior, serán supervisados por los controladores, es decir, aquellos quienes pueden reducir la probabilidad de un evento delictivo controlando cada uno de estos tres elementos, en el triángulo exterior. Así, el *cuidador* será la persona o personas con las que el infractor tiene una relación emocional, bien sea de parentesco, amistad, religiosa, respeto u otras. Su objetivo será mantener al potencial delincuente alejado de los problemas. Por su

parte, el gestor será el propietario o propietarios de los lugares o quienes los representan, porteros, empleados de las tiendas, camareros entre otros, tendrán que conseguir que no se produzcan problemas en el lugar. Finalmente, los guardianes buscan dar protección al objetivo. Policías, vigilantes de seguridad, aunque no sólo, también y en mayor medida los propietarios cuando vigilan sus pertenencias.

Ilustración 3. Triángulo de la criminalidad

Profundizando en estos conceptos Felson (1995) estimó que la probabilidad de que el guardián, el controlador (*handler*) o el gestor del lugar (manager) tengan éxito, deberá ponerse en relación con su grado de responsabilidad. De este modo, establece cuatro diferentes niveles: personal, como el que ostentan propietarios, familia y amigos; asignado, como el de los empleados a los que se ha atribuido

responsabilidades concretas de vigilancia; difusa, como la de los empleados con responsabilidades genéricas; y general, como la de cualquier persona. Con ello construye una matriz de 4x3 con 12 celdas, en la que sitúa en las filas los niveles de responsabilidad y en las columnas los elementos del delito y sus respectivos controles. De este modo, se puede analizar la probabilidad de éxito del controlador sobre un elemento determinado, siendo descendente según el nivel de responsabilidad. Tomando un objeto vigilado por un guardián, por ejemplo, un bolso, si quien lo vigila es su propietario el riesgo de ser robado será bajo, si es un empleado de seguridad, será bajo pero no tanto como si es su propietario, por el contrario si es un empleado con otros cometidos, el riesgo será mayor y finalmente si es una persona sin relación con el propietario del bolso, el riesgo aumentará.

Por su parte, Sampson, Eck y Dunham (2010) al analizar las razones por las que los controladores son inefectivos o sus acciones no son acertadas en ocasiones, desarrollan la idea de lo que denominan los "súper controladores", es decir, las personas, organizaciones e instituciones que generan incentivos para que los controladores prevengan o faciliten el delito y que sin influir de forma directa sobre sus elementos, pueden hacerlo de forma indirecta, incentivando su prevención. En esta extensión del triángulo de la criminalidad, se añade un tercer conjunto de elementos que se agrupan en torno a tres categorías, formal, difusa y personal y diez tipos, organizacional, contractual, financiera, regulatoria, *courts*, política, mercados, media, grupos y familia.

2. La aplicación de la teoría de las actividades cotidianas al ciberespacio

2.1. Desarrollos teóricos de la TAC al ciberespacio

Del mismo modo que Cohen y Felson, en los años setenta, se plantearon cómo los cambios en las actividades cotidianas incrementaban las oportunidades para el delito (Garrido et al, 2006), en la actualidad, algunos autores se plantean como las nuevas rutinas en el ciberespacio pueden incrementar o, en todo caso, crear nuevas oportunidades delictivas. En el pasado fue el aumento de las actividades de las personas fuera del hogar [22], los avances tecnológicos [23] y la aparición de los cajeros automáticos, [24] los que proporcionaron nuevos ámbitos de oportunidad delictiva al incrementar el número de objetivos adecuados, al posibilitar el contacto directo entre personas o sus propiedades y los delincuentes y disminuir los guardianes capaces de prevenir el delito (Medina, 2013).

En la actualidad, los hábitos de consumo y de comunicación entre las personas han cambiado: la comunicación entre las personas se realiza principalmente a través de las TIC, se publica todo tipo de

[22] Debido, entre otras causas, a la incorporación de la mujer a la actividad laboral, a la prolongación de las vacaciones, o a los continuos desplazamientos de un lugar a otro.
[23] Que favorecieron la aparición y consumo de pequeños electrodomésticos de elevado valor económico y poco peso (y por lo tanto muy atractivos y fáciles de sustraer y transportar).
[24] Con el consiguiente aumento de las transacciones y los pagos bancarios.

información personal y privada a través de las redes sociales, las transacciones bancarias ahora se realizan a través del ciberespacio mediante la banca *online*, se puede adquirir toda clase de productos a través de Internet mediante el uso de la tarjeta de crédito, etc. La pregunta es: ¿los nuevos hábitos de comunicación y consumo proporcionan nuevas oportunidades delictivas?. En otras palabras, como en su momento planteo Felson (1998), ¿la nueva sociedad virtual puede hacer que haya más probabilidades de que converjan un probable delincuente con un objetivo adecuado en ausencia de un guardián capaz?

2.1.1. Nuevas y viejas botellas y criminalidad en el ciberespacio: el enfoque de Peter Grabosky

Si hay un desarrollo teórico que se planteó en qué medida Internet cambiaba las oportunidades delictivas, es el de Peter Grabosky, que lleva por título "*Virtual Criminality: Old Wine in New Bottles?*" (2001). Con la metáfora "*old wine in the new bottles*" (viejo vino en nuevas botellas), el autor quiere poner de manifiesto que la cibercriminalidad sólo es la criminalidad de siempre, pero que ahora se realiza a través de un medio nuevo. Y es que afirma que "el cibercrimen es básicamente el mismo crimen que se comete en el espacio físico con el que estamos familiarizados. Y aunque, sin duda, alguna de que las manifestaciones son nuevas, gran cantidad los delitos cometidos -con o en contra de los ordenadores- sólo difieren en los términos del medio" (2001, p. 243).

Lo que pone de manifiesto Peter Grabosky (2007) es que el nuevo medio, a pesar de las ventajas que otorga, también "proporciona nuevas oportunidades para los criminales" (Grabosky, 2007, p.91). El crecimiento exponencial de la conectividad y las comunicaciones crea oportunidades para futuros delincuentes y riesgos paralelos para las víctimas potenciales.

Y es que Internet ha cambiado la forma de hacer las cosas. Los inversionistas ahora son capaces de comprar y vender acciones en línea sin necesidad de intermediarios, lo que supone una mejora de la eficacia de los mercados de valores, pero también ofrece oportunidades para la explotación criminal, pues en "la medida que Internet se vuelve cada vez más un medio de comercio, será cada vez más un medio de fraude" (Grabosky, 2001, p. 248). Y ya no es sólo la forma de hacer las cosas, la tecnología presenta ciertas particularidades que paradójicamente pueden ser usadas para fines legales pero también para los ilegales. Por ejemplo, el encriptado es necesario para realizar transacciones económicas con cierta seguridad, pero al mismo tiempo es usado por los criminales para dificultar su identificación. A ello hay que sumarle las facilidades que presenta Internet para ocultar la identidad real, que si bien pueden ser utilizadas por un policía para la búsqueda de criminales (por ejemplo, haciéndose pasar por un menores de trece años para detectar pedófilos), también permite a los agresores ocultar su verdadera identidad haciendo así más difícil su persecución. Y pese al anonimato que brinda Internet, es una práctica habitual entre los usuarios publicar todo tipo de información personal de manera libre que es aprovechada por las empresas para comercializar con ella y obtener así grandes beneficios económicos. Además, es prácticamente imposible hacer desaparecer la

comunicación personal realizada a través de los medios electrónicos. Así, por ejemplo, un mensaje enviado a través del correo electrónico, aunque se intente borrar, se pueden haber realizado copias e, incluso, puede estar almacenado en múltiples sistemas electrónicos, siendo prácticamente su eliminación definitiva. Esto ha llevado al autor a afirmar que "Internet constituye la mayor amenaza para la privacidad" (Grabosky, 2001, p. 246). Finalmente, la transnacionalidad también es otra de las características del ciberespacio, que si bien es beneficiosa porque acerca a millones de personas situadas a miles de kilómetros de distancia, también permite que los delitos puedan ser cometidos desde el otro lado del mundo tan fácilmente como desde el edificio de al lado. Y esta característica no es simplemente que haga más difícil la identificación del autor, sino que también impedirá en gran medida el enjuiciamiento del infractor debido, en gran parte, a las discrepancias entre los Estados para establecer los límites. Todas estas situaciones vienen a poner de manifiesto que el ciberespacio tiene la misma función que "una parada de autobús, el patio del colegio o la discoteca" (Grabosky, 2001, p. 244), es un lugar de encuentro entre agresores motivados y potenciales víctimas.

Para entender dónde y por qué ocurre el cibercrimen, Grabosky (2007) propone analizarlo desde el enfoque de las actividades cotidianas (Cohen y Felson, 1979), entendiendo que el cibercrimen puede ser explicado por la intersección de un agresor potencial, un objetivo adecuado o una probable víctima y la ausencia de un guardián capaz. La presencia de los tres factores en un mismo lugar favorece la aparición del cibercrimen, o lo que es lo mismo, la ausencia de uno de ellos puede hacer que el evento criminal no ocurra.

Cuando analiza los tres elementos por separado, sugiere respecto del primero (agresor potencial), que el número de personas motivadas para cometer un delito es un reflejo del número de individuos con acceso a Internet (Grabosky, 2007). Y cuantas más personas haya conectadas a Internet, más personas habrá en condiciones de utilizar la tecnología para fines ilegales.

El desarrollo que están alcanzando las tecnologías de la información y la comunicación permite la consecución de múltiples objetivos, ya sean estos legítimos o ilegítimos. Y en este sentido, advierte el autor que hay tantas motivaciones para cometer el delito como tipos de ataque se pueden realizar al ciberespacio y son "tan antiguos como la historia humana" (Grabosky, 2007; p.45). Además de tener en cuenta que un mismo hecho delictivo puede responder a muchas motivaciones. Así, el hacking y el cibervandalismo podrían ser realizados por curiosidad, por aventura, o para llamar la atención. Los delitos financieros suelen responder a la codicia. La lujuria es reflejada por la ubicuidad de los sitios web sexualmente explícitos. La rebelión a menudo subyace en los esfuerzos para causar daños a los símbolos del poder, como la Casa Blanca, McDonald´s, etc. Y la venganza puede verse reflejada en el robo, o en el daño infligido a una institución por parte de un empleado o ex empleado. En definitiva, lo que el autor sugiere es que las motivaciones de los delincuentes no son nuevas, el elemento de novedad en el cibercrimen "reside en la capacidad sin precedentes de la tecnología para facilitar que actúen estas motivaciones" (2001, p.244).

Sobre el segundo elemento de la TAC (las víctimas potenciales) entiende que, al igual que sucede con los agresores motivados, el

suministro de víctimas potenciales está en función del despegue de las tecnologías. Más allá del aumento exponencial en el número de usuarios individuales, y en la medida que aumenta la conectividad entre los ordenadores y las comunicaciones y aumenta la penetración de los ordenadores en las sociedades industriales occidentales, también pueden ser explotados para fines delictivos. Cualquier nueva aplicación (el chat, las transferencias bancarias, etc.) presentan nuevas oportunidades para cometer delitos.

Respecto al tercer elemento (el guardián) entiende que tiene la función básica de ejercer la vigilancia sobre las personas o lugares con el propósito de prevenir el delito, o para permitir una respuesta puntual en el caso de que éste se cometa. Considera que, al igual que en el mundo físico, la figura del guardián puede ser ejercida por los padres, profesores, policías, o por aplicaciones tecnológicas. Así, los padres pueden controlar lo que hacen los menores en Internet para que no accedan a lugares peligrosos; los empresarios pueden controlar que los trabajadores no lleven a cabo conductas que pueden ir desde el acoso sexual, a la exposición de virus; los administradores de sistemas también pueden impedir el acceso a códigos maliciosos que dañen la capacidad de la red. Además, el ciberespacio cuenta con abundantes sistemas tecnológicos que pueden ejercer de guardianes, como los programas de Windows que registran las páginas que han sido visitadas, el software que detecta intrusos, los programas de encriptado, etc.

Aunque advierte que los guardianes no siempre funcionan como deberían: los padres pueden tener pocos conocimientos o pueden descuidar la supervisión, los usuarios se preocupan poco por

las páginas web que visitan o por los archivos que reciben, usan contraseñas fáciles de adivinar o las dejan a la vista, pueden dejar de actualizar los antivirus, etc. Y es que argumenta que Internet fue diseñado para compartir información, no preocupándose desde el inicio por la seguridad, y que aunque las cosas están cambiando, todavía siguen existiendo oportunidades para el delito.

De cara a la prevención, advierte que se podrán aplicar antiguas estrategias en la medida que se trata de luchar contra viejas formas de criminalidad, pero también se tendrán que aplicar nuevas en la medida que estamos en un nuevo lugar. En este sentido, afirma que "el cibercrimen es tan diverso y está tan extendido que necesita el esfuerzo de muchos individuos, y de las instituciones, para hacer una prevención y un control efectivos. Al igual que las Policías de las sociedades industriales occidentales reconocen que la reducción efectiva de la delincuencia terrestre requerirá asociaciones con la industria y con la comunidad, por esa misma vía pasa la respuesta para el cibercrimen" (2007; p.91).

Establece, además, dos puntos fundamentales para reducir la oportunidad en el ciberespacio: por un lado, hay que minimizar las inconveniencias para los usuarios; y, por otro, maximizar el esfuerzo requerido por los agresores para llevar a cabo sus actividades delictivas. Respecto a este último punto, entiende que reducir el número de agresores es difícil pues "restringir el acceso a la tecnología se está convirtiendo en una respuesta poco realista para los delincuentes condenados" (2007; p.92). Y también piensa que poco se puede hacer para que las personas sean menos ambiciosas, lujuriosas o vengativas. Esto no implica que no se pueda mejorar el civismo en el

ciberespacio estableciendo normas básicas de funcionamientos. En este sentido, si el proceso de socialización informal es insuficiente para convencer a la gente sobre qué tipos de comportamientos son inaceptables, quizás una solución pueda ser que los gobiernos prevean sanciones para actos como la piratería, la denegación de servicios, etc. con el objetivo de conseguir que los delincuentes se lo piensen dos veces antes de llevar a cabo estas conductas.

Por otro lado, considera que es necesario "endurecer el destino" limitando las oportunidades de aquellos objetivos que son más vulnerables que otros. Del mismo modo que se instalan cerrojos en las ventanas y puertas de las casas para dificultar el acceso, en los sistemas informáticos se puede instalar programas como los *firewalls*, antivirus, filtros, accesos controlados por contraseñas, etc. que limiten la entrada. No obstante, atendiendo a las particularidades que presenta el cibercrimen y teniendo en cuenta la configuración del nuevo ámbito, será la propia víctima la que con sus actos impida desde un primer momento que el agresor alcance sus objetivos, pues como afirma Peter Grabosky "la primera línea para la defensa es la autodefensa" (Grabosky, 2001, p. 248).

2.1.2. La adaptación de la TAC al ciberespacio por Majid Yar

La propuesta de Peter Grabosky fue el caldo de cultivo para para posteriores trabajos en los que se plantea también la aplicabilidad de la TAC al ciberespacio. Una de las obras de referencia es la es la elaborada por Majid Yar, titulada "*The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory*" (2005). En este trabajo,

el autor se plantea si, del mismo modo que las actividades cotidianas de los actores sociales crean condiciones en que las personas y los bienes pasan a estar disponibles como dianas para aquellos que están motivados, las actividades cotidianas en línea ayudan (y cómo lo hacen) a que las personas traduzcan sus inclinaciones criminales a la acción.

La primera cuestión que sostiene el autor es que la TAC tiene un enfoque ecológico donde el lugar juega un papel fundamental en la explicación del evento delictivo, en el sentido de que los elementos del crimen deben converger en el espacio y en el tiempo. Así, para que las actividades cotidianas creen oportunidades delictivas, deben ocurrir en un espacio concreto y a unas determinadas horas, o lo que es lo mismo, la probabilidad de que un crimen se consuma dependerá de que los objetivos estén accesibles en términos de tiempo y espacio para el agresor potencial. Como afirma Felson (1998) "la organización del tiempo y el espacio es central… ayuda a explicar cómo ocurre el crimen y qué hacer con él" (p. 147). Por tanto, plantea Majid Yar que para poder trasladar la TAC al entorno virtual es necesario que en el ciberespacio se presenten las mismas particularidades en cuanto a lugar, proximidad, distancia y orden temporal.

Partiendo de la premisa de que el lugar es clave, compara en primer lugar los dos espacio, el físico y el virtual, para determinar la similitudes y diferencias entre ellos. Entre las similitudes destaca dos. La primera de ellas, es que el espacio físico debe ser concebido "no como una 'realidad virtual' sino más bien como una 'virtualidad real'" (Yar, 2005; p. 416). Esto es así porque el espacio virtual no es algo imaginario completamente alejado de la realidad, todo lo contrario, está completamente arraigado al mundo físico, en dos direcciones: a

través de Internet se establecen todo tipo de interacciones políticas, económicas, sociales y culturales; pero al mismo tiempo, todo lo que sucede en Internet tiene efecto directo sobre lo que sucede en el espacio físico. Señala como segunda similitud, que en el ciberespacio las distancias entre los lugares no son equidistantes. En este sentido argumenta, que si bien la distancia entre dos puntos es siempre la misma (distancia cero), hay dominios que tienen una mayor densidad de conexiones porque los motores de búsqueda priorizan sobre los sitios que tienen mayor número de vínculos, y por lo tanto, unos lugares están más accesibles.

En contraposición, considera que mientras que el espacio físico es relativamente estable y perdurable, el ciberespacio se caracteriza por una extrema volatilidad en sus configuraciones. En este sentido, los cambios en la organización en el espacio físico son graduales porque se materializan en objetos físicos duraderos (edificios, carreteras, puentes, paredes, etc.). Y aunque éstos sufren cambios (por ejemplo, la proximidad entre dos puntos puede depender del desarrollo de los transportes) lo cierto es que no se pueden comparar al ciberespacio donde los lugares y las entidades virtuales aparecen y desaparecen con un ritmo vertiginoso, pues la distancia entre dos sitios puede cambiar con la simple adición de un hipervínculo que proporciona una ruta directa.

Respecto a la estructura temporal, de nuevo, entiende que difícilmente se puede comparar con la del espacio físico. El ciberespacio, como entorno virtual global, está frecuentado por usuarios que viven en diferentes zona horarias, provocando que haya actividad las 24 horas al día y 7 días a la semana. Además, las

actividades en el ciberespacio relacionadas con el hogar, el trabajo y con las actividades de ocio no pueden ser claramente delimitadas como se hace en el espacio físico. Por lo tanto, al no haber franjas horarias perfectamente delimitadas en las que los actores puedan anticipar su presencia o ausencia provoca, desde el punto de vista de las TAC, desorganización espacio-temporal hace difícil identificar patrones donde converjan los elementos del crimen.

Las divergencias encontradas entre los elementos de continuidad espacial, proximidad, separación y distancia, que son claves para explicar la probabilidad de ocurra un delito, hace que el autor considere muy difícil la adaptación del enfoque de la TAC al espacio virtual. Sin embargo, señala muchas características que ponen de manifiesto que el ciberespacio es un lugar que ofrece oportunidades para cometer delitos.

Es precisamente la contracción del espacio lo que "hace posible encuentros instantáneos e interacción entre actores que están distanciados, creando nuevas posibilidades de asociación e intercambio. Esto nos hace vulnerables a potenciales depredadores que nos tienen al alcance inmediato, sin las barreras normales de la distancia física" (Yar, 2005; p.410). Además, destaca que las características del nuevo espacio amplifican las habilidades del potencial agresor para atacar a personas y bienes: "permite a una sola persona llegar, interactuar y afectar a miles de personas al mismo tiempo" (Yar, 2005; p. 411). En palabras de Yar, la "tecnología es un multiplicador de fuerzas, para que las personas con mínimos recursos generen enormes efectos negativos" (2005; p. 411), en el sentido de que el envío de correos "*scam*" masivos o *malware* a miles de personas

tiene un coste bajo, pero sus efectos son especialmente dañinos. Finalmente, también señala, al igual que Grabosky (2001), que el anonimato favorece la criminalidad, pues el hecho de que una persona pueda adoptar una identidad distinta, le permite realizar actos delictivos sin que sea posible identificarlo.

Por tanto, desde una perspectiva "macro", la compresión de las barreras espacio-temporales, la mayor conectividad, el anonimato y las plasticidades de la identidad, hacen posible nuevas formas y patrones de actividad ilícita. Pero no se limita a hacer un análisis desde una perspectiva "macro", también lo hace desde una perspectiva "micro" analizando de manera separada todos los elementos que componen el triángulo del delitos (delincuente potencia, objetivo adecuado y guardián capaz). Respecto al primero de los elementos, el agresor potencial, se limita a comentar que su presencia es esencial para la comisión del crimen sin hacer mayores interpretaciones sobre el elemento. En cambio, sí se para a analizar cómo los otros dos elementos, objetivo adecuado y guardián capaz, encajan en el entorno virtual.

Sobre el objetivo adecuado, piensa que las características que lo configuran varían unos grados cuando se trasladan al mundo virtual. Sin entrar a profundizar en este aspecto, pues se analizará con detalle más adelante, el autor entiende que las cuatro características que propone Felson mediante el acrónimo VIVA (*value, inertia, visibility y accesibility*), es el valor la única que no difiere en el espacio virtual, en tanto que el valor dependerá de la intencionalidad del agresor. Respecto a la inercia, argumenta que mientras que en el espacio físico podemos diferenciar claramente los diferentes objetivos por sus

propiedades físicas, en el ciberespacio al ser todos bienes informacionales apenas se pueden hacer distinciones entre ellos por sus propiedades intrínsecas, por lo que la adecuación del objetivo no va a variar tanto como si sucede en el espacio físico. Y respecto a las dos últimas cualidades (visibilidad y accesibilidad), concluye que debido a las diferencias estructurales del ciberespacio en cuanto a la distancia, la ubicación y el movimiento, los objetivos están más visibles y más accesibles que en el espacio físico.

Respecto al guardián capaz, afirma que su presencia es casi imposible en el ciberespacio, dada la facilidad de movilidad del delincuente y las irregularidades temporales en él. Con ello no quiere decir que el elemento guardián no sea trasladable al ciberespacio, sino que su eficacia se ve limitada. De hecho, al igual que ocurre en el espacio físico, en el espacio virtual hay guardianes formales, privados e informacionales. La policía está presente en el ciberespacio, sin embargo, es muy poco probable que no esté en el lugar concreto cuando se produce el crimen (como generalmente sucede en el espacio físico). También los administradores de sistemas, el personal de seguridad, y los ciudadanos, pueden ejercer una amplia gama de controles sobre el comportamiento *online* de los demás. Pero los que ejercen mayor protección son los guardianes físicos o tecnológicos como los sistemas antivirus que están activos constantemente. No obstante, como ya se ha comentado, lo que han provocado las propiedades espacio-temporales del nuevo entorno es que se hayan amplificado las limitaciones establecidas al guardián físico en el espacio físico.

En resumen, respecto a los tres elementos: hay similitudes entre los delincuentes motivados entre los dos entornos; la construcción del objetivo adecuado es más complejo, y hay semejanzas respecto al valor pero no respecto a la inercia, visibilidad y accesibilidad; y el elemento guardián capaz puede ajustarse mejor, pero es más difícil una tutela efectiva. Todo ello, debido a la organización del espacio y el tiempo, que en el ámbito físico es relativamente fijo, mientras que en el ciberespacio es desorganizado, lo que hace que no sea posible la aplicación directa de la TAC al ciberespacio. Así, haciendo referencia a la metáfora realizada por Peter Grabosky (2001), Majid Yar considera que, más que "viejo vino en nuevas botellas" ('*old wine in the new bottle'),* el cibercrimen es "viejo vino en la no botella" ('old wine in no bottle') o, más bien, "viejo vino en botellas de diferentes formas y fluidos" ('old wine" in bottles of varying and fluid shape').

2.1.3. La teoría de las actividades cotidianas en el ciberespacio de Fernando Miró

Por su parte, Fernando Miró (2012) entiende que existe una posición intermedia entre las adoptadas por Peter Grabosky (2001) y Majid Yar (2005) cuando afirma que "la cibercriminalidad comparte con la delincuencia todos los elementos definitorios del concepto de 'crimen', pero dándose los mismos de una forma tal en el nuevo ámbito que es el ciberespacio, que puede influir significativamente en la explicación del delito y, por tanto, en su prevención" (Miró, 2012; p.144). Siguiendo el símil de "*Old wine en new bottles"*, Miró (2011) dice que "el cibercrimen es el mismo vino pero en botellas distintas, no ya sólo nuevas, sino diferentes, en las que probablemente la forma

tradicional de beber ya no sea válida [...] se tratará de beber vino, pero tenemos que replantearnos cómo hacerlo, dado que el recipiente desde el que se ingiere es ahora otro" (p. 43).

Miró (2011) coincide con Yar (2005) en que las características espacio-temporales del nuevo ámbito cambian y hacen que se modifiquen los condicionantes del delito. Pero discrepa, al entender que el enfoque de las actividades cotidianas (como así entiende Garbosky, 2007) es apto para explicar el fenómeno de la criminalidad en el ámbito virtual. Argumenta, en primer lugar, que es precisamente el hecho de que la teoría pone el acento en el lugar y no en el delincuente -como tradicionalmente han hecho otras teorías- lo que permite su adaptación. El hecho de que nos encontremos ante un lugar nuevo, con unas características intrínsecas y extrínsecas distintas al espacio tradicional, es lo que hace oportuno seleccionar aquellas teorías o enfoques que prestan atención al lugar de comisión delictiva para comprobar los nuevos caracteres del evento criminal.

Afirma también, como segundo argumento, que "si en el momento en que se anunció esta teoría, ello se apoya en evoluciones tecnológicas como el automóvil y sociales como la igualdad entre hombre y mujer, que habían modificado la relación entre el ofensor motivado, el objetivo y la ausencia de mecanismos de defensa, hoy, la aparición de un nuevo espacio de comunicación personal transnacional, universal y sujeto a revolución permanente, como es el ciberespacio, anticipa la existencia de un nuevo contexto de oportunidad criminal que coexistirá en el tiempo con el de la realidad física, y que pudiendo compartir con éste el que el delito dependerá de la relación entre victimario, víctima y mecanismos de protección,

divergirá en la manifestación concreta de estos mismos factores, fruto de la especialidad del medio en que convergen. Una teoría, como la de las actividades cotidianas, que presta tanto atención a la relación entre cambio tecnológico y cambio del crimen, es especialmente adecuada para el análisis de si las TIC conllevan la creación de un ámbito de oportunidad criminal nuevo y distinto." (Miró, 2011; p. 17).

Por último, otra razón en la que se basa el autor para recurrir a las teorías de la oportunidad, está centrada en la necesidad de encontrar teorías que pongan el acento de la prevención en el control no formal. El ciberespacio es transnacional y anonimizado, lo que hace que hace que el Sistema de Justicia Penal tenga una capacidad aún más limitada ante esta forma de criminalidad, y sea necesario acudir, no sólo a lo normativo y lo formal, sino también a lo ambiental y al propio actuar cotidiano de quienes acceden e interactúan en Internet.

El planteamiento de Miró Llinares, en todo caso, es algo más ambicioso dado que inicia su análisis tratando de comprender los caracteres del nuevo espacio de oportunidad criminal. Siguiendo la idea de Capeller (2001)[25], Miró (2001) comienza haciendo un análisis del "lugar" para, a continuación, analizar cómo los cambios estructurales afectan a los elementos del crimen. La contracción de las distancias, haciendo posible que la comunicación se expanda, sumado a otras características extrínsecas del ciberespacio (como la transnacionalidad, la neutralidad, a su carácter descentralizado,

[25] Capeller, ya en 2001, apuntaba que ciertas características de Internet (transnacionalidad, fugacidad, volatilidad de sus contenidos, y estrategias de los operadores de la comunidad virtual) hacen necesaria una revisión de la teoría criminológica.

distribuido, universal, popular, anonimizado, sujeto a revolución permanente y abierto al cambio), hacen que los elementos inicialmente planteados, así como los incorporados en las siguientes formulaciones, sigan presentes en el cibercrimen, sin modificaciones esenciales pero sí cambiando la manera en que éstos se relacionan.

No obstante, advierte que el campo de oportunidad de un agresor motivado es mucho más amplio en el ciberespacio. La principal razón se debe a la inexistencia de barreras físicas que impidan el acercamiento entre agresores motivados y potenciales víctimas. Es decir, el hecho de que no sea necesario que exista una cercanía física entre agresor y víctima, conlleva que el campo de actuación del agresor sea mucho mayor. En las propias palabras del autor: "aumenta considerablemente el número de personas que pueden contactar unas con otras como agresores y objetivos adecuados, expandiéndose, por tanto, el ámbito de oportunidad criminal" (Miró, 2011; p. 21). Además, la configuración del nuevo lugar afecta a las posibilidades de motivación del potencial agresor por dos vías: la primera de ellas derivada de la eliminación de la distancia y el tiempo necesarios para atacar un bien, por lo que se incrementa el número de potenciales objetivos sobre los que se puede tomar la decisión de si es el adecuado; y, por otro lado, también se reducen los costes espacio-temporales para cometer el delito, no sólo en cuanto a la aproximación al objetivo, sino también en los términos del coste de huida del lugar del delito, al igual como ocurre en el espacio físico.

Apunta, como también advierte Yar (2005), que las nuevas tecnologías aumentan las posibilidades de ataque, ya no sólo en cuanto al número de potenciales víctimas, sino al daño que pueden

generar con los mínimos costes. En este sentido, un usuario con motivación delictiva puede atacar a muchos otros a la vez, aunque éstos se encuentren a miles de kilómetros de distancia con el agresor y entre ellos mismos. Si lo trasladamos al espacio real, pocas armas podremos encontrar que puedan atacar a objetivos que se encuentren a kilómetros de distancia y, menos aún, que puedan atacar a múltiples objetivos que entre sí se encuentren también a kilómetros.

Además, diferentes agresores se pueden poner de acuerdo para atacar a un solo objetivo, y también, un solo agresor puede emplear distintos sistemas informáticos situados en múltiples lugares, creando por ejemplo una *botnet*[26], para realizar múltiples ataques a un objetivo -o a varios- sin que sea necesario trasladarse de un lugar a otro. Incluso no es necesario que el agresor seleccione a una sola víctima concreta. Sobre todo en el caso del *malware*, donde el agresor puede depositarlo en un lugar en forma de archivo multimedia (Taylor et al., 2006), esperando que sea la propia víctima la que, al interactuar con el archivo, se infecte. Incluso, que sea la propia víctima la que propague la infección a otros usuarios, sin necesidad de mayor esfuerzo por parte del agresor.

[26] Un *botnet* se define como un conjunto de ordenadores controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de *spam*, ataques de *DoS*, etc. Definición obtenida el 16 de mayo de 2014 del Instituto Nacional de las Tecnologías de la comunicación http://www.inteco.es/glossary/Formacion/Glosario/Botnet

Por tanto, (hablando en términos de la víctima adecuada) si la limitación de barreras físicas aumenta el número de potenciales agresores, a su vez, también aumenta el número de potenciales víctimas, dado que el ciberespacio acerca a un mismo lugar a todos los usuarios. Tal como afirma, "los *suitable targuets* no tienen que encontrarse a una distancia cercana al agresor para serlo, sino que pueden convertirse en víctima objetivos situados en el mismo ciberespacio, aunque a miles de kilómetros de distancia" (Miró, 2011, p. 26).

En lo que sí difiere el autor respecto al planteamiento inicial de la TAC, es en los elementos que hacen adecuado a un objetivo en el ciberespacio. Considera que son distintos al espacio físico, precisamente por el cambio sustancial del lugar. La configuración del nuevo espacio, no sólo hace que la relación entre los elementos cambie, sino que las características que hacen que sea más adecuado para al agresor cambian también, tal como se verá en profundidad más adelante.

Finalmente, respecto al último elemento (guardián capaz) el autor considera que disminuye su capacidad en el ciberespacio. La eliminación de las barreras físicas así como la popularización de las TIC, su transnacionalidad y su anonimización hacen muy difícil que el guardián pueda proteger a la víctima. Esto, a su vez, hace que el potencial agresor perciba un menor riesgo, aumentando así su motivación hacia el delito, al considerar más compleja su identificación y su persecución por el sistema de Justicia.

Realiza un análisis del guardián capaz, distinguiendo entre el *manager* o gestor del lugar, y el guardián que opera directamente

sobre la víctima, de acuerdo con la propuesta realizada por Eck (1994). Sobre el *manager* , o gestor, que es el encargado de proteger el lugar, considera Miró que la ausencia de controles supranacionales que tomen decisiones relativas a los servidores que estén por encima de las legislaciones estatales (debido a que el ciberespacio es descentralizado y distribuido) imposibilita que haya unos gestores centralizados que vigilen el ciberespacio de forma global. Así, el ámbito de actuación del control formal es reducido.

Cuestión distinta es el guardián capaz, aquél que se encarga de la vigilancia con respecto de los objetivos adecuados. Para Miró, y como han identificado otros autores (Bossler y Holt, 2009; Choi, 2008; Grabosky, 2007; Holt y Bossler, 2009; Yar, 2005), los guardianes pueden ser los diferentes programas creados para la lucha contra las intrusiones como los antivirus, firewall, anti espías, etc. Sin embargo, apunta Miró (2011), que estos elementos, dependen en última instancia de la actuación de la víctima, pues será ella quien deba instalarlos y mantenerlos actualizados para su correcto funcionamiento. Por tanto, Miró Llinares anticipa que más que de un guardián ajeno, estos son elementos que configurarían la propia autodefensa. Si siguiéramos lo planteado por Cohen y Felson, que interpretaban el guardián como elementos que no parten de la propia víctima, como vecinos, amigos, cámaras de seguridad, no podríamos hablar en estos casos de guardián capaz sino del elemento objetivo adecuado. En todo caso Miró también afirma la existencia de otros elementos o personas que sí que pueden ejercer protección sobre las potenciales víctimas. Un ejemplo de esto, puede ser la propuesta que realiza Marcum (2008), acerca de que los padres pueden ejercer como guardianes de sus hijos cuando navegan por Internet.

2.2. La aplicación de la teoría de las actividades cotidianas al análisis del riesgo de cibervictimización

Además de todos los trabajos teóricos que tratan de reinterpretar la teoría de las actividades cotidianas al nuevo ámbito de oportunidad criminal que es el ciberespacio, en los últimos años han proliferado los estudios que, desde una perspectiva empírica, también han tratado de analizar la aplicabilidad de la teoría de las actividades cotidianas al cibercrimen. Todos lo han hecho dirigiéndose directamente a los usuarios de Internet y preguntándoles a través de encuestas de victimización (bien en formato papel, digital o llamada telefónica) sobre su experiencia ante la victimización, y sobre su uso cotidiano de Internet. Pero, como se verá a continuación, cada uno lo lleva a la práctica de manera distinta. En vista de ello, el objetivo de este apartado, no es otro que analizar cómo los autores han operativizado los diferentes constructos de la teoría de las actividades cotidianas, cuáles son los factores determinantes en el producción de la cibervictimización y las principales conclusiones respecto a la aplicabilidad de esta teoría al cibercrimen. Y todo ello, haciendo distinción entre los estudios enfocados al análisis de la cibercriminalidad económica, y los centrados en la cibercriminalidad social.

2.2.1. Estudios de la TAC aplicados a la cibervictimización económica

Como ya se ha dicho, cuando nos referimos a la cibercriminalidad económica lo hacemos en un sentido criminológico,

como categoría que incluye toda forma de cibercriminalidad realizada por su autor con un propósito o intención de obtener un beneficio patrimonial. Así, y siguiendo a Miró (2012), el cibercrimen económico, por tanto, no es tan sólo aquél tipo de ataque delictivo que afecta al patrimonio de las personas individuales o al sistema económico en relación con las transacciones comerciales en Internet, sino que también entraría dentro de esta categoría todos los ciberataques cuyo objetivo final sea la consecución de un beneficio económico aunque afecten a otros bienes jurídicos como la intimidad, la seguridad de los sistemas y redes, etc.

Y si bien no es el propósito de esta tesis doctoral es el estudio de los factores de riesgo de victimización asociados a la denominada cibervictimización económica, sí que resulta del máximo interés analizar cómo se han llevado a cabo los estudios que tratan de relacionar las actividades cotidianas de los usuarios de Internet con la victimización por conductas tan usuales como la infección de virus, la recepción de correos de *phishing* o *scam*, y similares.

Seguidamente, pues, se procederá a un análisis de los estudios que se han hecho al respecto prestando especial atención a dos cuestiones de especial importancia: La primera, el análisis de cómo se han concretado las diferentes variables derivadas de la utilización teórica del *approach* de las actividades cotidianas. La segunda, teniendo en cuenta los resultados de los estudios especialmente en lo relativo a la identificación de los factores de riesgo para la victimización por los ciberdelitos objeto de estudio en cada trabajo.

2.2.1.1. Operativización de las variables

La aplicación de la Teoría de las actividades cotidianas a la cibercriminalidad por medio de estudios empíricos basados en encuestas de victimización, ha sido llevada a cabo por la gran mayoría de los autores tratando de identificar variables independientes derivadas de cada uno de los elementos del triángulo del crimen. Con la excepción de Miró (2014c), todos los autores que han desarrollado estudios de este tipo, han tratado de identificar en la cotidianeidad de los sujetos usuarios de Internet variables relacionadas con el agresor potencial, con el objetivo adecuado y con el guardián capaz. La idea vendría a ser que, si la teoría afirma que para que exista un cibercrimen es necesario que confluyan un agresor potencial, un objetivo adecuado y la ausencia de un vigilante, es necesario identificar por medio de variables condiciones que hacen que aparezca el agresor, que el objetivo sea adecuado, y que no funcione la vigilancia por parte el guardián. Esto también ha sido así en el caso de los estudios de victimización económica tal y como veremos a continuación al analizar cómo se han tratado de definir dichas variables.

De los tres elementos de la teoría de las actividades cotidianas en el ciberespacio (agresor motivado, objetivo adecuado y guardián capaz) parece que es el del "guardián capaz" el que con mayor facilidad identifican los autores. No obstante, se puede observar como cada uno de ellos hace su reinterpretación y añade elementos que los diferencian unos de otros. El primer estudio que se realizó lo llevó a cabo Choi (2008), que entendió que el guardián capaz en el ciberespacio tenía que ser identificado con los sistemas digitales de protección. Así distinguió dos variables: una relativa al uso de software de seguridad

(poseer antivirus, antiespía y cortafuegos) y otra relativa al tiempo de tenencia de éste tipo de *software*. Bossler y Holt (2009), por su parte, consideran que, además de los diferentes programas informáticos, hay otros elementos que se deben identificar como guardián capaz. Así, distinguen entre el guardián físico, el social y el personal. El guardián físico, como así considera Choi (2008), es cada uno de los diferentes programas informáticos de seguridad incorporados por el usuario a sus sistemas informáticos. El guardián social es identificado con tener amigos con comportamientos desviados en Internet.[27] Y el guardián personal es la habilidad de los usuarios en el manejo de los sistemas informáticos. Ngo y Paternoster (2011) distinguen, por un lado, como guardián físico, el uso de software de seguridad (antivirus, antiespía y cortafuegos); y, por otro, el guardián social, entendido como la habilidad en el manejo de los equipos informáticos, y el haberse formado sobre los riesgos en Internet, bien asistiendo a cursos o bien autoformándose mediante páginas de Internet.

Más complicada resulta la identificación de los otros dos elementos de la teoría de las actividades cotidianas (agresor motivado y objetivo adecuado). Respecto del primer elemento, casi resulta obvio que a partir de una encuesta de victimización no podamos obtener información práctica, pues desde el momento en el que estamos obteniendo la información desde la óptica de la víctima, difícilmente podemos obtener una información libre de subjetividad. No es de

[27] Sin entrar a discutir su idoneidad, pues no ejercen un control directo sobre la víctima o sus bienes, su medición se basa en preguntar a los usuarios cuántos amigos tienen que piratean software u otros archivos media, ven pornografía o material obsceno *online*, o practican *hacking*.

extrañar, por tanto, que diferentes autores hayan decidido cambiar el elemento agresor motivado por la "exposición al delincuente motivado". En este sentido, Ngo y Paternoster (2011) han identificado la exposición al delincuente motivado con el número de horas pasado en Internet, el número de horas utilizando el correo electrónico, el número de horas pasadas utilizando la mensajería instantánea, y el número de horas utilizando salas de chat. Estas variables han sido utilizadas por otros autores pero identificándolas con otros constructos. Así por ejemplo, Choi (2008) habla de estilo de vida de los usuario en Internet. Para ello crea tres escalas. La primera de ellas, denominada "*vocational and leisure activities scale*", tiene como objetivo preguntar a los usuarios por el uso de la mensajería instantánea, el tiempo dedicado a descargar archivos, a comprar, a pasar el tiempo en Internet para entretenerse, a pasar el tiempo en Internet cuando se está aburrido, a ver noticias, o a comprobar y enviar correos electrónicos. La segunda, denominada "*Risky Leisure Activities*", incluye como ítems visitar páginas web, y descargar juegos, músicas y películas. Y la tercera, "*Risky Vocational Activities*", incluye abrir enlaces o archivos recibidos a través del correo electrónico y mensajería instantánea, y acceder a los mensajes pop-up. Bossler y Holt (2009), también denominan como uso rutinario del ordenador ("*routine computer use*") el compartir el ordenador, el tipo de conexión, el tiempo dedicado a la semana a comprar o jugar a videojuegos, a comprobar el correo electrónico, a utilizar salas de chat, mensajería instantánea, o redes sociales, a descargar programas, programar, y hacer uso de la banca *online*. Pratt, Holtfreter y Reisig (2010), para el análisis del ciberfraude, también hablan de factores relativos a las

actividades cotidianas de los usuarios, incluyendo el número de horas pasadas a la semana en Internet y si han realizado compras *online*.

Respecto del "objetivo adecuado", solo hay tres trabajos que hacen mención a este constructo en el análisis de la cibercriminalidad económica. El primero es el de Ngo y Paternoster (2011), que identifican este elemento con realizar comunicaciones con extraños y proporcionar información personal a otras personas a través de Internet. El segundo trabajo es el realizado por Wilsem (2011), que incluye sólo variables relativas al objetivo adecuado, distinguiendo dos tipos de actividades cotidianas: las que ofrecen accesibilidad al objetivo (incluyendo como variable comprar) y las que hacen que el sujeto sea visible en el ciberespacio: visitar foros, hacer uso de las redes sociales y de la webcam.

Finalmente, Miró (2014c) hace un planteamiento completamente distinto al que hemos visto que realizan el resto de autores, entendiendo que todos los elementos estudiados en este tipo de análisis son factores relativos a la propia víctima. En la medida en que se está preguntado a la víctima por su actuar en Internet (qué es lo que hace) y no por lo que hacen otros con respecto a ella, se están estudiando los elementos que hacen a un usuario "adecuado" (*suitable*) para la victimización. Esto incluye, obviamente, lo denominado por los autores como "exposición al delincuente motivado", como "actividad cotidiana". Pero, también contiene otros elementos. Desde este punto de vista, el "comportamiento desviado de los usuarios" identificado por Bossler y Holt (2009) y también por Ngo y Paternoster (2011) con piratear, ver pornografía *online*, intentar averiguar contraseñas y acceder a otros ordenadores (*hacking*),

también son elementos del objetivo adecuado, en tanto en cuanto es un comportamiento de la potencial víctima. Asimismo, incluye también como objetivo adecuado aquellos elementos identificados hasta el momento por otros autores como "guardián capaz", pues tener software de seguridad depende de que los usuarios se hagan con él y, en cualquier caso, se requiere para su correcto funcionamiento que los usuarios lo actualicen. Y más aún, cuando hacen referencia a la habilidad del sujeto para el uso de las TIC (guardián personal propuesto por Ngo y Paternoster, 2011), o tener amigos que tienen un comportamiento desviado en Internet (guardián social propuesto por Bossler y Holt, 2009).

Teniendo en cuenta que Miró (2014c) hace en todo momento referencia al constructo "objetivo adecuado", distingue dos factores: interacción y autoprotección. Con el término interacción hace referencia a las actividades que realizan los sujetos que les hacen ser más visibles en el ciberespacio, como el uso de la mensajería instantánea, redes sociales, foros y blogs, videoconferencias, comprar, descargar archivos, consumir pornografía, jugar a videojuegos *online*, facilitar información personal, y contactar con extraños. Y con el de autoprotección, se refiere al conjunto de los actos que realiza el sujeto para protegerse, como hacer uso de antivirus, no usar la misma contraseña para todo y cambiarla con frecuencia, y hacer uso de software de seguridad.

Para facilitar la consulta sobre como los autores han concretado las diferentes variables relativas a la TAC en el estudio de la cibervictimización económica, a continuación se presenta un tabla resumen:

Tabla 1. Revisión sobre la construcción de las variables de la TAC en los estudios de victimización económica

Referencia	Muestra	Variable dependiente	Variable Independiente	Análisis
Bossler y Holt (2009)	578 universitarios, 43% hombres y 57 % mujeres, edad: entre 19 y 26 años (media 20 años)	Pérdida de información por infección de *software* malicioso	Uso rutinario del ordenador: - compartir ordenador - tipo de conexión - comprar, - jugar - correo electrónico - usar salas de chat, - mensajería instantánea, - redes sociales - descargar programas, programas - hacer uso de la banca online Guardián Capaz: - Guardián físico (uso de software de seguridad) - Guardián social (tener amigos con comportamientos desviados en Internet) - Guardián personal (habilidad del usuario en manejo de sistemas informáticos)	Modelo de regresión logística
Choi (2008)	204 Universitarios de Pensilvania	Infección de *software* malicioso	Agresor motivado: - *Vocational and leisure activities scale*: uso de mensajería instantánea, descarga archivos, compras, tiempo en Internet como entretenimiento, a pasar tiempo en Internet cuando se está aburrido, a ver noticias o a comprobar y enviar correos electrónicos) - *Risky Leisure Activities*: visitar webs, descargar juegos, música, películas	Modelo de ecuación estructural

			- *Risky Vocational Activities*: abrir enlaces o archivos recibidos a través de correo electrónico y mensajería instantánea, acceder a mensajes pop-up Guardián capaz: - Uso de *software* de seguridad - Tiempo de uso *software*	
Miró (2014c)	500 españoles 44,4% hombres y 55,6% mujeres, Edad: entre 18 y 65 años (Media 40,21 años)	-*Malware* -*Scam* -*Spam*	Objetivo adecuado: - Interacción: usar mensajería instantánea, redes sociales, foros y blogs, videoconferencias, comprar, descargar archivos, consumir pornografía, jugar a videojuegos online, facilitar información - Autoprotección (hacer uso de antivirus, no usar la misma contraseña para todo y cambiarla con frecuencia y hacer uso de software de seguridad)	Modelo de regresión logística
Ngo y Paternoster (2011)	295 universitarios. 66% mujeres y 34% hombres Edad: 18 y 87 años, (media de 40)	Infección por virus	Exposición al delincuente motivado: - Número horas en Internet - Número de horas utilizando correo electrónico, mensajería instantánea y salas de chat. Objetivo Adecuado: - Comunicar con extraños - Proporcionar información personal Guardián Capaz: - Guardián físico (uso de software de seguridad) - Guardián social (habilidad en el manejo de los equipos informáticos. Formación	Modelo de regresión logística

			sobre los riesgos en Internet)	
Pratt, Holtfretter and Reisig (2010)	922 sujetos	*Fraud Targeting* (ciberfraude)	- Número de horas pasadas a la semana en Internet - Realizar compras online	Modelo de regresión logística
Wilsem (2011)	6,201	Ciberfraude	Objetivo Adecuado: - Accesibilidad al objetivo: Comprar - Visibilidad en el ciberespacio: Visitar fotos, hacer uso de las redes sociales y de la webcam	Modelo de regresión logística

2.2.1.2. Factores de riesgo

Independientemente de cada una de las diferentes conceptualizaciones y de la operativización de las distintas variables, lo cierto es, que cada uno de estos estudios acaba obteniendo como resultados una serie de factores que pueden ser considerados como de "riesgo", en la medida en que su realización por parte de los usuarios de Internet facilitaría o incrementaría la posibilidad de ser víctima de un cibercrimen económico de los analizados en cada estudio.

Concretamente, los factores de riesgo asociados a ser víctima de *malware* son, según los resultados de Choi (2008), los relacionados con las actividades de ocio en Internet (visitar páginas web y descargar videojuegos, música y películas) y con el ámbito profesional (abrir cualquier archivo adjunto o enlace recibido por correo electrónico o mensajería instantánea). Estos resultados son contrarios a los encontrados por Bossler y Holt (2009), aunque hacen referencia a la pérdida de información provocada por la infección de *malware*,

quienes encontraron que hacer uso *software* de seguridad no reduce los riesgo, ni tampoco el hecho de tener más habilidades de manejo de las TIC. Para ellos, lo que realmente resulta un riesgo es tener amigos que consuman pornografía *online*, la velocidad de conexión a Internet (de manera que las personas que tienen un acceso más rápido y más eficiente son menos propensos a ser víctimas que los individuos con conexiones más lentas) y usar, hacer o compartir con otra persona archivos piratas. Resultados muy distintos y contradictorios obtienen Ngo y Paternoster (2011) para la infección de *malware*, pues aquellos usuarios que frecuentemente abren los archivos adjuntos o los enlaces web enviados por desconocidos al correo electrónico, o por mensajería instantánea, tienen menos probabilidad de ser victimizados. Y sin embargo, tener *software* de seguridad es un factor de riesgo. Por su parte, Miró (2014c) encontró que comprar aumenta la probabilidad de sufrir infección de *malware* en un 62,9%, pero también la aumenta consumir pornografía a través de Internet y descargarse archivos en un 69,5% y en un 66,1%, respectivamente. Es importante resaltar respecto a estas dos últimas conductas, que la literatura las ha resaltado como potencialmente dañinas porque los *hacker* suelen ocultar el *malware* en archivos que aparentemente contienen pornografía y en los archivos con contenido digital pirata para propagar la infección por el ciberespacio (Taylor et. al, 2006).

Para el caso concreto del ciberfraude, Pratt, Holtfreter y Reisig (2010) realizaron tres modelos para obtener los factores de riesgo. En el primer modelo incluyeron únicamente las variables sociodemográficas, y obtuvieron que son los jóvenes con estudios los que tienen más probabilidad de ser víctimas de fraude. En el segundo modelo, incluyeron solamente las variables de comportamiento

cotidiano, y obtuvieron que el factor que con mayor fuerza puede predecir la victimización por fraude es comprar. Finalmente, elaboraron un tercer modelo incluyendo ambos tipos de variables, las sociodemográficas y las correspondientes a las rutinas en internet, y obtuvieron como único factor explicativo el comprar a través de Internet. Estos resultados son corroborados por Wilsem (2011) pues obtuvo que comprar a través de Internet es el factor que con mayor fuerza incide en la victimización por fraude, pero que también la tiene visitar foros en Internet.

Respecto al *phishing,* la única variable que hasta el momento se ha detectado como factor de riesgo es el llevar a cabo comportamientos desviados en la red. De acuerdo con la propuesta de Ngo y Paternoster (2011), el comportamiento concreto que aumenta el riesgo es hacer o dar a otra persona software, música, películas o series de televisión piratas; acceder a los archivos o cuentas de otras personas sin previo permiso; agregar, borrar, cambiar o imprimir los archivos de otra persona sin permiso; y consumir pornografía, o material obsceno, *online*. Por su parte, Hutchings y Hayes (2009) resaltan otros factores. Concretamente, la poca experiencia en el manejo de los ordenadores y de Internet, además de hacer uso de la banca electrónica.

En cuanto a la victimización por *spam,* señala Miró (2014c) que las conductas que aumentan el riesgo de victimización son: ver pornografía a través de Internet que aumenta la probabilidad en un 72,1% frente a los que no lo hacen, escribir en foros o blogs aumenta la probabilidad en un 67,9%, realizar videoconferencias aumenta la probabilidad en un 66,5%, usar la mensajería instantánea aumenta la probabilidad en un 63,6%, usar software pirata en un 65% y usar la

misma contraseña para todo en un 63,6%. Similares resultados encuentra para ser víctima de *scam*: comprar aumenta de manera significativa la probabilidad de ser víctima en un 77,3%, consumir pornografía aumenta la probabilidad de ser víctima en un 67,3%, escribir en foros y blogs en un 64,2%, realizar videoconferencias en un 63,7%, usar la mensajería instantánea en un 63,6% y usar software pirata lo hace en un 72,5%, mientras que cambiar las contraseñas, como mínimo una vez al año, disminuye el riesgo.

Del mismo modo que en el apartado anterior, a continuación se incluye una tabla resumen sobre los resultados obtenidos en los estudios de cibervictimización económica, con el fin de facilitar el lector la consulta de los mismos:

Tabla 2. Revisión de los factores de riesgo relacionados con la cibervictimización económica

Referencia	Resultados	Predictores
Bossler y Holt (2009)	Prevalencia destrucción de datos por *software* malicioso: 36,5% Modelos: Modelo 1: R^2=0,11 Modelo 2: R^2=0,138	Pérdida de información por infección de *malware*: - Tener amigos que consuman pornografía online - Velocidad de conexión a Internet (más rápida y eficiente menor probabilidad) - Usar, hacer o compartir con otra persona archivos piratas.
Choi (2008)		*Malware:* - Actividades de ocio en Internet (visitar páginas web y descargar videojuegos, música y películas) - Ámbito profesional (abrir cualquier archivo adjunto o enlace recibido por correo electrónico o mensajería instantánea) - No usar *software* de seguridad

Hutchings y hayes (2009)	Prevalencia *phishing*: 2% Modelo1: R^2=0,26	*Phishing*: - Poca experiencia en el uso de ordenadores y de Internet. - Hacer uso de la banca electrónica.
Miró (2014c)	Prevalencia: *Spam:* 48,7% *Scam:* 47,4% *Malware*: 77,12% Modelos: Modelo 1 *spam*: R^2=0,296 Modelo 2 *scam*: R^2=0,257 Modelo 3 *malware*: R^2=0,108	Infección de *malware*: - Comprar en Internet. - Consumir pornografía a través de Internet. - Descargarse archivos *Spam*: - Ver pornografía a través de Internet. - Escribir en foros o blogs - Realizar videoconferencias - Usar mensajería instantánea - Usar s*oftware* pirata - Usar la misma contraseña para todo *Scam*: - Comprar a través de Internet. - Consumir pornografía - Escribir en foros o blogs - Realizar videoconferencias - Usar mensajería instantánea - Usar *software* pirata - No cambiar las contraseñas
Ngo y Paternoster (2011)	Modelos: Modelo 1 *Malware*: R^2=0,232 Modelo 2 *Phishing*: R^2=0,104	Infección de malware: - Tener software de seguridad *Phishing*: - Hacer o dar a otra persona *software*, música, películas o series de televisión piratas. - Acceder a archivos o cuentas ajenas sin previo permiso. - Agregar, borrar, cambiar o imprimir archivos de otras personas sin permiso. - Consumir pornografía o material obsceno online.
Pratt, Holtfretter and Reisig (2010)	Prevalencia Ciberfraude: 15,18% Modelo1:R^2=0,9	Ciberfraude - Sociodemográfico: Jóvenes con estudios - Comportamiento cotidiano: comprar *online*
Wilsem (2011)	Prevalencia ciberfraude: 2,5% Modelo1: R^2=0,068	Ciberfraude: - Comprar a través de Internet. - Visitar foros.

2.2.2. Estudios de la TAC aplicados a la cibervictimización por acoso

No sólo se ha aplicado la Teoría de las Actividades Cotidianas a la victimización por cibercriminaliad económica, sino que también se ha tratado de encontrar en las actividades cotidianas de los usuarios de Internet factores de riesgo de ser víctima de ciberdelitos sociales, especialmente de ataques de *harassment* tal y como ha sido conceptualizado tal categoría anteriormente. A continuación procederé a presentar los distintos estudios que aplican la TAC a la victimización social presentando en tablas individualizadas las características principales de cada uno de los trabajos.

El primero de los estudios realizados con este enfoque fue el de Catherine Marcum, titulado *Identifying Potencial Factors of Adolescent Online Victimization for High School Seniors* y publicado en la revista *International Journal of Cyber Criminology*. En él, la autora analiza los factores de riesgo asociados a la victimización por la exposición a material sexual explícito, *harassment* y solicitudes sexuales no deseadas, creados a partir de los constructos de la TAC.

Tabla 3. Ficha técnica del estudio *Identifying Potential Factors of Adolescent Online Victimization for High School Seniors* (Marcum, 2008)

Autor	Catherine Marcum (2008)[28]
Muestra	483 estudiantes de último curso de instituto y primero de universidad, de los cuales el 40% hombres y 60% mujeres, con una edad comprendida entre 18 (51,3%) y 19 (48,7%) años.
Variable Dependiente	Incluye tres variables dependientes: • Exposición a material explícito • Recibir solicitudes de contacto sexual • *Harassment*
Variable Independiente	Exposición al delincuente motivado: lugares en Internet que están más habitados por delincuentes motivados • Horas pasadas en Internet y horas haciendo uso de las herramientas de comunicación que provee Internet (correo electrónico, mensajería instantánea, salas de chat y redes sociales) • Actividades concretas que se suelen realizar con esas herramientas (buscar información, jugar, planificar viajes, comprar, socializar con otros y otras actividades) Objetivo adecuado: • Grado de privacidad de las cuentas de redes sociales • La información facilitada a otras personas • Información publicada en las redes sociales Guardián capaz: identificado con la cantidad de supervisión experimentada por los encuestados. • 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.)

[28] Dos años después la autora publicó otro estudio junto con Melissa L. Ricketts y George E. Higgins, usando la misma muestra y las mismas variables pero presentando los resultados distinguiendo los factores de riesgo entre chicos y chicas.

	• Restricciones de uso de Internet • Sistemas de control (ej. bloqueadores de *software*)
Análisis	Regresión logística usando el método por pasos aumentando el criterio de inclusión de las variables en el modelo a 0,2

Posteriormente se presenta en la revista *Deviant Behavior*, el artículo de Thomas J. Holt y Adam M. Bossler, titulado *Examining the applicability of lifestile-routine activities theory for cyberime victimization,* cuyo objetivo es determinar los factores de riesgo asociados al *harassment.*

Tabla 4. Ficha técnica del estudio *Examining the applicability of lifestyle-routine activities theory for cybercrime victimization* (Holt y Bossler, 2009)

Autores	Thomas J. Holt y Adam M. Bossler (2009)
Muestra	578 universitarios, 43% hombres y 57% mujeres, con una edad comprendida entre 19 y 26 años (Media 20 años)
Variable Dependiente	*Online Harassment*. Mediante la formulación de una pregunta sin especificar el tipo de conducta ("*How many times within the last 12 months have they been the victim of someone harassing them in a chatroom, IRC or Instant Message chat*")
Variable Independiente	Uso cotidiano de Internet: • Comprar, jugar, usar el correo electrónico, las redes sociales y chats • Velocidad de conexión a Internet • Compartir con otras personas el ordenador, • Horas dedicadas a Internet por cuestiones laborales, escolares u ocio • Habilidad informática • comportamiento desviado

	Guardián capaz: • Guardián físico: diferentes programas destinados a la protección (antivirus, *Spybot*, *Ad-Aware*, *firewall, hardware firewall*, *Microsoft Update*, etc.) • Guardián social: conjunto de amigos con comportamiento antisocial en Internet
Análisis	Regresión logística usando el método por pasos aumentando el criterio de inclusión de las variables en el modelo a 0,2

Otro trabajo es la Tesis realizada por Bradford W. Reyns, que lleva por título *Being a Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective.* Y cuyos resultados también fueron publicados un año más tarde en la revista *Criminal Justice and Behavior* junto con Bill Henson y Bonnie S. Fisher (Reyns et al., 2011).

Tabla 5. Ficha técnica del estudio Being a Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective (Reyns, 2010)

Autor	Bradford W. Reyns (2010)
Muestra	974 sujetos estudiantes universitarios, de los cuales el 39% son hombres y 61% mujeres con una edad entre 18 y 24 años (Media 22 años).
Variable Dependiente	Cyberstalking, entendido como la suma de cinco formas de *online harassment:* contacto repetido no deseado, haber sido hostigado (*harassed)* repetidamente, recibir insinuaciones sexuales no deseadas, haber sido amenazado con violencia y el robo de identidad.

Variable Independiente	Exposición al delincuente motivado: • El tiempo pasado en Internet • Tipo de actividades realizadas: número de redes sociales, actualización de estado y la publicación de fotos en las redes sociales, el tiempo dedicado a las redes sociales, y el uso de mensajería instantánea Proximidad al delincuente motivado: • Agregar a extraños en las redes sociales, • Número total de amigos agregados a las redes sociales • Usar páginas web para buscar amigos Objetivo adecuado: información que se publican en las redes sociales (nombre completo, estado civil, orientación sexual, dirección postal, página web personal o blog, actividades, intereses, fotos y vídeos) Guardián capaz: • Privacidad de las cuentas de las redes sociales • Uso de programas que rastrean los usuarios que acceden a las cuentas de redes sociales. Comportamiento desviado (contacto no deseado, *harassment*, solicitud sexo, amenazar, *hacking*, descargas ilegales, enviar imágenes explicitas y recibir imágenes explicitas) Autocontrol
Análisis	Regresión logística binaria

También se ha tenido en cuenta el trabajo de Fawn T. Ngo y Paymond Paternoster, publicado también en la revista *International Journal of Cyber Criminology* en 2011, con el título *Cybercrime Victimization: An examination of Individual and Situacional level factors*. Los autores se centran en el análisis de la cibervictimización por la exposición no deseada a material pornográfico y la solicitudes no deseadas de sexo, como habían realizado otros autores previamente, y

añade como novedad, la conducta de difamación y la conducta de *harassment* distinguiendo cuando es realizada por un conocido o por un desconocido.

Tabla 6. Ficha técnica del estudio *Cybercrime Victimization: An examination of Individual and Situacional level factors* (Ngo y Paternoster, 2011)

Autores	Fawn T. Ngo y Raymond Paternoster (2011)
Muestra	295 universitarios (jóvenes y tercera edad)
Variable Dependiente	• Exposición no deseada a material pornográfico • Recibir solicitudes sexuales • *Harassment* realizado por desconocidos • *Harassment* realizado por conocidos • Difamación en línea[29]
Variable Independiente	Exposición al delincuente motivado: • Número de horas sumando las dedicadas al correo electrónico • Número de horas pasadas usando la mensajería instantánea • Número de horas usando salas de chat Objetivo adecuado: • Proporcionar información personal • Comunicación con extraños Guardián capaz: • Guardián físico: *software* de seguridad (antivirus, antiespía y cortafuegos)

[29] Los autores incluyen otras formas de victimización económica (*malware* y *phishing*) que no se incluyen en este punto por no formarte del objeto de análisis.

	• Guardián social: habilidad en el manejo de los equipos informáticos, y haberse formado sobre los riesgos de Internet asistiendo a cursos o autoformándose mediante páginas de Internet Comportamiento desviado (hacer o dar a otra persona *software*, música, películas o series de televisión piratas; acceder a los archivos o cuentas de otras personas sin previo permiso; agregar, borrar, cambiar o imprimir los archivos de otra persona sin permiso; y consumir pornografía)
Análisis	Regresión logística

Finalmente, contamos con el único estudio realizado hasta el momento con una muestra española, siguiendo la dinámica de los otros trabajo americanos, aunque añadiendo una visión distinta respecto a la construcción del objetivo adecuado. Nos referimos al trabajo elaborado por Fernando Miró Llinares, que lleva por título "*La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio",* y fue publicado en 2013 en la *Revista Española de Investigación Criminológica.*

Tabla 7. Ficha técnica del estudio La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio (Miró, 2013c)

Autor	Fernando Miró Llinares (2013c)
Muestra	500 participantes españoles de los cuales 222 (44,4%) son hombres y 278 (55,6%) mujeres, con una edad comprendida entre los 18 y 65 años (Media 40,21 años)
Variable Dependiente	*Online harassment*: • 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 • haber sido injuriado o haberse vertido acusaciones falsas sobre las personas
Variable Independiente	Incluye tres variables como objetivo adecuado: • Introducción: 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 • Interacción Personal: uso del correo electrónico, salas de chat, mensajería instantánea, redes sociales, foros, hacer videoconferencia, descargar archivos, consumir pornografía y jugar videojuegos online • Interacción con extraños: 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 • Autoprotección: 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
Análisis	Regresión logística

Una vez descritas sus características principales, procederemos a analizar los estudios realizados aplicando la TAC a la cibervictimización social, prestando especial atención tanto a cómo se han ido operativizando las distintas variables relacionadas con la aplicación al ciberespacio de la Teoría de las Actividades Cotidianas, como a los factores que, en los diferentes estudios analizados, han sido identificados como "de riesgo" para la victimización por las conductas establecidas como variables independientes.

2.2.2.1. Operativización de las variables

Al igual que sucede con la cibercriminalidad económica, los autores operativizan los constructos de la teoría de las actividades cotidianas de muy diferente forma, pero la gran mayoría tratan de definir variables a partir del desarrollo conceptual de cada uno de los tres elementos del triángulo del crimen: el delincuente potencial, que la mayoría de los autores identifica con la exposición al mismo; el objetivo adecuado y el guardián capaz.

Respecto a este último, el guardián capaz, Marcum (2008) lo identifica con la cantidad de supervisión experimentada por los

encuestados. Esto es, el lugar donde hacen uso de Internet (en estancias de la casa como el salón, la habitación, etc., en el colegio, en casa de amigos, *coffee shops*, etc.), y si tienen restricciones de uso de Internet y sistemas de control como los bloqueadores de software. Por su parte, Holt y Bossler (2009) hacen distinción 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 es el conjunto de amigos con comportamiento antisocial en Internet. Ngo y Paternoster (2011) también identifican el guardián físico con el software de seguridad (antivirus, antiespía y cortafuegos), pero el guardián social lo operativizan como la habilidad en el manejo de los equipos informáticos, y como haberse formado sobre los riesgos de Internet, bien asistiendo a cursos o bien autoformándose mediante páginas de Internet. Variables completamente distintas identifica Reyns (2010) como guardián capaz, al incluir la privacidad de las cuentas de las redes sociales y el uso de programas que rastrean los usuarios que acceden a las cuentas de ellas.

Respecto al constructo "exposición al delincuente motivado", Marcum (2008) considera que hay sitios en Internet que están más habitados por delincuentes motivados y que, por lo tanto, acceder a ellos puede aumentar el riesgo de convertirse en víctima de acoso sexual. Por eso, mide por un lado, las horas pasadas en Internet y las horas haciendo uso de las herramientas de comunicación que provee Internet (correo electrónico, mensajería instantánea, salas de chat y redes sociales) y, por otro lado, las actividades concretas que se suelen realizar con esas herramientas: buscar información, jugar, planificar viajes, comprar, socializar con otros y otras actividades. Holt y Bossler (2009), también han considerado incluir en su estudio las distintas

actividades que se pueden realizar en Internet (comprar, jugar, usar el correo electrónico, las redes sociales y chats). Pero además añaden la velocidad de conexión a Internet, si se comparte con otras personas el ordenador, las horas dedicadas a Internet por cuestiones laborales, escolares u ocio, la habilidad informática (a diferencia de lo que hacen en el otro estudio que lo incluyen como guardián personal) y el comportamiento desviado. Reyns (2010) también mide como "exposición al delincuente motivado" el tiempo pasado en Internet y el tipo de actividades realizadas: número de redes sociales, actualización de estado y la publicación de fotos en las redes sociales, el tiempo dedicado a las redes sociales y el uso de mensajería instantánea. Este autor añade un cuarto constructo, al que denomina "proximidad al delincuente motivado" y que tratamos en este punto por similitud con la argumentación realizada por Marcum (2008) cuando habla de "exposición al delincuente motivado". Y es que Reyns (2010) entiende que hay lugares en los que hay mayor presencia de agresores motivados. Lugares que, si se frecuentan, aumentan la probabilidad de ser victimizados. Así, añade como variables agregar a extraños en las redes sociales, el número total de amigos agregados a ellas, y hacer uso de páginas web para buscar amigos. Y finalmente, Ngo y Paternoster (2011) también incluyen como "exposición al delincuente motivado" el número de horas sumando las dedicadas al correo electrónico, el número de horas pasadas usando la mensajería instantánea, y el número de horas usando salas de chat.

Finalmente, respecto al "objetivo adecuado", Marcum (2008) lo conceptualiza 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. Reyns (2010) también lo operativiza a

partir de los distintos tipos de información que se publican en las redes sociales (nombre completo, estado civil, orientación sexual, dirección postal, página web personal o blog, actividades, intereses, fotos y vídeos). Ngo y Paternoster (2011), además de proporcionar información personal, lo identifican con la comunicación con extraños. Miró (2013c), por su parte, añade tres variables como características del objetivo adecuado. La primera de ellas, denominada "introducción", incluye guardar en el ordenador con el que se conectan a Internet información personal (un archivo con contraseñas, fotos personales, fotos íntimas, videos personales e información sensible de la empresas), usar datos personales reales para abrir perfiles de redes sociales, facilitar información personal a través de redes sociales y foros, y facilitar las contraseñas a otras personas. La segunda, denominada "interacción", en la que distingue "interacción personal" (que incluye el uso del correo electrónico, chat, mensajería instantánea, redes sociales, foros, consumir pornografía, hacer videoconferencias y jugar a videojuegos *online)* e "interacción con extraños" (usar webs de contacto, contactar con extraños a través de las redes sociales y la mensajería instantánea, y descargar archivos o abrir enlaces enviados por desconocidos al correo electrónico o a través de la mensajería instantánea). Y la tercera variable, denominada "no-autoprotección", incluye no tener antivirus, usar *software* pirata, usar la misma contraseña para todo, no cambiar sus contraseñas como mínimo una vez al año y tener los perfiles de las redes sociales abiertos para permitiendo que pueda acceder todos los usuarios a su información.

2.2.2.2. Factores de riesgo

Una vez analizados la manera en que los autores conceptualizan la TAC aplicadas a la cibervictimización social, procedemos a identificar los factores de riesgo detectados para cada una de las formas concretas de *cyberharassment* analizadas.

Respecto a la victimización por exposición no deseada a material sexual explícito, son varios los factores de riesgo encontrados. En este sentido, Marcum (2008) halló que lo que determina en mayor medida este tipo de victimización es comprar a través de Internet, pasar más horas en salas de chat, facilitar información personal a otras personas a través de Internet y tener más privilegios por parte de los padres. Sin embargo, advierte más adelante que los factores varían en función de la edad y el sexo de los sujetos (Marcum et al., 2010). Por otro lado, Ngo y Paternoster (2011) encontraron que las actividades que suponen un mayor riesgo para estar expuesto a material sexual no deseado son realizar comportamientos desviados en Internet (piratear *software* o películas, acceder a los archivos o cuentas de otras personas sin previo permiso, etc.) y haberse formado previamente sobre los riesgos de Internet.

En cuanto a la victimización consistente en recibir solicitudes de contacto sexual, los factores de riesgo asociados son 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 (Marcum, 2008). Sin embargo, éstos pueden variar dependiendo de la edad y el sexo de acuerdo con lo mostrado por Marcum et al. (2010): tanto para las chicas

como para los chicos estudiantes de último curso de secundaria, el factor que con mayor fuerza predice la victimización es el uso de chat, mientras que las restricciones impuestas por los padres minimiza los riesgos; y para los chicos universitarios, los factores de riesgo son el uso del correo electrónico y comunicarse con extraños; y para las chicas universitarias el uso de la mensajería y facilitar información personal.

El *harassment* es probablemente la forma de cibervictimización social que más se ha estudiado desde la perspectiva de las actividades cotidianas. Marcum (2008) encontró que los predictores para el *harassment* en población juvenil son: usar Internet para socializar, el número de horas a la semana dedicado al correo electrónico, proporcionar información personal, y querer tener éxito en la escuela. Holt y Bossler (2009), que realizaron el estudio con una muestra de universitarios, encontraron que resulta significativo el uso de las salas de chat, comportarse 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 (como, por ejemplo, acceder a los contextos específicos frecuentados por agresores). Reyns (2010), por su parte, también determinó que el comportamiento desviado aumenta el riesgo (si bien este comportamiento hace referencia a las distintas formas de acoso que se pueden realizar en el ciberespacio) y además añadió que los amigos también acosen a otras personas a través de Internet y admitir extraños en las redes sociales.

Ngo y Paternoster (2011) concluyeron que los factores de riesgo varían cuando el acoso es llevado a cabo por alguien conocido

por la víctima o no. En el primero de los casos, cuando el acosador es alguien conocido, los factores precipitantes son el uso de la mensajería instantánea y, especialmente, comportarse de manera desviada en Internet. En el segundo de los casos, cuando el autor del *harassment* es alguien no conocido por la víctima, hacer uso de *software* de seguridad y estar desempleado. Finalmente, Miró (2013c) encontró que los 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. Concretamente, aquellos sujetos que guardan información personal en los dispositivos con los que se conectan a Internet y facilitan información personal real a través de las distintas herramientas de comunicación que proporciona Internet tienen una probabilidad del 72,3% de ser victimizados. También que interactuar, tanto con personas conocidas como con desconocidos, aumenta la probabilidad en un 63,3% y un 55,04% respectivamente. Y también lo hace no autoprotegerse, es decir, no usar antivirus, no cambiar las contraseñas frecuentemente, usar la misma contraseña para todo y usar *software* pirata.

Por último, de acuerdo con los resultados de Reyns (2010), los factores de riesgo varían dependiendo de la conducta concreta de *harassment* que queremos predecir. Para el contacto repetido no deseado son el uso de las redes sociales, tener programas que rastrean los usuarios que acceden a las cuentas de redes sociales (aunque el propio autor advierte para este factor que puede haber un problema de temporalidad y no ser un factor de protección sino una consecuencia), acosar a otros a través de Internet (comportamiento desviado) y que también los amigos acosen a otros a través de Internet

(comportamiento desviado de los amigos). En el caso de la recepción de insinuaciones sexuales, se repiten los factores de hacer uso de programas que rastrean los usuarios que acceden a las cuentas de redes sociales, el comportamiento desviado de la víctima y el de los amigos; y como factor distinto, el número de publicaciones del estado en los perfiles de redes sociales. Para las amenazas encontró que son también factores de riesgo el comportamiento desviado y el uso de programas que rastrean los usuarios que acceden a las cuentas de redes sociales. Similares factores encuentra para el *cyberstalking:* mayor número de perfiles de redes sociales, el uso de la mensajería instantánea, admitir extraños en las redes sociales, comportamiento desviado de la víctima y el de los amigos. Y finalmente, los factores de riesgo asociados al robo de identidad son: admitir extraños como "amigos" en las redes sociales, usar páginas web de búsqueda de amigos y el comportamiento desviado de los amigos.

A continuación, se adjunta una tabla donde se recogen los resultados obtenidos de manera esquemática, como se ha realizado en apartados anteriores, con el fin de facilitar al lector la consulta de los mismos:

Tabla 8. Revisión de los factores de riesgo relacionados con la cibervictimización social

Referencia	Resultados	Predictores
Marcum (2008)	Prevalencia: -Recibir material sexual explicito 22,8%. - Harassment no sexual 30,8%. - Solicitud de sexo 9,6%. Modelos: M.1 para la exposición a material sexual: R^2N=,183 M. 2 para la *online harassment*: R^2N=,219 M. 3 para la solicitud de sexo: R^2N=,300	Exposición a material sexual: - comprar a través de Internet - horas en salas de chat - facilitar información personal - tener más privilegios por parte de los padres. Recibir solicitudes de contacto sexual: - usar Internet en lugares distintos al hogar - tener privilegios por parte de los padres para el uso de Internet Harassment: - usar Internet para socializar - número de horas a la semana dedicado al correo electrónico - proporcionar información personal - tener éxito en la escuela.
Holt y Bossler (2009)	Victimización harassment 18,9%. Modelo 1: R^2=,179 Modelo 2: R^2=,19	Harassment: - uso de las salas de chat - comportamiento desviado (concretamente *hacking*) - tener amigos que realizan también comportamientos desviados
Reyns (2010)	*Cyberstalking*: 40,8% - Contacto no deseado: 23,3% - Acecho: 20,1% - Contacto sexual no deseado: 13,9% - Amenaza con violencia: 4,4%	*Harassment*: - comportamiento desviado - tener amigos agresores - admitir extraños en las redes sociales Contacto repetido no deseado: - uso de las redes sociales

	- Fraude de identidad: 10,6%	- tener programas que rastrean los usuarios que acceden a las cuentas de redes sociales[30] - comportamiento desviado - tener amigos agresores Recepción de insinuaciones sexuales: - uso de programas que rastrean los usuarios que acceden a las cuentas de redes sociales - comportamiento desviado - tener amigos agresores - número de publicaciones del estado en los perfiles de redes sociales Amenazas: - comportamiento desviado - uso de programas que rastrean los usuarios que acceden a las cuentas de redes sociales. Cyberstalking: - mayor número de perfiles de redes sociales - uso de la mensajería instantánea - admitir extraños en las redes sociales - comportamiento desviado - amigos agresores Robo de identidad: - admitir extraños como "amigos" en las redes sociales - usar páginas web de búsqueda de amigos - tener amigos agresores

[30] El propio autor advierte para este factor que puede haber un problema de temporalidad y no ser un factor de protección sino una consecuencia.

Ngo y Paternoster (2011)	Prevalencias: - *harassment* extraños: 14,1% - *harassment* conocidos: 13,4% - exposición a material pornográfico: 20,9% - Solicitud de sexo: 14,7% - Difamación *online*: 7,6% Modelos: Modelo 1[31]: harassment extraños: R^2=0,13 harassment conocidos: R^2=0,256 material pornográfico: R^2=0,104 solicitud de sexo: R^2=0,089 difamación: R^2=0,145 Modelo 2: harassment extraños: R^2=0,19 harassment conocido: R^2=,0267 pornografía: R^2=0,207 solicitud de sexo R^2=0,197 difamación R^2=0,194	*Harassment* realizado por conocido: - uso de la mensajería instantánea - comportamiento desviado *Harassment* realizado por no conocido: - hacer uso de software de seguridad - estar desempleado Exposición a material pornográfico: - comportamiento desviados - formarse previamente sobre los riesgos de Internet Para la difamación *online* no se han encontrado factores de riesgo
Miró (2013c)	Prevalencia	*Harassment*:

[31] El autor realiza dos modelos para comprobar el efecto de las variables relativas a las actividades cotidianas. Así en el primero incluye las variables independientes autocontrol, sexo, edad, raza, empleado, situación civil (estar casado) y comportamiento desviado en la Red. En el segundo introduce las variable, además de las variables del modelo 1, las relativas a la exposición al delincuente, el objetivo adecuado y el guardián capaz.

	- Publicar información sin consentimiento: 10,2% - Contacto repetido no deseado 10% -Amenazas 3,2% - Suplantación de identidad 3,2% - Injurias 1,2% - Intimidar 1% Modelo: R^2 = 0,150	- Introducir más objetivos en el ciberespacio - Interaccionar con conocidos - Interaccionar con desconocido - No auto protegerse

3. Teoría de las actividades cotidianas y cibervictimización. Toma de posición y replanteamiento funcional de la teoría

3.1. Sentido funcional de la aplicación de la TAC a los estudios de victimización y elementos a medir

Como se ha puesto de manifiesto en el apartado anterior, todas los intentos de utilización del enfoque de la TAC al ciberespacio mediante métodos empíricos, se han realizado a través de encuestas de victimización. En todos los casos, se les ha preguntado directamente a las víctimas sobre su uso cotidiano de las TIC y ello se ha puesto en relación con las diferentes agresiones sufridas. Realizar el análisis desde la perspectiva de la víctima nos lleva a concluir que los factores de riesgo de la victimización, por lo menos en los evaluados desde este enfoque, son conductas que forman parte de la cotidianeidad de los usuarios (Miró, 2014c), y aunque también podría haberse construido las variables preguntando a las víctimas potenciales por elementos externos a ellas mismas, tales como las conductas de quienes les agreden o el comportamiento de quienes debieran haberles vigilado, eso, en todos los estudios analizados, no es así.

Cuando los diferentes autores han tratado de medir el constructo del "delincuente motivado" han tenido que reconceptualizar la variable como la "exposición al delincuente motivado" (Marcum, 2008; Ngo y Paternoster, 2011), o también como la "proximidad al delincuente motivado" (Reyns, 2010). En ambos casos

se hace referencia a conductas como visitar determinados lugares virtuales que están más frecuentados por agresores motivados, pero la operativización real de las variables se lleva a cabo teniendo en cuenta concretas acciones de comunicación llevadas a cabo por las propias víctimas. Así, en el primero de los casos, exposición al delincuente motivado, se identifica la misma como el número de horas pasadas en Internet, el uso de herramientas de comunicación (el correo electrónico, el chat, las redes sociales, mensajería instantánea, etc.), buscar información, jugar online, comprar, etc. Y en el segundo de los casos, proximidad al delincuente motivado, agregar mayor número de personas como 'amigos' a las cuentas de redes sociales, agregar extraños, y hacer uso de portales de búsquedas de amigos. Esto ha sido denominado por otros autores directamente como "uso cotidiano del ordenador" (Bossler y Holt, 2009; Pratt et al., 2010), pues en realidad están haciendo referencia a aquello que puede realizar un sujeto en el ciberespacio y especialmente, en referencia a sus acciones de comunicación.

Como conclusión, por tanto, puede decirse que existe un empeño, poco exitoso por otra parte, en identificar como características del "delincuente motivado" lo que, finalmente, no son más que elementos definitorios de la potencial adecuación de los objetivos a partir de su actuar cotidiano. Y lo mismo sucede cuando analizan el constructo del "guardián capaz", aunque en este caso consideramos que podría configurarse tal constructo separándolo claramente del elemento autoprotección.

Es generalizada la identificación, más bien confusión, del guardián capaz con la realización, por parte de la propia víctima, de

conductas de autoprotección. Esto se operativiza, en la mayoría de los casos, a través del uso por parte de las víctimas, de diferentes programas de protección de antivirus, antiespías, cortafuegos, etc. (Choi, 2008; Bossler y Holt, 2009; Holt y Bossler, 2009; Ngo y Paternoster, 2011) y en menor medida (aunque también desde la perspectiva de la víctima), de su habilidad con el manejo de los sistemas informáticos (Ngo y Paternoster, 2011). La excepción a esta regla general la constituye la operativización del guardián capaz a partir de la cantidad de supervisión experimentada en el caso de que los objetivos sean menores de edad (Marcum, 2008; Marcum et al., 2010). Realmente eso sí es guardián capaz: lo que se mide, aun preguntando a la propia víctima potencial, es la vigilancia que otros pueden estar ejerciendo sobre ella en aras de protegerla. Así, y salvo en este caso en el que realmente si se está valorando la incidencia de un tercero guardián con respecto al objetivo adecuado, la gran mayoría de los estudios lo que están haciendo realmente es dar relevancia a lo que hace la víctima en relación con su propia victimización, sin tener en cuenta otros factores externos.

Con esto lo que queremos poner de manifiesto es que el foco primario y esencial de los estudios de cibervictimización basados en el enfoque de la TAC se sitúa en la concreción de las características del objetivo adecuado, por mucho que haya un empeño, difícilmente comprensible en alguna ocasión, en incorporar al análisis todos los elementos del conocido "triángulo del crimen". Y decimos esto no porque no puedan operativizarse para un estudio criminológico determinado los constructos delincuente motivado o guardián capaz, ni siquiera porque no deba hacerse, sino porque no tendría que ser imprescindible hacerlo pero, en el caso de que se quiera, resulta

necesario operativizar bien las variables y definir de forma adecuada las hipótesis para no confundir lo que es objetivo adecuado, de lo que es guardián capaz. Trataremos de explicar estas reflexiones con mayor claridad aunque sea brevemente.

En primer lugar hay que decir que no se entiende el empeño en utilizar variables procedentes de los tres elementos básicos que conforman el delito en la Teoría de las Actividades Cotidianas, como si esa fuera la única forma posible de utilizar tal teoría a la hora de su relación con la victimización por cibercrimen. La teoría de las Actividades Cotidianas en particular, y las teorías del crimen en general, lo que ponen de manifiesto es que el entorno ecológico forma parte también del evento delictivo y lo condiciona, de modo que puede separarse para su análisis alguno de estos elementos en particular y tratar, a partir de él, determinar su relevancia como factor del crimen. Esto se ha hecho en múltiples estudios en los que se mide el factor lugar, y también en muchos otros en los que se mide el factor víctima tal y como puede y debe ser el caso de la gran parte de los estudios que hemos analizado. La relevancia del elemento guardián capaz, por ejemplo, se ha podido medir en interesantes estudios sobre la criminalidad en el espacio físico comparándose datos sobre delincuencia con información objetiva respecto a la vigilancia de lugares concreto, por ejemplo el uso de circuitos cerrados de televisión (Piza et al., 2013) o teniendo en cuenta el tiempo de vigilancia policial (Medina, 2013).

En segundo lugar, es importante comprender las limitaciones propias que tendrá la investigación derivadas del instrumento y la metodología que va a utilizarse para la misma. Si el instrumento

metodológico que va a utilizarse es una encuesta de victimización *ad hoc* que compare tal variable dependiente con las actividades cotidianas de los usuarios de Internet, siempre será más fácil centrarse en la identificación de las características del objetivo adecuado que en la determinación de las del agresor potencial, aunque no sería imposible hacerlo. Ello exigiría, como es lógico, obtener información relativa a aquél factor, y no únicamente obtener información relativa a la propia víctima. Lo que carece totalmente de sentido es empeñarse en pretender operativizar constructos como el del delincuente potencial y el del guardián capaz por medio de estudios victimológicos si se cuestiona a la víctima solo sobre lo que ella hace y sin obtener ningún tipo de información de lo que hacen los demás. Así, identificar como factor "delincuente potencial" variables que dependen de qué es lo que hace la víctima potencial en concreto, cómo se hace visible, accesible etc., supone, a nuestro humilde parecer, un error de planteamiento. Lo mismo sucede cuando se denomina guardián capaz a los sistemas antivirus que no controlan nada sino que son sistemas que tienen que ser incorporados y utilizados por la víctima y que la hacen más o menos accesibles al ataque potencial en Internet. Resulta esencial admitir, por tanto, que lo que hacen la gran mayoría de los estudios revisados, por mucho que digan a veces que hacen más, es tratar de identificar el elemento objetivo adecuado o, más concretamente, plantearse cuáles son aquellas particularidades o características que hacen a los usuarios o sus bienes, ser objetivos "adecuados" para un agresor potencial.

Pero que no se haya hecho no significa que no pueda hacerse. Que los estudios que hayamos analizado, y con la mera excepción de uno de los factores por parte de Marcum (2008), no hayan tenido en

cuenta otras variables derivadas del constructo guardián capaz, no implica que sea imposible hacerlo. Puede hacerse, pero es importante concretar bien qué pertenece al objetivo adecuado y qué al guardián capaz.

En nuestra opinión, y frente a las construcciones no coherentes con los elementos de la TAC que hemos visto anteriormente, acierta Miró (2011) cuando en sus estudios de victimización económica y social identifica como elementos de auto-protección factores como no usar la mismas contraseña para todo, cambiarlas con frecuencia o usar antivirus. Lo que sucede es que es discutible que estos factores se relacionen efectivamente con la cibercriminalidad social. Tiene todo el sentido considerar como elementos de autoprotección para la no victimización económica el uso de antivirus, hacer una gestión correcta de las contraseñas, no usar software pirata, limitar el acceso a los perfiles de las redes sociales, etc. Pero asiste razón en este sentido a Holt y Bossler (2009) cuando señalan que tales sistemas de protección no están pensados para este tipo de cibercriminalidad, sino para la de tipo económico, especialmente, aquellas conductas que tienen que ver con los ataques a los sistemas informáticos. Por tanto, la autoprotección puede ser una característica, similar a la accesibilidad en el espacio físico, de interés para la configuración de los caracteres del objetivo adecuado, pero parece tener más sentido en la cibercriminalidad económica que en la que nos ocupa.

Y, en cambio, en la cibercriminalidad que nos ocupa puede tener muchísima importancia la vigilancia de los guardianes capaces, especialmente de los padres, hermanos y amigos que pueden formar parte de las relaciones sociales a través de Internet y, así, observar la

intercomunicación personal de la potencial víctima con terceros. Si lo que nos ocupa en este caso son las conductas que se producen por el uso social de las TIC, puede ser del máximo interés analizar las pautas de cotidianeidad que suponen con quién se relaciona el potencial objetivo en Internet y, a partir de ahí, quién puede constituir un vigilante o guardián potencialmente capaz para evitar que sobre aquél se cometan actos delictivos.

La pregunta, entonces, es si se puede, por medio de una encuesta de victimización, obtener información sobre la vigilancia potencial que pueden estar ejerciendo personas distintas a la propia víctima sobre su actuar cotidiano en Internet. Y la respuesta es sí, aunque probablemente no toda la información deseable. No se podrá saber toda aquella información que esté fuera del alcance del encuestado como víctima potencial, pero sí aquella que él tenga. Así, la víctima potencial puede informarnos de si su sistema informático es utilizado por ella misma o por más personas, si en sus redes sociales están agregados sus parientes o si estos le controlan de algún modo el uso que ésta hace del ciberespacio. Esa es información que podemos obtener del propio encuestado, son datos relativos a su propia cotidianeidad, pero no es información referida a la adecuación del objetivo, sino a la potencial vigilancia sobre el mismo que pueden ejercer otros.

También sería posible obtener información sobre los caracteres del agresor potencial preguntando a la víctima con quién se relaciona y demás. Sin embargo, además de que parece más complicado operativizar tal constructo, el principal objetivo de este trabajo es obtener información sobre qué hace la propia víctima que le convierte

en especialmente adecuado para ser objeto de un cibercrimen social en aras de definir adecuadas estrategias preventivas, y eso concuerda mucho más con la definición, a partir de la información de la propia víctima, de los caracteres del objetivo adecuado y de parte de la información relativa al guardián capaz, que a la definición del agresor potencial.

Creemos, pues, que debe centrarse el análisis de la TAC aplicada a la cibercriminalidad social y realizada por medio de encuestas de victimización, primero en el elemento objetivo adecuado, esencial a la hora de configurar las variables de la cibervictimización, pero también en el elemento guardián capaz, utilizando la información que nos de la propia víctima respecto a su actuar cotidiano en relación con familiares que nos aporten datos sobre la vigilancia potencial que éstos pueden ejercer.

3.2. TAC y características del objetivo adecuado en el ciberespacio

Cuando Cohen y Felson (1979) determinaron las características que hacían adecuado a un objetivo, lo hicieron atendiendo a unas concretas formas de delincuencia con unas determinadas características de tipo espacio-temporal. Lo hicieron concretamente pensando en delitos perpetrados en el espacio físico y más específicamente en crímenes de tipo predatorio. Dadas las evidentes diferencias encontradas en la configuración del espacio virtual respecto al espacio físico, como así se ha puesto de manifiesto en apartados anteriores, cabe plantearse si también cambian las propiedades que

hacen adecuado al objetivo en el nuevo lugar. Se trata de revisar la validez de los caracteres tradicionalmente asociados al "objetivo adecuado". Teniendo en cuenta, además, que las características del objetivo dependerán básicamente del tipo de cibercrimen de que se trate, pues no todos los ciberdelitos persiguen el mismo tipo de objetivo.

3.2.1. Aplicación del VIVA al ciberespacio

¿Son también el valor, la inercia, la visibilidad y la accesibilidad lo que hace que un objetivo sea adecuado en el ciberespacio? Antes de responder nosotros a esta pregunta se procederá a realizar una sintética revisión de cómo lo han hecho otros autores que han tratado de definir los caracteres del objetivo adecuado en Internet.

El primero de los autores que se planteó la cuestión fue Majid Yar (2005) como fórmula para determinar si la cibercriminalidad es distinta a la criminalidad cometida en el espacio físico, si bien después otros autores como Miró (2011) y Yucedal (2010) han tratado también el tema con opiniones divergentes de las de Yar (2005). En lugar de analizar de forma vertical los argumentos de cada uno de ellos, procederemos a entremezclarlos en un análisis que parta de cada uno de los caracteres que conforman el famoso VIVA de Felson (1998).

Respecto a la primera cualidad, el valor del objetivo, Yar (2005) considera que también se reproduce en el ciberespacio y, además, se da con la misma complejidad que en el espacio físico. Hay que tener en cuenta que las cuatro propiedades (recogidas en el acrónimo VIVA)

son elaboradas desde la perspectiva del delincuente y, por tanto, cuando se habla del valor del objetivo, éste debe ser calculado desde la perspectiva del quien quiere cometer el delito (Felson, 1998). Esto hace que el cálculo del valor sea algo complicado, pues además del hecho de que el valor de un objeto puede depender de cuestiones culturales o económicas cambiantes como la moda, también dependerá del fin que tenga el delincuente con la obtención del objetivo. Un agresor puede apropiarse un objeto para su disfrute personal, pero también puede obtenerlo con la idea de realizar otro hecho delictivo, para realizar una actividad ilícita o para su posterior venta, entre otras múltiples opciones. En el ciberespacio también ocurre que una acción delictiva contra un objetivo puede tener distintos fines que afectarán al cálculo del valor, como el envío de *malware* que, en algunos casos, se realiza con el propósito de obtener unos datos con los que después se pueda realizar ciberfraude o por obtener notoriedad. A esto hay que sumar que, además, existen muchos tipos de objetivos en el ciberespacio, desde un sistema informático a una persona en concreto que puede ser víctima de *cyberstalking* o un grupo de personas que pueden ser objeto de victimización por cuestiones sexuales, étnicas, religiosas, etc.

Miró (2011), por su parte, considera, al igual que Yar (2005) que el elemento valor determina la adecuación de un objetivo. Argumenta, que en el ciberespacio las cosas de poco valor por sí mismo puede adquirir gran valor gracias a la facilidad para obtener la información, relacionarla y convertirla en un objetivo de riesgo. Una contraseña compuesta por cuatro dígitos que a priori pueden no tener valor, puede dar acceso a una cuenta bancaria y por lo tanto, tales número puede acabar teniendo un gran valor. Pero independientemente de

ello, el valor vendrá determinado por la finalidad del delincuente para obtener el objetivo. Por lo tanto, ambos autores se ponen de acuerdo (aunque con argumentos ligeramente distintos) en afirmar que el valor es una cualidad que debe ser tenida en cuenta para determinar la adecuación de un objetivo en el ciberespacio.

En cambio, respecto a la segunda cualidad, la inercia, parece existir consenso en que no puede ser trasladado al ciberespacio para determinar la adecuación de un objetivo. Cuando Felson (1998) habla de *inertia* (inercia) lo hace refiriéndose al tamaño, peso y forma, esto es, los aspectos físicos de la persona o el bien, que funcionan como obstáculos o impedimento para que el delincuente lo vea como adecuado. Cuanto más grande y pesado sea el objeto, mayor dificultad tendrá el delincuente para hacerse con él y, por consiguiente, menor será la idoneidad del objetivo. De acuerdo con Yar (2005), la operativización de esta propiedad al espacio virtual parece más complicado, pues en términos de volumen y masa, los objetivos en el ciberespacio son informacionales y podrán ser más o menos pesados pero no se pueden equiparar a las propiedades físicas de los objetivos o victimas del espacio físico. Aun así, considera Yar (2005) que los objetivos informáticos conservan, en cierto grado, las propiedades de inercia. Por un lado, el volumen de los datos afectará a la portabilidad del objetivo. Los documentos que tiene mayor tamaño presentan mayores dificultades para ser descargados. Lo que conlleva, por otro lado, al uso de sistemas informáticos con mayor capacidad. El tipo de herramientas que use el agresor pondrá límites a la apropiación de grandes objetivos informacionales. En definitiva, "aunque los objetivos informacionales ofrecen poca resistencia inercial, su 'ingravidez' no es absoluta" (Yar, 2005; p. 420).

En cambio, Miró (2011) y Yucedal (2010) discrepan con Yar (2005) al afirmar que, salvo casos excepcionales, los bienes en el ciberespacio no se diferencia entre sí por sus mayores o menores condiciones intrínsecas. Borrar, reproducir o alterar la información en el ciberespacio no tiene costes (Geer, 2007; Yucedal, 2010), y puede ser obtenida por muchos individuos como es el caso de la piratería digital (Grabosky, 2001). En cualquier caso, llegan a la misma conclusión: la inercia tampoco sería una de las características que conformaran la idoneidad del objetivo.

La tercera cualidad, la visibilidad, es la exposición de los objetivos a los delincuentes (Felson, 1998). Los delincuente deben saber de la existencia del objetivo y cuanto más visibles sean mayor será la probabilidad de convertirse en blancos. Considera Yar (2005) que Internet facilita la comunicación y la interacción y que, por lo tanto, la visibilidad es una característica presente. Salvo excepción de las "intranet" que son entidades virtuales privadas que restringen el acceso, Internet es un medio inherentemente público donde todos los usuarios son visibles. La gran diferencia con respecto al espacio físico, es que ya no existen las barrera de la distancia física, y que por lo tanto, todos los usuarios pasan a estar visibles para los agresores motivados.

Frente a esto, apunta Miró (2011), que el hecho de que desaparezcan las barreras de las distancias físicas acercando a todos los usuarios a un mismo lugar y del carácter público del ciberespacio, no hace que todos los objetivos sean visibles como propone Yar (2005), sino que lo son cuando interaccionan con otros sujetos y otros servicios. El ciberespacio es tan ingente y universal, que es difícil hacerse visible pues todos los usuarios conforman la red en la que hace

difícil distinguir unos de otros. Para convertirse en un sujeto visible, es necesario interaccionar, esto es realizar comunicaciones en el ciberespacio con otras personas a través de las distintas herramientas existentes, comprar, visitar páginas web, etc.

La cuarta y última cualidad, la accesibilidad, es referida al diseño del lugar y la ubicación del objeto que aumenta el riesgo de ataque o lo facilita. Felson (1998) se refiere a la "capacidad de un delincuente para llegar al objetivo y luego escapar de la escena del crimen" (p. 58). A mayor accesibilidad del objetivo, mayor será su idoneidad y viceversa. Considera Yar (2005), que a diferencia de lo que ocurre en el espacio físico donde las diferentes rutas para llegar al objetivo sí modifican las probabilidades de ser atacadas (Beavon et al., 1994), en el ciberespacio es posible ir de un punto a otro (dado que el recorrido no es lineal), dificultando así la consideración de la accesibilidad como una propiedad del objetivo que aumenta o disminuye la probabilidad de que sea atacado. Y cuando se analiza la accesibilidad en términos de huida de la escena del crimen, también cambia en el ciberespacio. Ya que la posibilidad de alejarse de la escena del crimen puede resultar tan sencillo como desconectarse de la Red. Esto no implica, como señala Yar (2005) que el delincuente no pueda ser observado durante la comisión del delito, y luego se rastree su posición mediante diferentes técnicas. Aunque el rastreo también puede ser eludido haciendo uso de herramientas tales como dispositivos de cifrado, o con la utilización de sistemas informáticos de terceros. Según el autor, la única dimensión de la accesibilidad donde puede ser compatible con la operativización dada en el espacio físico, es mediante el uso de sistemas que impiden el acceso no autorizado. Es decir, que se requieran contraseñas o medidas de autenticación para acceder al

objetivo. Pero, de nuevo, estas barreras pueden ser superadas con distintas herramientas.

Planteamiento muy distinto es el de Miró (2011) al considerar que, dada la contracción de la distancia en el ciberespacio, todos los objetivos son potencialmente igual de accesibles. Y que si se tiene en cuenta que esta característica está asociada a las capacidades del agresor, en vez de a las particularidades del objetivo, pues se trata de la habilidad del agresor para contactar con un objetivo y llevárselo de la escena del crimen, entonces la accesibilidad no será condicionante de la educación de un objetivo.

Por tanto, a la pregunta ¿son también el valor, la inercia, la visibilidad y la accesibilidad lo que hace que un objetivo sea adecuado en el ciberespacio? la respuesta parece ser negativa. Los elementos no pueden ser directamente trasladados al ciberespacio, es necesario una reformulación de los mismos o la propuesta de nuevos. Para Yar (2005), de las cuatro características que hacen a un objetivo adecuado en el ciberespacio, sólo el valor es la única que quedaría de igual forma en el ciberespacio. El resto son, según su opinión, propiedades que difícilmente pueden ser trasladadas debido a la configuración del nuevo lugar de actuación criminal.

Miró (2011), por su parte, considera que el valor podría mantenerse como elemento necesario para la adecuación del objetivo, si bien debería diferenciarse según el ciberdelito. Y la visibilidad también, pero reconceptualizado en la interacción, pues lo que hace visible a un objetivo a ojos de un delincuente potencial (que sea identificable) es su movimiento a través del ciberespacio. En cambio, eliminaría de la ecuación las características de inercia y accesibilidad.

Así, propone el autor un cambio de acrónimo del VIVA al IVI, manteniendo el valor del objetivo y añadiendo "introducción" e "interacción" como elementos de adecuación del objetivo adecuado al ciberespacio.

Cuando habla de "introducción", hace referencia a la acción de trasladar voluntaria, o involuntariamente, bienes del espacio físico al ciberespacio. Explica, en este sentido, que en el espacio físico hay algunos tipos de bienes que la persona puede llevar consigo, como los de tipo económico (por ejemplo, dinero). Pero hay otros bienes personalísimos de los que la persona no se puede deshacer, como la libertad, el honor, la dignidad, la salud, etc. En cambio, esto no sucede en el espacio virtual porque al ciberespacio hay que entrar (a diferencia de lo que ocurre en el espacio físico donde simplemente se está), y al hacerlo se podrá decidir aquellos bienes que pueden estar disponibles en el ciberespacio.

Esta distinción se muestra claramente a través de las siguientes ilustraciones. Así, se puede observar en la primera como el agresor con intención delictiva puede atacar a los bienes que lleva la persona (libertad sexual, patrimonio, salud, intimidad, honor, etc.). En cambio en el ciberespacio, como se muestra en la segunda ilustración, el agresor que tenga intención de llevar a cabo un ataque solo lo podrá hacer sobre los bienes que hayan sido introducidos previamente en el ciberespacio. De esta forma, solo se podrá afectar al patrimonio cuando esté presente en el ciberespacio, por ejemplo, cuando un usuario tenga banca online o haga uso de su tarjeta de crédito insertando su número para realizar una compra. Lo mismo sucede con la intimidad o privacidad, que se podrá afectar cuando un usuario publique fotos

personales porque pasan a estar disponibles para otras personas en el ciberespacio.

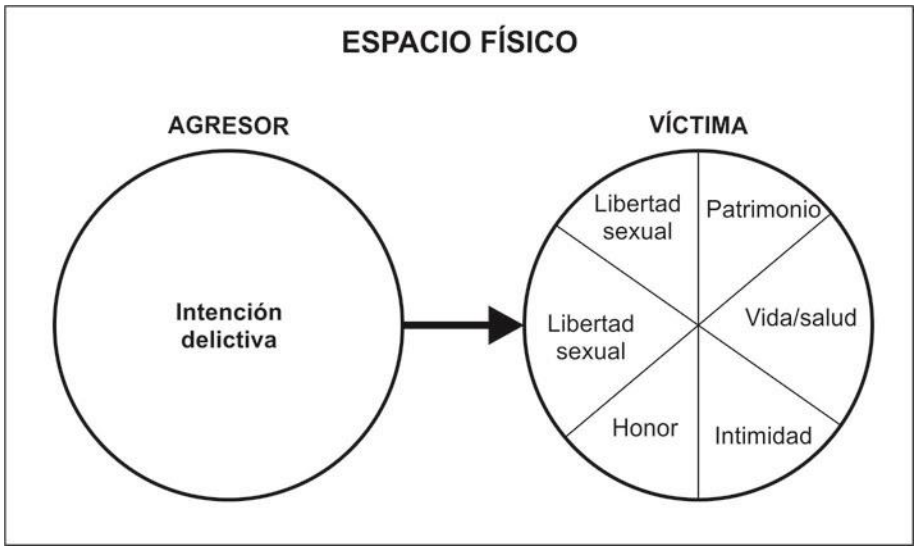


Ilustración 4. Representación del contacto en el espacio físico entre un agresor motivado y una víctima. Obtenido de Miró (2011, p.27)

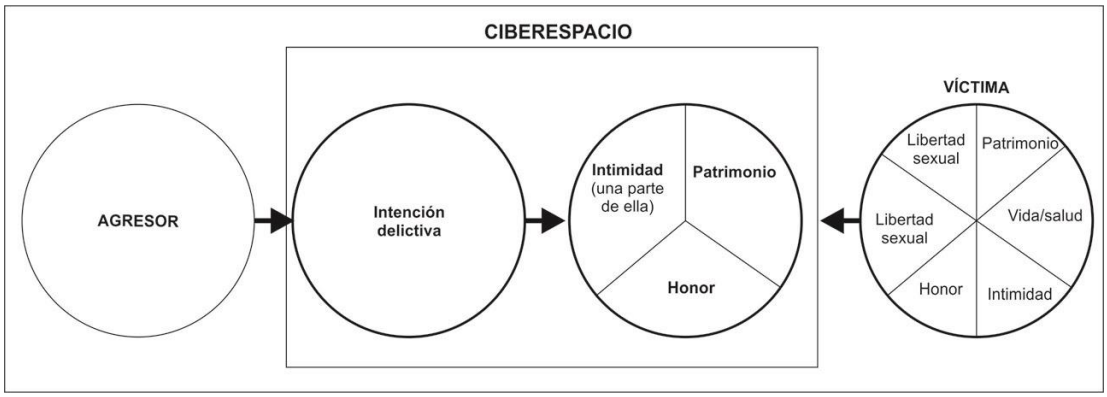


Ilustración 5. Representación del contacto en el ciberespacio entre un agresor motivado y una víctima. Obtenido de Miró (2011; p. 28)

Pero no basta con la introducción de los bienes en el ciberespacio para que puedan considerarse objetivos adecuados. Es necesario que se hagan visibles al agresor para que puedan ser atacados. Dice Miró (2011) en este sentido, que es complicado hacerse visible en el ciberespacio porque "todos los usuarios conforman una maraña en la que es difícil distinguir a unos y otros" (p. 31). A diferencia de lo que opina Yar (2005) de que el ciberespacio es de carácter público y, por lo tanto, todos los objetivos son en sí visibles a nivel mundial, es lo que hace que todos puedan pasar desapercibidos para los agresores (Miró, 2013c). Tanto para los delitos de carácter económico como los de carácter social, la probabilidad de que un usuario sea víctima dependerá de su interacción. Cuanto más interactúe mayor será la probabilidad de convertirse en víctima. Esta interacción la identifica con la frecuencia y el tiempo de acceso a Internet, actividades que conllevan la divulgación de datos personales, visitar determinadas webs, descargarse programas, realizar todo tipo de acciones de compra, etc. Así, de manera gráfica, muestra como un sujeto se mueve por el ciberespacio realizando este tipo de actividades, y convirtiéndose así en un sujeto visible.

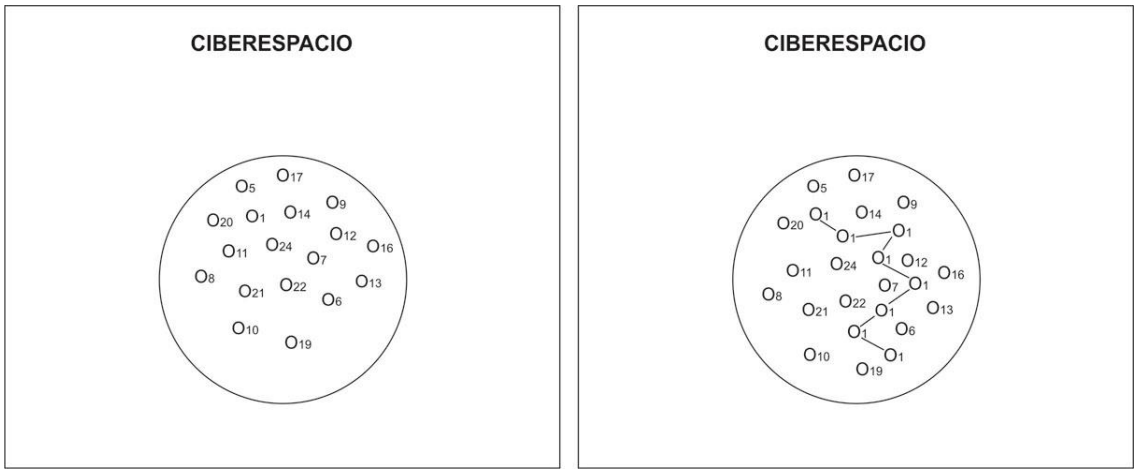


Ilustración 6. Interacción en el ciberespacio de un usuario. Obtenido de Miró (2011; p. 32)

En resumen, entiende Miró (2011), que si objetivo ha sido introducido en el ciberespacio, es visible debido a su interacción, y tiene valor, es un objetivo adecuado para ser atacado por un potencial agresor.

3.2.2. Recapitulación

Los desarrollos teóricos en relación a los elementos que hacen a un objetivo adecuado al ciberespacio, ponen de manifiesto que el VIVA, tal y como originariamente lo formularon Cohen y Felson (1979), no puede ser trasladado al ciberespacio, pero puede constituir una magnífica referencia para tratar de identificar las características del ciberobjetivo adecuado. Será necesario, para ello, encontrar otros caracteres, o cuanto menos, reformular los originales para adaptarlos al nuevo espacio. Esto es así, porque el espacio virtual es diferente al espacio físico. Y al cambiar el lugar, sigue siendo necesario que

converjan un agresor potencial y un objetivo adecuado en ausencia de un guardián capaz, pero la manera de relacionarse entre ellos cambia. Al hacerlo, también cambian las características que hacen a un objetivo ser adecuado. Esto ha llevado a la creación de otras fórmulas como la propuesta por Miró (2011), en la que sustituye tres de los cuatro elementos iniciales por dos nuevos: inercia, visibilidad y accesibilidad por interacción e introducción.

Tanto Yar (2005) como Miró (2011) consideran que el valor del objetivo modula su adecuación. Sin embargo, el valor va a depender del tipo de criminalidad de que se trate y, en particular, del interés pretendido por el agresor (Felson, 1998). Como así ha señalado Miró (2011), habrán determinados objetivos que aparentemente tengan poco valor, como una cifra con cuatro dígitos, pero en realidad tiene un alto valor económico porque son la clave de acceso a una cuenta bancaria *online*. Pero como ya se ha comentado, el valor dependerá del tipo de cibercriminalidad, y la que ocupa este trabajo son formas concretas de ciberacoso a menores, cuya finalidad suele ser dañar, humillar, etc. En realidad, sobre el valor poco puede hacer la víctima para cambiarlo, una vez que ha sido introducido en el ciberespacio por ésta. Por ejemplo, un *hacker* puede lanzar un *malware* con el objetivo de acceder a un sistema informático para, o bien obtener unos datos económicos de la víctima y, por tanto, el cálculo del valor del objetivo responderá a una finalidad económica; o bien, para acceder al ordenador y realizar una acción en la que la víctima sienta que está siendo acosada, por lo que el cálculo del valor dependerá de la intencionalidad que tenga el agresor. En cualquier caso, el ataque se realiza sobre el sistema informático que la víctima ha puesto a disposición de otros agresores. Pero, para la víctima, el valor del

objetivo (en este caso el sistema informático) será el mismo, independientemente de la finalidad del agresor. Por tanto, la víctima no puede hacer nada para cambiar el valor del objetivo, pues dependerá de lo que el agresor pretenda con su ataque.

En definitiva, la víctima podrá introducir el objetivo en el ciberespacio haciendo que esté disponible para un potencial agresor, lo podrá hacer más visible en función de su interacción, y, dependiendo del cibercrimen de que se trate, lo podrá proteger más o menos para evitar el ataque, pero poco podrá hacer sobre el valor que dependerá, completamente, del interés real del potencial agresor.

4. Interacción e introducción como factores de adecuación del objetivo en el ciberespacio y vigilancia familiar como concreción del elemento guardián capaz

Desde un punto de vista teórico, a la pregunta ¿qué es entonces lo que hace a un objetivo ser 'adecuado' en el ciberespacio?, la posible respuesta podría ser que un objetivo es adecuado cuando ha sido introducido en el ciberespacio y, por tanto, está disponible para el agresor y se ha hecho visible para éste gracias a la interacción. A esto podría añadirse la respuesta y es accesible, en el sentido de que esté suficientemente protegido por la propia víctima. Desarrollaremos a continuación estos argumentos por medio de una aproximación

teórica a las propiedades que hacen a un objetivo adecuado para la comisión del delito, apoyándonos para ello, además, en una revisión y ordenación de los factores de riesgo y de protección encontrados hasta el momento por la comunidad científica.

Introducción

Existen claras diferencias entre el contacto que se produce entre las personas en el espacio físico con respecto al contacto en el espacio virtual. Mientras que en el espacio real las personas generalmente se comunican de manera física y directa, en el ciberespacio las personas físicas no se comunican directamente, sino que lo hacen a través de una representación de ellas mismas (Miró, 2011). Esta representación virtual de las personas físicas vendrá determinada por la imagen que construyan de ellos mismos a través de diferentes acciones de comunicación. Algunas de estas acciones podrían ser usar las redes sociales, y otros canales de comunicación, para verter pensamientos e ideas que invitan a la respuesta de otras personas (Mitchell, Wolak, Finkelhor, 2008); o publicar imágenes, vídeos o todo tipo de información personal, como hacen especialmente los jóvenes (Casas et al., 2013). Esta forma de introducción de bienes personales en el ciberespacio, así como otros de carácter económico, va a ser clave para la adecuación de un objetivo en el ciberespacio, en tanto que los ponen a disposición de agresores potenciales.

Diferentes autores han demostrado, a través de estudios empíricos, como realizar diferentes acciones de introducción de bienes en el ciberespacio, favorecen la victimización. En este sentido, la cesión

voluntaria de información personal real a través de diferentes canales (como las redes sociales, foros, blogs, mensajería instantánea, etc.) incide en el proceso de cibervictimización, especialmente en el caso del ciberacoso (Marcum, 2008; Marcum et al., 2010; Miró, 2013c; Patchin y Hinduja, 2010; Reyns, 2010). Facilitar información personal a otras personas puede aumentar la probabilidad de sufrir un ataque de *harassment* en un 73% como apunta Miró (2013c). También supone un riesgo, como ha señalado Reyns (2010) para el *cyberstalking*, cambiar el "estado" los perfiles de las redes sociales y publicar todo información personal como el nombre completo, fotos de sí mismo[32], el estado civil, la orientación sexual, la dirección de correo, intereses o aficiones. Otros factores de riesgo destacados por la comunidad científica son abrir las cuentas de las redes sociales usando datos personales reales (Miró, 2013c) y facilitar las contraseñas a otras personas a través de diferentes medios electrónicos (Sengupta y Chaudhuri, 2011; Patchin y Hinduja, 2010; Mishna et al., 2012).

Asimismo, sucede que, en ocasiones, acceder o introducir bienes en el ciberespacio no responde a una decisión voluntaria. Habrá situaciones en que serán terceros los que introduzcan nuestra imagen, nuestra vida privada, etc. Otras en cambio, serán acciones involuntarias de los usuarios las que lo hagan (Miró, 2011). Muchas personas no son conscientes de que cuando se accede con el ordenador, la *tablet* o el *smartphone* al ciberespacio, toda la información contenida en ellos pasa a estar disponible para los agresores motivados. Mediante el

[32] Similares resultados obtienen Sengupta y Chaudhuri (2011) al señalar que publicar fotos es un factor de riesgo y también publicar el colegio en el que se estudia y el número de teléfono.

envío de *malware* se puede acceder a nuestra información y copiarla, borrarla, etc. Si tenemos un archivo con nuestras contraseñas se puede hacer uso de ellas para realizar cualquier tipo de ciberataque económico. También, si tenemos fotos personales o en situación comprometida, pueden ser utilizadas posteriormente para dañar nuestra imagen, el honor, la dignidad, etc[33]. Este hecho ha sido comprobado recientemente en un estudio empírico: el guardar información personal en los dispositivos con los que se conecta a Internet como un archivo con contraseñas, fotos personales, fotos íntimas e información sensible de la empresa, aumenta el riesgo de ser víctima de *harassment* (Miró, 2013c). Pese a que ello no siempre depende del usuario, en la mayoría de las ocasiones es su actividad en el ciberespacio, y las rutinas que tenga, las que determinaran en gran medida que el sujeto se convierta en víctima en el mismo.

Interacción

Son múltiples las formas de interacción que hacen a un sujeto visible en el ciberespacio. Se ha demostrado empíricamente que a mayor uso de Internet, es decir, mayor número de horas pasadas en Internet, mayor es la probabilidad de convertirse en víctima en el ciberespacio (Beckman et al., 2013; Casas et al., 2013; Didden et al.,

[33] Son muchos los famosos a los que han hackeado sus teléfonos móviles para hacerse con fotos comprometidas. El 15 de septiembre de 2011 el elpais.com publicaba que Scarlett Johansson había sufrido un ataque de este tipo. Unos hackers habían entrado en su teléfono y se habían hecho con fotos de desnudos y en situación comprometida http://elpais.com/elpais/2011/09/15/actualidad/1316069330_850215.html

2009; Juvonen y Gross, 2007; Misha et al, 2012; Wolak, Mitchell y Finkelhor, 2007; Ybarra y Mitchell, 2004a).

Otras de las formas que permite hacerse visible a un usuario en Internet es utilizando las diferentes herramientas que éste proporciona para la comunicación. Los estudios han confirmado que haciendo uso de ellas se aumenta el riesgo de sufrir ataques. Entre las herramientas que aumentan el riesgo de victimización se encuentran: el correo electrónico (Marcum, 2008; Ybarra y Mitchell, 2004a), las salas de chat (Holt y Bossler, 2009; Marcum, 2008; Sengupta y Chaudhuri, 2011; Ybarra y Mitchell, 2004a), los foros (Miró, 2014c), los blogs (Miró, 2014c; Mitchell, Wolak y Finkelhor, 2008), las videoconferencias (Juvonen y Gross, 2007; Miró, 2014c), la mensajería instantánea (Miró, 2014c; Ngo y Paternoster, 2011; Sengupta y Chaudhuri, 2011) y las redes sociales (Reyns, 2010; Sengupta y Chaudhuri, 2011).

Pero también son otras las actividades de interacción que se pueden realizar en el ciberespacio y que se relacionan con la cibervictimización. Entre ellas se destaca el uso de la banca electrónica (Hutchings y Hayes, 2009), realizar compras por Internet (Marcum, 2008; Miró, 2014c; Ngo y Paternóster, 2011; Pratt, Holtfreter y Reisig, 2010; Wilsem, 2011), descargar videojuegos, música y películas (Choi, 2008; Miró, 2014c; Miró, 2013c; Reyns et al., 2011). Y también abrir archivos adjuntos, o enlaces recibidos por correo electrónico, o mensajería instantánea (Choi, 2008), lo que se muestra especialmente peligroso en relación con la cibercriminalidad económica.

El ciberespacio se ha convertido en un medio poderoso para la comunicación entre las personas. Hacer uso de las distintas herramientas para socializar también es una actividad que hace visible

a un usuario, y por tanto aumenta su probabilidad de riesgo (Marcum, 2008). Pero si hay algo que se ha demostrado que es especialmente peligroso, tanto en relación con la cibercriminalidad económica como la social, es contactar con personas conocidas a través de Internet (Marcum et al., 2010; Misha et al., 2012; Mitchell, Wolak y Finkelhor, 2008; Sengupta y Chaudhuri, 2011; Vandebosch y Van Cleemput, 2009). Especialmente en los casos en los que la víctima desconoce la identidad del agresor (Wolak, Mitchell y Finkelhor, 2007). Abrir enlaces o archivos adjuntos enviados por desconocidos a correo electrónico, o por mensajería instantánea, supone un riesgo (Ngo y Paternoster, 2011) y también agregar a extraños como 'amigos' en las redes sociales (Reyns, 2012). El contactar con desconocidos puede ofrecer oportunidad a los agresores de acceder a potenciales objetivos. Y son los propias usuarios los que se están haciendo visibles para los agresores.

Finalmente, otra forma de interacción a través de la Red es comunicarse con otras personas para realizar agresiones, lo que algunos autores han venido a llamar "comportamiento desviado". Contactar con alguien en repetidas ocasiones cuando le han pedido que pare, acosar o molestar a alguien por Internet, solicitar sexo a alguien que no quiere, amenazar por Internet y enviar imágenes de contenido sexual aumenta la probabilidad de ser víctima (Reyns et al., 2011). En otras palabras, hacer uso de Internet para acosar a otras personas aumenta significativamente las probabilidad de ser víctimas en un futuro (Wolak, Mitchell y Finkelhor, 2007; Vandebosch y Van Cleemput, 2009). Y no sólo el comportamiento desviado contra personas, también los relacionados con la piratería y *hacking*. Entre estas actividades se destaca: hacer o dar a otra persona *software,* música, películas o series de televisión piratas; acceder a los archivos o

cuentas de otras personas sin previo permiso; agregar, borrar, cambiar o imprimir los archivos de otra persona sin permiso; (Bossler y Holt, 2009; Holt y Bossler, 2009; Ngo y Paternoster, 2011) y consumir pornografía o material obsceno *online* (Bossler y Holt, 2009; Holt y Bossler, 2009; Miró, 2014c; Ngo y Paternoster, 2011).

En resumen, hacer uso de todas las herramientas que proporciona Internet (chats, correo electrónico, mensajería instantánea, blogs, foros…) comprar, descargar archivos, contactar con extraños, realizar comportamientos desviados en Internet, etc., es lo que hace que el sujeto pase de estar "quieto" en el ciberespacio a ser un sujeto visible en Internet y, por consiguiente, convertirse en adecuado para el ciberdelito.

Estos dos elementos, interacción e introducción, serían los caracteres esenciales del objetivo adecuado. A ellos podría sumarse un tercero, el de autoprotección, pero este factor concuerda más con la adecuación del sistema como objetivo que de la persona, que es, en la cibercriminalidad social, de lo que realmente estamos hablando. En efecto, se ha podido constatar cómo el no hacer uso de los distintos programas diseñados para la seguridad de los equipos como (antivirus, antiespías, cortafuegos, etc.) está estrechamente relacionado con la probabilidad de ser víctima en el ciberespacio (Choi, 2008; Yucedal, 2010). También la forma en la que se gestionen las contraseñas va a tener efecto, de manera que quienes usan la misma contraseña para todo, y no las cambian con frecuencia, están expuestos a un mayor riesgo (Miro, 2013 y 2014). Son muchos los autores que han tratado de identificar los elementos de protección (antivirus, antiespías, cortafuegos, etc.) como guardianes físicos externos a la propia víctima

(Choi, 2008; Bossler y Holt, 2009; Grabosky, 2001; Holt y Bossler, 2009; Ngo y Paternoster, 2011; Yar, 2005). En cambio, estos elementos, como argumenta Miró (2011), no son externos a la propia víctima, en tanto en cuanto su correcto uso depende del actuar de ella.

Hay que reconocer, sin embargo, que en estos casos el objetivo adecuado es, primero, el sistema informático y, luego, la información o el patrimonio del titular del mismo o de otros. En la cibercriminalidad social, en cambio, el objetivo adecuado no es el sistema informático, sino la persona, la víctima del ciberacoso en la modalidad de que se trate. Y la persona se hace a sí mismo accesible cuando interacciona en Internet y se relaciona con otros, cuando introduce información sensible a ella misma. Por eso el elemento autoprotección, en contra de lo que han hecho otros como Miró (2013c), no parece apropiado para configurar el elemento objetivo adecuado. La verdadera protección frente a los ataques sociales serán, especialmente en el caso de los menores, vendrá por parte de quien tienen la obligación de protegerlos o de terceros que con su simple presencia o con su actuar cotidiano pueda evitarlo.

Vigilancia familiar

Al igual que en el espacio físico, la figura del guardián podrá ser representada por la policía, pero espacialmente en el caso de menores, por los padres, educadores o cualquier persona cercana que con su actividad cotidiana pueda protegerla (Grabosky, 2001; Miró, 2011). En este sentido, el estudio realizado por Marcum (2008) muestra como

efectivamente aquellos menores que están más controlados por sus padres, tienen menos probabilidades de ser víctimas de un ataque.

Sin embargo, la víctima puede variar con su actuar la probabilidad de ser más o menos vigilado, y por lo tanto más o menos protegido, por estos guardianes. Esto no significa que la protección dependa exclusivamente de la víctima, todo lo contrario, dependerá de quién puede ejercer la protección real, es decir, los terceros. Pero como sucede en el espacio físico, una persona puede plantearse pasear por una avenida que tiene una fuerte presencia policial y múltiples cámaras de seguridad o pasear por una calle estrecha, con poco tránsito y apenas control policial. En cualquiera de las dos opciones, es la propia víctima la que con su decisión está aumentando las posibilidades de estar más o menos vigilada, pues si decide la primera opción estará más vigilada que si opta por la segunda. En cualquier caso, quien tiene la capacidad de proteger al objetivo (en este caso a la persona que está paseando), es la policía mediante la visualización directa o a través de las CCTV. Esto trasladado al ciberespacio, y especialmente para el caso de los menores, puede ser el hecho de agregar o no a los padres como "amigos" a las redes sociales. Si el menor decide agregarlos está aumentado la probabilidad de que los padres puedan ejercer de guardianes frente a aquellos que no los agregan. Es decir, no será el menor el que se proteja así mismo, sino que ofrecerá la oportunidad de que los padres puedan ejercer de guardianes. Es cierto, por otra parte, que probablemente la capacidad efectiva de los padres como guardianes también estará mediada por otras variables, que sería recomendable estudiar mediante otras técnicas, pero lo cierto es que estarán más vigilados, y por lo tanto más protegidos, que los que simplemente no agregan a sus padres y familiares.

La misma cuestión se puede plantear cuando los menores comparten los sistemas electrónicos con los que navegan en Internet con otros familiares. El hecho de compartirlo con los hermanos implica incluir a otra persona que pueda ejercer de guardián, como lo es, en el espacio físico, el vecino que alerta a la policía de que otra persona está sufriendo una agresión física. En este caso, sin embargo, se podría plantear hasta qué punto el menor puede decidir sobre el hecho de compartir o no su ordenador. Probablemente, esta decisión dependerá en la mayoría de los casos de los padres, dado que se trata de menores, pero en cualquier caso, lo que interesa saber es si hay otra persona que pueda ejercer la vigilancia y por lo tanto, de guardián.

En definitiva, los que se trata de explicar es que para la cibercriminalidad social ejercida sobre los menores, el elemento guardián capaz puede ser concretado en la vigilancia que pueden ejercer los padres, estableciendo un control directo sobre las actividades cotidianas de los menores del ciberespacio o bien frecuentando los mismos espacios virtuales por los que se mueve el menor. Por tanto, a partir de la información que ofrecen los menores respecto a su actuar cotidiano, los objetivos de este trabajo son, por un lado, definir los elementos que hacen que un menor sea un objetivo adecuado en el ciberespacio y, por otro lado, analizar el efecto de la vigilancia familiar como parte del constructo del guardián capaz. Y todo ello, con el fin último de poder ofrecer información precisa, sobre la cual se puedan construir estrategias concretas de prevención que ayuden a disminuir de forma efectiva los riesgo de los menores en Internet.

Parte II. Estudio empírico

Capítulo I. Estudio empírico: Análisis de la victimización de ciberacoso continuado no sexual en menores de la provincia de Alicante

"Observar sin pensar es tan peligroso como pensar sin observar."

Ramón y Cajal

Sobre la base de las premisas teóricas comentadas en el capítulo anterior nos proponemos abordar una investigación que describa la prevalencia de victimización por conductas de ciberacoso o *harassment*, concretamente por las más graves de ellas, las que se realizan de forma continuada. El estudio se realizará sobre una muestra representativa de menores de edad de la provincia de Alicante, al haberse constatado que el uso de las TIC como herramienta de comunicación personal es mucho mayor entre los menores. El principal interés del estudio, en todo caso, no es la determinación de la prevalencia, sino la concreción de aquellas actividades cotidianas de los menores que les sitúan en una situación de riesgo de victimización por este tipo de delincuencia y, más allá, el elaborar un modelo predictivo de victimización que permita, en última estancia, determinar la probabilidad de riesgo de un menor atendiendo a sus hábitos en

Internet. Lo que también debe servir como medio para establecer estrategias de prevención precisas en este ámbito.

En este capítulo presentaremos los objetivos que se pretenden alcanzar con el trabajo y las hipótesis planteadas, para a continuación, mostrar la metodología empleada, y los resultados más relevantes de la investigación.

1. Objetivos e hipótesis de partida

1.1. Objetivos

El estudio tiene como **objetivos generales** conocer, por un lado, la prevalencia de victimización por ciberacoso continuado no sexual de menores de la provincia de Alicante; y por otro, determinar qué prácticas habituales de los menores, es decir, qué actividades cotidianas, inciden en la probabilidad de que un menor sea víctima de esta forma de cibercriminalidad.

Para alcanzar estos dos objetivos generales, se proponen los siguientes **específicos**:

a. Determinar la prevalencia de menores afectados por ciberacoso continuado no sexual.
b. Conocer la prevalencia de cada una de las formas de victimización que conforman el ciberacoso continuado no sexual.

c. Obtener una descripción detallada de los hábitos de uso de Internet de los menores.
d. Determinar las características demográficas de las víctimas de ciberacoso continuado.
e. Analizar la relación existente entre los hábitos de los menores en Internet con las distintas modalidades de ciberacoso continuado no sexual.
f. Comprobar, mediante modelos matemáticos, si los hábitos de los menores en Internet se agrupan de acuerdo a los planteamientos teóricos de las actividades cotidianas en el ciberespacio.

1. 2. Hipótesis

A partir de los planteamientos anteriores, se han formulado tres hipótesis, basadas en la idea de que son las actividades cotidianas que realiza el menor en el ciberespacio las que determinan la probabilidad de ser víctima en el ciberespacio. Pretenden ser contrastadas mediante el análisis de la relación entre las actividades que realizan los menores en el ciberespacio y la experiencia de cibervictimización.

La primera de las hipótesis postula que los menores que introducen en el ciberespacio bienes personales tienen más riesgo de ser víctima de ciberacoso continuado. Son varias las formas que tienen los menores de trasladar los bienes personales al ciberespacio. Pueden hacerlo mediante la cesión voluntaria de información personal a otros usuarios (bien publicándolos en los perfiles de las redes sociales o mediante otras herramientas de comunicación) o guardando en los

dispositivos con los que se conectan a Internet contenidos personales como fotos, videos, contraseñas, etc. La introducción consciente o inconsciente de bienes personales en el ciberespacio implica que pasan a estar disponibles para otras personas. Siguiendo esta idea, la primera hipótesis quedaría formulada de la siguiente manera:

A. Los menores que introducen mayor información sobre sí mismos en el ciberespacio tienen más probabilidad de convertirse en víctimas de ciberacoso continuado en él.

La segunda hipótesis está basada en la idea de que el usuario de Internet no se hace visible simplemente con su presencia en el ciberespacio. Este nuevo lugar es tan vasto, que lo que determina su visualización es su movimiento por él (Miró, 2011). Es decir, un usuario se hace visible en el ciberespacio cuando interacciona con otros. Por ejemplo, cuando hace uso del correo electrónico, las redes sociales u otras herramientas de comunicación. Por lo tanto, la segunda hipótesis quedaría formulada de la siguiente manera:

B. Los menores que interactúan más en el ciberespacio tienen más probabilidad de convertirse en víctimas de ciberacoso continuado.

La tercera hipótesis postula que la probabilidad de ser víctima también viene determinada por la cotidiana posibilidad de vigilancia

de padres, otros familiares y amigos de las víctimas respecto a las acciones que ellos, y otros sobre ellos, realizan en Internet. Así, tener pautas de uso cotidiano de las TIC que permitan, cuanto menos potencialmente, una vigilancia de su comportamiento en el ciberespacio, tales como tener en los perfiles de sus redes sociales a padres o familiares, o recibir un control sobre el uso del móvil y del ordenador con el que navegan en Internet, reducirá la posibilidad de ser víctima de estos delitos

C. Los menores que hagan un uso de las TIC que conlleve una menor posibilidad de control familiar, tienen más probabilidad de convertirse en víctimas de ciberacoso continuado.

2. Método

2.1. Muestra

La muestra empleada para la realización de este estudio está compuesta por 2.038 alumnos de educación secundaria y bachillerato de la provincia de Alicante. En total han participado 1.029 chicos (50,5%) y 1.009 chicas (49,5%), de edades comprendidas entre los entre los 12 y los 18 años, siendo la edad media de 14,6 años de edad (D.T.=1,72). Los participantes en el estudio se distribuyen entre los cuatro cursos de educación secundaria obligatoria y los dos de

bachillerato: 1º E.SO. (18,7%), 2º E.S.O. (18,7%), 3º E.SO. (18,8%), 4º E.S.O. (19%), 1º BACH (17,5%) y 2º BACH (7,3%).

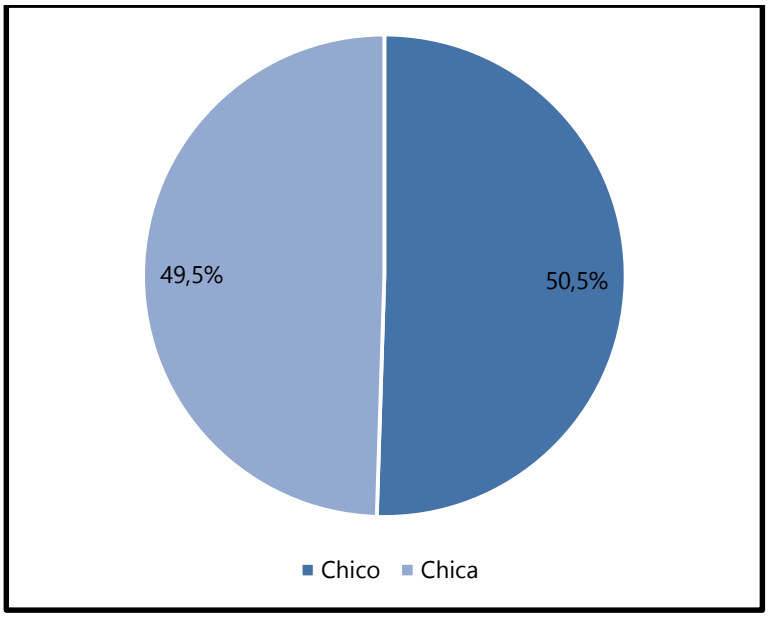


Ilustración 7. Sexo de los participantes

Tabla 9. Estadísticos de la variable edad

Estadísticos	
Media	14,63
Desv. típ.	1,717
Mínimo	12
Máximo	18

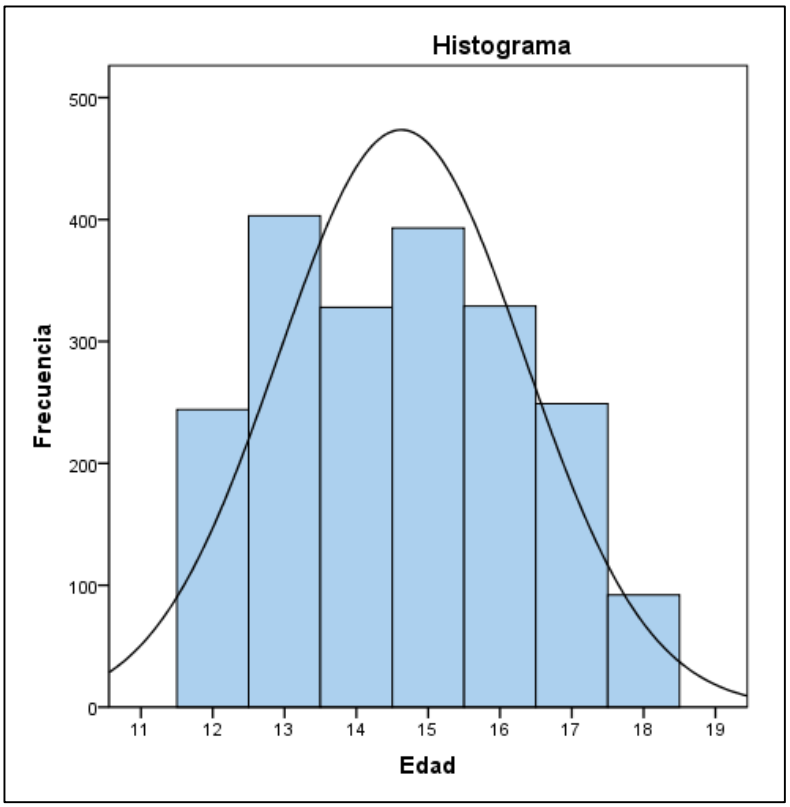


Ilustración 8. Histograma edad

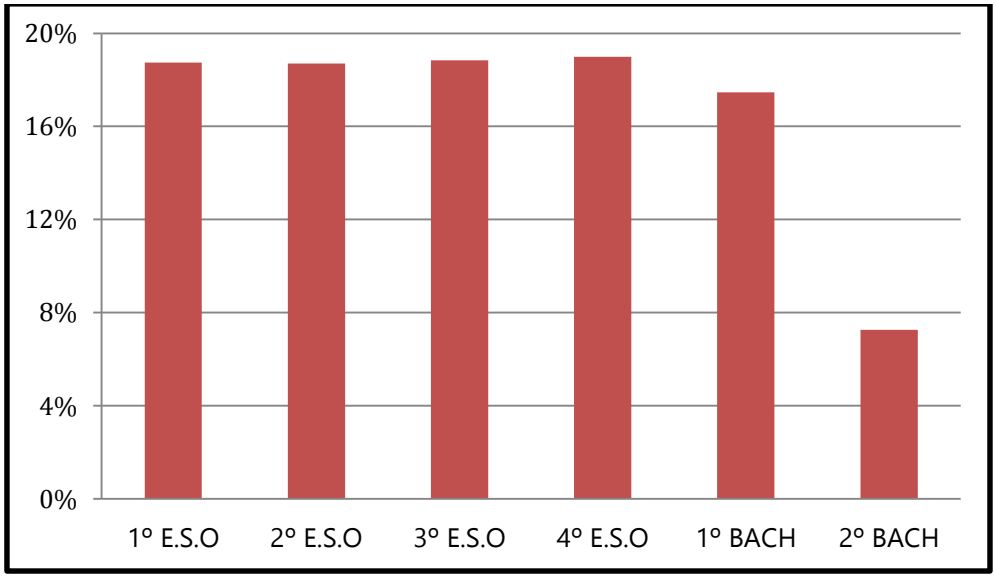


Ilustración 9. Distribución de los participantes por curso

El error muestral adopta un valor de +/- 2,1% con un nivel de confianza del 95%, para p=q=0,5.

$$n=\frac{z^2_{\alpha/2}\cdot pq}{E^2_{máx}}$$

2.2. Procedimiento de selección de la muestra

Para la obtención de la muestra se seleccionaron de manera aleatoria veinte centros de educación secundaria y bachillerato de la provincia de Alicante, tanto públicos como concertados. Para ello, en primer lugar, se obtuvo una relación de todos los centros donde se imparte enseñanza secundaria y bachillerato en la provincia de Alicante, proporcionada por la Consellería de Educación Cultura y Deporte, y se le asignó un número a cada uno de ellos. En segundo lugar, mediante un programa generador de números aleatorios se extrajeron los centros participantes.

Una vez elaborada la lista, se solicitó a la Consellería de Educación, Cultura y Deporte el permiso preceptivo para poder obtener información de los estudiantes de la Comunidad Valenciana. Una vez obtenido el permiso pertinente, se solicitó a los centros seleccionados su participación en el estudio. Tras la aceptación correspondiente, se procedió al envío de los consentimientos paternos a los centros, quienes se encargaron del reparto de los mismos a todos los alumnos

tanto de educación secundaria obligatoria como bachillerato. Finalmente, los centros que participaron en el estudio fueron: I.E.S Número 3 (Villajoyosa), I.E.S Mare Nostrum (Alicante), I.E.S Torrellano (Torrellano), I.E.S Xixona (Jijona), I.E.S Mediterranea (Benidorm), I.E.S Macià Abela (Crevillente), I.E.S Colegio Sagrado Corazón HH Maristas (Alicante), I.E.S Fray Ignacio Barrachina (Ibi), I.E.S Libertas (Torrevieja), I.E.S Figueras Pacheco (Alicante), I.E.S La Melva (Elda), I.E.S Haygón (San Vicente del Raspeig), I.E.S Pedro Ibarra Ruiz (Elche), I.E.S Cayetano Sempere (Elche), I.E.S Santa Pola (Santa Pola), I.E.S Luis García Berlanga (San Juan de Alicante), I.E.S Antonio Sequeros (Almoradí), I.E.S Enric Valor (Castalla), I.E.S La Nía (Aspe), Colegio Inmaculada Jesuitas (Alicante). De los centros participantes, dieciocho son de régimen público mientras que dos son de régimen concertado.

2.3. Variables

2.3.1. Variables dependientes

Siguiendo la tendencia de otros estudios similares, se ha optado por analizar la victimización por actos concretos de *cyberharassment* o ciberacoso continuado. Como se ha señalado en el marco teórico, es posible que estas conductas no tengan la suficiente gravedad para ser constitutivas de delito, eso no implica que no puedan causar daños psicológicos leves o incluso graves a quienes las padecen.

Con todo ello, se han incluido cuatro variables dependientes en el estudio relativas al ciberacoso continuado de carácter no sexual a

través de Internet, a las que a continuación se hará referencia detalladamente.

a. Insultar

Se trata de una variable cualitativa nominal con dos categorías, que hacen referencia a si a los sujetos de la muestra, en algún momento de su vida, alguien les ha insultado o ridiculizado repetidamente a través de Internet o el móvil (*P24. ¿En algún momento de tu vida alguien te ha insultado o ridiculizado repetidamente a través de Internet o del móvil?*). Aquellos sujetos que contestaron de manera afirmativa fueron categorizados como víctimas (1=Víctima) mientras que los que contestaron de manera negativa fueron categorizados como no víctimas (2=No víctima).

b. Rumores

Siguiendo el mismo procedimiento, la variable "rumores" cualitativa nominal con dos categorías, hace referencia a si algún sujeto de la muestra ha sufrido en algún momento de su vida que alguien difundiera rumores o mentiras sobre él de manera repetida con la intención de hacerle daño a través de Internet (*P26. ¿Alguien ha contado rumores o mentiras sobre ti de forma repetida para hacerte daño a través de Internet o del móvil?*). Aquellos sujetos que contestaron de manera afirmativa fueron categorizados como víctimas (1=Víctima)

mientras que los que contestaron de manera negativa fueron categorizados como no víctimas (2=No víctima).

c. Contacto repetido no deseado

También es una variable cualitativa nominal que hace referencia a si los sujetos de la muestra, en algún momento de su vida, alguien les ha contactado de manera repetida a través de Internet o el móvil tras haberle pedido que no lo hiciera (*P48. ¿Alguien ha contactado contigo repetidamente a través de Internet o el móvil tras haberle pedido que no lo hiciera?*). Aquellos sujetos que contestaron de manera afirmativa fueron categorizados como víctimas (1=Víctima) mientras que los que contestaron de manera negativa fueron categorizados como no víctimas (2=No víctima).

d. Marginar

Finalmente, se incluyó la variable marginar, también de naturaleza cualitativa nominal con dos categorías de respuesta, que hace referencia a la situación de marginación o exclusión a la que ha estado expuesto un sujeto de la muestra de manera repetida (*P37. ¿Alguien ha utilizado Internet o el móvil para marginarte o excluirte de manera continuada?)*. Aquellos sujetos que contestaron de manera afirmativa fueron categorizados como víctimas (1=Víctima) mientras que los que contestaron de manera negativa fueron categorizados como no víctimas (2=No víctima).

2.3.2. Variables independientes

Se incluyeron un total de setenta y nueve variables independientes, todas ellas relativas a las actividades cotidianas de los menores en Internet que, a continuación, se describen de manera detallada.

a. Ofrecer datos personales a través de Internet

Con esta variable cualitativa se obtuvo información de aquellos menores que han facilitado datos personales reales a través de Internet. La pregunta realizada a los menores es: *P102. ¿Alguna vez has dado tus datos reales a alguien través de Internet?.* Las dos categorías de respuesta son 1 = No y 2 = Si.

b. Tipo de datos personales ofrecidos a través de Internet

Esta variable estudia el tipo de datos que los menores introducen en la red. Aquellos sujetos que contestaron de manera afirmativa a facilitar datos personales reales se les preguntaba cuál, ofreciéndoles diez opciones de respuesta. Dado que se trata de una pregunta de respuesta múltiple, cada una de las respuestas ha sido entendida a su vez como una variable cualitativa. Todas ellas tienen dos categorías 1 = No y 2 = Si. Las variables son:

- He dado el nombre a través de Internet.
- He dado los apellidos a través de Internet
- He dado el número de teléfono a través de Internet.

- He dado fotos mías a otras personas a través de Internet.
- He dado el correo electrónico a través de Internet.
- He dado el nombre del colegio a través de Internet.
- He dado mi ubicación a través de Internet.
- He dado mi dirección a través de Internet.
- He dado mi edad a través de Internet.
- He dado mi estado civil a través de Internet.

c. Medio empleado por los sujetos para ceder sus datos personales a otras personas

Cuando los sujetos de la muestra afirmaban haber cedido datos personales a través de Internet, se les preguntaba por el medio empleado para realizar esta acción, ofreciéndoles seis opciones de respuesta. De nuevo, al tratarse de una pregunta con respuestas múltiples, cada una de las respuestas ha sido entendida a su vez como una variable. Todas ellas tienen dos categorías de respuesta 1 = No y 2 = Si. Las variables son:

- Dar datos personales reales a través del correo electrónico.
- Dar datos personales reales a través de mensajería instantánea.
- Dar datos personales reales a través de las redes sociales.
- Dar datos personales reales a través de páginas de videojuegos.

- Dar datos personales reales a través de las salas de chat.
- Dar datos personales reales a través de foros.

d. Información contenida en el ordenador con el que se conectan a Internet.

A los sujetos se les preguntó si guardaban información en el ordenador con el que se conectaban a Internet (*P120. ¿En el ordenador/Tablet con el que te conectas a Internet tienes guardadas alguna de estas cosas?)*. Se trataba de una pregunta con respuesta múltiple con cinco opciones de respuesta: 1. Ninguna; 2. Fotos personales; 3. Fotos íntimas; 4. Vídeos personales; 5. Información personal íntima. Todas las opciones fueron entendidas como variables independientes con dos opciones de respuesta (1 = No y 2 = Si). Por tanto, las variables incluidas son:

- No guardar archivos en el ordenador/Tablet con el que se conectan a Internet.
- Guardar fotos en el ordenador/Tablet con el que se conectan a Internet
- Guardar fotos íntimas en el ordenador/Tablet con el que se conectan a Internet.
- Guardar vídeos personales en el ordenador/Tablet con el que se conectan a Internet.

- Guardar información secreta o íntima en el ordenador/Tablet con el que se conectan a Internet.

e. Información contenida en el móvil con el que se conectan a Internet.

También se le preguntó a los sujetos si guardaban información en el móvil con el que se conectaban a Internet (*P121. ¿En el móvil con el que te conectas a Internet tienes guardadas alguna de estas cosas?)*. Se trataba de una pregunta con respuesta múltiple con cinco opciones de respuesta: 1. Ninguna; 2. Fotos personales; 3. Fotos íntimas; 4. Vídeos personales; 5. Información personal íntima. Todas las opciones fueron entendidas como variables independientes con dos opciones de respuesta (1 = No y 2 = Si). Por tanto, las variables incluidas son:

- No guardar archivos en el móvil con el que se conectan a Internet.
- Guardar fotos en el móvil con el que se conectan a Internet.
- Guardar fotos íntimas en el móvil con el que se conectan a Internet.
- Guardar vídeos personales en el móvil con el que se conectan a Internet.
- Guardar información secreta o íntima en el móvil con el que se conectan a Internet.

f. Uso otorgado al móvil con el que se conectan a Internet.

Se le preguntó a los participantes en el estudio por el uso que le otorgaban al móvil (*P15. ¿Para qué usas el móvil con el que te conectas a Internet?)*. Se trataba de una pregunta con respuesta múltiple. Las cuatro opciones de respuesta fueron entendidas como variables cualitativas independientes con dos categorías de respuesta 1 = No y 2 = Si. Las variables son:

- Usar el móvil para conocer personas nuevas.
- Usar el móvil para mantener contacto con personas conocidas.
- Usar el móvil para cotillear.
- Usar el móvil para ligar.

g. Número de correos electrónicos recibidos al día.

Es una variable de naturaleza ordinal que mide el número de correo recibidos al día (*P66. ¿Cuántos correos electrónicos recibes aproximadamente al día?)*. Esta pregunta tiene una escala de respuesta tipo Likert (1=Ninguno; 2= De 1 a 3; 3 = De 4 a 7; 4= De 8 a 15; 5= De 15 a 30; 6=Más de 30).

h. Horas a la semana dedicadas a chatear.

Variable de naturaleza ordinal que mide las horas a la semana que dedican los sujetos a chatear (*P80. ¿Cuántas horas a la*

semana dedicas aproximadamente a chatear por el ordenador/tablet). La escala de respuesta es de tipo Likert: 1=Ninguna; 2=Menos de 1h; 3=De 1 a 3h; 4=De 4 a 7h; 5=De 8 a 15h; 6=Más de 15h.

i. Horas al día dedicadas a las redes sociales

Variable de tipo ordinal que mide el número de horas que dedican los participantes en el estudio a las redes sociales (*P81. ¿Cuántas horas al día dedicas aproximadamente a las redes sociales como Tuenti, Instagram, Facebook, Twitter u otros?).* La escala de respuesta es de tipo Likert: 1=Ninguna; 2=Menos de 1h; 3=De 1 a 3h; 4=De 4 a 7h; 5=De 8 a 15h; 6=Más de 15h.

j. Número de perfiles de redes sociales creados usando datos personales reales.

Variable numérica que informa sobre el número de cuentas de redes sociales que han abierto los sujetos de la muestra usando para ello datos personales reales *(P82. ¿Cuántas cuentas has abierto usando datos personales reales?).*

k. Uso empleado a las redes sociales.

Se le preguntó a los participantes en el estudio por el uso que le otorgaban a las redes sociales (*P83. ¿Para que usas las redes sociales?)*. Se trataba de una pregunta con respuesta múltiple. Las siete opciones de respuesta fueron entendidas como

variables cualitativas independientes con dos categorías de respuesta 1 = No y 2 = Si. Las variables son:

- Usar las redes sociales para conocer personas nuevas.
- Usar las redes sociales para organizar fiestas.
- Usar las redes sociales para quedar con amigos.
- Usar las redes sociales para mantener el contacto con conocidos.
- Usar las redes sociales para cotillear.
- Usar las redes sociales para ligar.
- Usar las redes sociales para jugar.

l. Personas que agregan a los perfiles de redes sociales.

Esta variable incluida en el estudio analiza las personas a las que agregan los sujetos a las redes sociales (*P84. ¿Qué tipo de personas agregas a tus redes sociales?).* Se trataba de una pregunta con respuesta múltiple donde las opciones contempladas eran agregar a compañeros de clase, a compañeros de otras clases del colegio, a compañeros de actividades extraescolares, a amigos de otros amigos, a los padres, a los hermanos, a otros familiares y a desconocidos. Todas las respuestas se trataron como variables cualitativas independientes con dos categorías de respuesta 1 = No y 2=Si. Por tanto, las variables incluidas en el estudio son:

- Agrego a compañeros de clase a mis cuentas de redes sociales.
- Agrego a compañeros de otras clases a mis cuentas de redes sociales.
- Agrego a compañeros de actividades extraescolares a mis cuentas de redes sociales.
- Agrego a amigos de mis amigos a mis cuentas de redes sociales.
- Agrego a mis padres a mis cuentas de redes sociales.
- Agrego a mis hermanos a mis cuentas de redes sociales.
- Agregar a otros familiares a mis cuentas de redes sociales.
- Agregar a desconocidos a mis cuentas de redes sociales.

m. Poseer un blog propio.

Variable de naturaleza categórica con dos opciones de respuesta que hace distinción entre los sujetos de la muestra que tienen un blog propio y los que no (1=No; 2=Si), (*P89. ¿Tienes un blog propio?).*

n. Escribir en blogs o foros ajenos.

Variable de naturaleza categórica con dos opciones de respuesta que distingue entre aquellos sujetos que escriben en

foros o blogs ajenos de los que no (1 = No y 2=Si), (*P92. ¿Escribes en foros o blogs ajenos?*).

o. Realizar videoconferencias o videollamadas.

Variable de tipo ordinal que mide el número de horas que dedican los participantes en el estudio a realizar videoconferencias o videollamadas (*P96. ¿Cuántas horas a la semana dedicas a hacer videoconferencias o videollamadas?*). La escala de respuesta es de tipo Likert: 1=Ninguna; 2=Menos de 1h; 3=De 1 a 3h; 4=De 4 a 7h; 5=De 8 a 15h; 6=Más de 15h.

p. Horas a la semana dedicadas a jugar a videojuegos *online* con el ordenador.

Variable de tipo ordinal que mide el número de horas que dedican los participantes en el estudio a jugar a videojuegos *online* a través del ordenador (*P100_1. ¿Cuántas horas a la semana pasas jugando a videojuegos online con el ordenador?*). La escala de respuesta es de tipo Likert: 1=Ninguna; 2=Menos de 1h; 3=De 1 a 3h; 4=De 4 a 7h; 5=De 8 a 15h; 6=Más de 15h.

q. Horas a la semana dedicadas a jugar a videojuegos *online* con el móvil.

Variable de tipo ordinal que analiza el número de horas que dedican los participantes en el estudio a jugar a videojuegos

online a través del móvil (*P100_2. ¿Cuántas horas a la semana pasas jugando a videojuegos online con el ordenador?*). La escala de respuesta es de tipo Likert: 1=Ninguna; 2=Menos de 1h; 3=De 1 a 3h; 4=De 4 a 7h; 5=De 8 a 15h; 6=Más de 15h.

r. Chatear a través de los videojuegos *online*.

Variable cualitativa con dos opciones de respuesta que identifica a los sujetos de la muestra que chatean a través de los canales que facilita los videojuegos *online* (*P101. ¿Utilizas los videojuegos para hablar (chatear) con otros jugadores? 1=No y 2=Si*).

s. Contactar con desconocidos a través de Internet.

Variable numérica que mide el número de veces que los participantes en el estudio han contactado con desconocidos a través de Internet (*P105. ¿Cuántas veces has contactado con desconocidos a través de Internet?*).

t. Medio usado para contactar con desconocidos a través de Internet.

A los sujetos que informaron que habían contactado con desconocidos a través de Internet se les preguntó por el medio empleado para hacerlo (*P107. ¿A través de que medio has*

contactado con desconocidos?). Al tratarse de una pregunta con respuesta múltiple, se optó por usar cada respuesta como una variable cualitativa independiente con dos opciones de respuesta (1=No y 2=Si). Las variables incluidas son:

- Contactar con desconocidos a través de la mensajería instantánea.
- Contactar con desconocidos a través de salas de chat.
- Contactar con desconocidos a través de los videojuegos *online.*
- Contactar con desconocidos a través de las redes sociales.

u. Motivo por el que contactan con desconocidos a través de Internet.

Además de preguntarles por el medio empleado para contactar con desconocidos, se les preguntó por el motivo para hacerlo (*P106. ¿Qué tipo de contacto?).* De nuevo, la pregunta es de respuesta múltiple por lo que las respuestas fueron entendidas como variables cualitativas independientes con dos opciones de respuesta (1=No y 2=Si). Las variables son:

- Contactar con desconocidos para mantener una amistad.
- Contactar con desconocidos para mantener una relación.

- Contactar con desconocidos para jugar.

v. Sexting.

Para medir si los participantes en el estudio habían hecho alguna vez *sexting* se optó por realizar dos preguntas, una relacionada con el número de veces que había enviado fotos suyas en situación comprometida y, otra, sobre el número de veces que habían enviado vídeos suyos en situación comprometida (*P114. ¿Alguna vez te has hecho una foto comprometida (íntima) y se la has enviado a alguien a través del móvil o Internet? y P116. ¿Alguna vez te has hecho un vídeo comprometido (íntimo) y se lo has enviado a alguien a través del móvil o Internet?*). Ambas variables fueron reagrupadas en una sola variable de naturaleza categórica con dos opciones de respuesta: los sujetos que afirmaron que en alguna ocasión se habían hecho una foto o vídeo en situación comprometida y luego lo se lo habían enviado a alguien a través de Internet se les incluyó en la categoría "2=Si" y los que afirmaron que nunca lo había hecho en la categoría "1=No".

w. Comportamiento desviado.

También se analizó la posibilidad de que los sujetos hubiesen realizado comportamientos desviados a través de Internet o el móvil, es decir, que también hubieran realizado comportamientos de ciberacoso, tanto de manera continuada como no continuada. Se incluyeron un total de ocho conductas,

por lo tanto se han incluido en el estudio ocho variables de naturaleza categórica con dos opciones de respuesta (0=No y 1=Si). Las variables incluidas son:

- Haber insultado o ridiculizado de manera repetida a través de Internet (*P128. Alguna vez has insultado o ridiculizado a alguien de forma repetida a través de Internet?*).
- Haber difundido rumores o mentiras sobre alguien de forma repetida a través de Internet o el móvil con la intención de hacerle daño (*P130. ¿Alguna vez has contado rumores o mentiras sobre alguien de forma repetida para hacerle daño a través de Internet?*).
- Haber contactado de manera repetida con una persona a través de Internet tras haberle pedido que no lo hiciera (*P146. ¿Has contactado con alguien de forma repetida a través de Internet tras haberte pedido que no lo hicieras?*).
- Haber marginado de manera repetida a otra persona a través de Internet (*P138. Has utilizado Internet para marginar o excluir de manera continuada a alguien?*).
- Haber difundido información secreta o íntima de otra persona a través de Internet sin su consentimiento (*P134. ¿Alguna vez has difundido información secreta o íntima de alguien, sin su consentimiento a través de Internet o del móvil?*).

- Haber amenazado a otra persona a través de Internet (*P140. ¿Has amenazado a través de Internet o el móvil a alguien?*).
- Haber coaccionado a otra persona a través de Internet (*P142. ¿Has obligado con violencia o intimidación a alguien a hacer algo que no quería a través de Internet o el móvil?*).
- Haber suplantado la identidad de otra persona a través de Internet (*P144. ¿Te has hecho pasar por alguien para dañarle por Internet o el móvil?*).

x. Compartir el ordenador con otras personas.

Se preguntó a los participantes si compartían el ordenador con otras personas y con quién. Se trataba de una pregunta con respuesta múltiple por lo que cada respuesta se trató como variables cualitativas independientes con dos opciones de respuesta (1=No y 2=Si). Las variables son:

- No compartir el ordenador.
- Compartir el ordenador con los padres.
- Compartir el ordenador con los hermanos.
- Compartir el ordenador con otros familiares.

y. No limitar el acceso a los perfiles de redes sociales.

Variable cualitativa con dos opciones de respuesta que distingue entre los que limitan el acceso a sus perfiles de redes

sociales y los que no (*P85. ¿Limitas el acceso a tus cuentas en redes sociales?*). Para mantener la dirección de la variable respecto a las demás, se optó por codificar la variable de forma inversa, de manera que la variable queda etiquetada como "No limitar el acceso a los perfiles de redes sociales" y cuyas respuestas son 1=No y 2=Si.

z. No comunicar a los padres el uso de las redes sociales.

También se les preguntó a los participantes si sus padres tenían conocimiento de la existencia de sus perfiles de redes sociales (*P86. ¿Tus padres saben que tienes cuentas en redes sociales?*). Del mismo modo que en la variable anterior, entendiendo que el no conocimiento de los padres puede ser un factor de riesgo, se optó por codificar la variable de la siguiente forma: aquellos que sus padres no tenían conocimiento se les codificó con un dos, mientras que aquellos que si lo sabían fueron codificados con un uno (1= No y 2=Si).

aa. No control de los padres sobre el uso del ordenador y del móvil.

También se optó por preguntar a los sujetos de la muestra por el control que realizaban los padres sobre el uso que hacía del ordenador y del móvil (*P22_1. ¿Tus padres controlan lo que haces en Internet con el ordenador? y P22_2. ¿Tus padres controlan lo que haces en Internet con el móvil?*). De nuevo, se

entendió que la falta de control es un factor de riesgo por lo que se decidió cambiar la dirección de las variables, por lo que finalmente quedaron incluidas dos variables de naturaleza cualitativa con dos opciones de respuesta (1=No y 2=Si):

- No control de los padres sobre el uso del ordenador.
- No control de los padres sobre el uso de móvil.

Para facilitar la consulta del conjunto de variables, a continuación se presenta un tabla resumen:

Tabla 10. Tabla resumen de las variables incluidas en el estudio

NOMBRE VARIABLE	ETIQUETA VARIABLE	CODIFICACIÓN
Variables dependiente		
V_INSULTO	¿En algún momento de tu vida alguien te ha insultado o ridiculizado repetidamente a través de Internet o del móvil?	1 "No Víctima" 2 "Víctima".
V_RUMORES	¿Alguien ha contado rumores o mentiras sobre ti de forma repetida para hacerte daño a través de Internet o del móvil?".	1 "No Víctima" 2 "Víctima".
V_CONTACTO	¿Alguien ha contactado contigo repetidamente a través de Internet o el móvil tras haberle pedido que no lo hiciera?	1 "No Víctima" 2 "Víctima".
V_MARGINAR	¿Alguien ha utilizado Internet o el móvil para marginarte o excluirte de manera continuada?	1 "No Víctima" 2 "Víctima".
Variables independientes		
DATOS_PERSONALES	¿Alguna vez has dado tus datos reales a alguien a través de Internet?	1 'NO' 2 'SI'
DAR_NOMBRE	He dado el nombre a través de Internet.	1 'NO' 2 'SI'
DAR_APELLIDOS	He dado los apellidos a través de Internet	1 'NO' 2 'SI'
DAR_TELEFONO	He dado el número de teléfono a través de Internet	1 'NO' 2 'SI'
DAR_FOTOS	He dado fotos mías a otras personas a través de Internet	1 'NO' 2 'SI'
DAR_EMAIL	He dado el correo electrónico a través de Internet	1 'NO' 2 'SI'
DAR_COLEGIO	He dado el nombre del colegio a través de Internet	1 'NO' 2 'SI'

DAR_UBICACION	He dado mi ubicación a través de Internet	1 'NO' 2 'SI'
DAR_DIRECCION	He dado mi dirección a través de Internet	1 'NO' 2 'SI'
DAR_EDAD	He dado mi edad a través de Internet	1 'NO' 2 'SI'
DAR_ESTCIV	He dado mi estado civil a través de Internet	1 'NO' 2 'SI'
DP_EMAIL	Dar datos personales a través del correo electrónico	1 'NO' 2 'SI'
DP_MENSAJERIA	Dar datos personales a través de la mensajería instantánea	1 'NO' 2 'SI'
DP_REDES	Dar datos personales a través de redes sociales	1 'NO' 2 'SI'
DP_VIDEOJUEGO	Dar datos personales a través de páginas de videojuegos	1 'NO' 2 'SI'
DP_FOROS	Dar datos personales a través de foros	1 'NO' 2 'SI'
DP_CHAT	Dar datos personales a través de salas de chat	1 'NO' 2 'SI'
NO_GUARDAR_ORDENADOR	No guardar archivos en el ordenador/*tablet*	1 'NO' 2 'SI'
GUARDAR_OR_FOTOS	Guardar en el ordenador/*tablet* fotos	1 'NO' 2 'SI'
GUARDAR_OR_FOTOS_INTIMAS	Guardar en el ordenador/*tablet* fotos íntimas	1 'NO' 2 'SI'
GUARDAR_OR_VIDEOS	Guardar en el ordenador/*tablet* videos	1 'NO' 2 'SI'
GUARDAR_OR_INFO	Guardar en el ordenador/*tablet* información personal/íntima	1 'NO' 2 'SI'
NO_GUARDAR_MOVIL	No guardar archivos en el móvil	1 'NO' 2 'SI'
GUARDAR_MO_FOTOS	Guardar en el móvil fotos	1 'NO' 2 'SI'

GUARDAR_MO_FOTOS_INTIMAS	Guardar en el móvil fotos íntimas	1 'NO' 2 'SI'
GUARDAR_MO_VIDEOS	Guardar en el móvil videos	1 'NO' 2 'SI'
GUARDAR_MO_INFO	Guardar en el móvil información personal o íntima	1 'NO' 2 'SI'
MOVIL_DESCONOCIDOS	Usar el móvil para conocer personas nuevas	1 'NO' 2 'SI'
MOVIL_CONOCIDOS	Usar el móvil para mantener contacto con conocidos	1 'NO' 2 'SI'
MOVIL_COTILLEAR	Usar el móvil para cotillear	1 'NO' 2 'SI'
MOVIL_LIGAR	Usar el móvil para ligar	1 'NO' 2 'SI'
CORREOS_DIA	Correos electrónicos recibidos al día	1=0; 2= 1-3; 3=4-7; 4=8-15; 5=15-30; 6=>30
CHATEAR	Horas a la semana dedicadas a chatear	1=0; 2=1-3; 3=4-7; 4=8-15; 5=15-30; 6=>30
REDES_SOCIALES_H.	Horas al día dedicadas a las redes sociales	1=0; 2=<1; 3=1-3; 4=4-7; 5=8-15; 6=>15
REDES_SOCIALES_N	Número de cuentas abiertas usando datos reales	Numérica
RS_DESCONOCIDOS	Usar las redes sociales para conocer personas nuevas	1 'NO' 2 'SI'
RS_FIESTAS	Usar las redes sociales para organizar fiestas	1 'NO' 2 'SI'
RS_QUEDARAMIGOS	Usar las redes sociales para quedar con amigos	1 'NO' 2 'SI'
RS_AMIGOS	Usar las redes sociales para mantener el contacto con conocidos	1 'NO' 2 'SI'

RS_COTILLEAR	Usar las redes sociales para cotillear	1 'NO' 2 'SI'
RS_LIGAR	Usar las redes sociales para ligar	1 'NO' 2 'SI'
RS_JUGAR	Usar las redes sociales para jugar	1 'NO' 2 'SI'
RS_AGR_COMPANEROSCLASE	Agregar a sus redes sociales a compañeros de clase	1 'NO' 2 'SI'
RS_AGR_COMPANEROSCOLE	Agregar a sus redes sociales a compañeros de otras clases	1 'NO' 2 'SI'
RS_AGR_COMPANEROSEXTRA	Agregar a sus redes sociales a compañeros de actividades extraescolares	1 'NO' 2 'SI'
RS_AGR_AMIGOSDEAMIGOS	Agregar a sus redes sociales a amigos de sus amigos	1 'NO' 2 'SI'
RS_AGR_PADRES	Agregar a sus redes sociales a sus padres	1 'NO' 2 'SI'
RS_AGR_HERMANOS	Agregar a sus redes sociales a sus hermanos	1 'NO' 2 'SI'
RS_AGR_OTROSFAMILIARES	Agregar a sus redes sociales a otros familiares	1 'NO' 2 'SI'
RS_AGR_DESCONOCIDOS	Agregar a desconocidos a sus redes sociales	1 'NO' 2 'SI'
BLOG_PROPIO	Tener un blog propio	1 'NO' 2 'SI'
BLOG_AJENO	Escribir comentarios en blog o foros ajenos	1 'NO' 2 'SI'
VIDEOLLAMADA	Realizar videoconferencias o videollamadas	1=0; 2=<1; 3=1-3; 4=4-7; 5=8-15; 6=>30
VIDEOJUEGO_ORDENADOR	Horas a la semana dedicadas a jugar a videojuegos *online* con el ordenador	1=0; 2=<1; 3=1-3; 4=4-7; 5=8-15; 6=>15

VIDEOJUEGO_MOVIL	Horas a la semana dedicadas a jugar a videojuegos *online* con el móvil	1=0; 2=<1; 3=1-3; 4=4-7; 5=8-15; 6=>15
VIDEOJUEGO_CHAT	Chatear a través de los videojuegos *online*	1 'NO' 2 'SI'
CONTACTO_DESCONOCIDOS	Contactar con desconocidos a través de Internet	1 'NO' 2 'SI'
CD_MENSAJERIA	Contactar con desconocidos a través de mensajería instantánea	1 'NO' 2 'SI'
CD_CHAT	Contactar con desconocidos a través de chat	1 'NO' 2 'SI'
CD_RS	Contactar con desconocidos a través de redes sociales	1 'NO' 2 'SI'
CD_VIDEOJUEGO	Contactar con desconocidos a través de videojuegos *online*	1 'NO' 2 'SI'
CD_MOT_AMISTAD	Contactar con desconocidos para mantener una amistad	1 'NO' 2 'SI'
CD_MOT_RELACION	Contactar con desconocidos para mantener una relación	1 'NO' 2 'SI'
CD_MOT_JUGAR	Contactar con desconocidos para jugar	1 'NO' 2 'SI'
SEXTING	Haber hecho *sexting* al menos una vez	1 'NO' 2 'SI'
INSULTAR	Haber insultado de manera repetida a través de Internet	1 'NO' 2 'SI'
RUMORES	Haber contado rumores falsos sobre otra persona de manera repetida a través de Internet	1 'NO' 2 'SI'
CONTACTO_REPETIDO	Haber contactado de manera repetida a otra persona a través de Internet tras haberle pedido que no lo hiciera	1 'NO' 2 'SI'
MARGINAR	Haber marginado de manera repetida a otra persona a través de Internet	1 'NO' 2 'SI'

DIFUNDIR_INFO	Haber difundido información personal de otra persona a través de Internet	1 'NO' 2 'SI'
AMENAZAR	Haber amenazado a otra persona a través de Internet	1 'NO' 2 'SI'
COACCIONAR	Haber coaccionado a otra persona a través de Internet	1 'NO' 2 'SI'
SUPLANTAR	Haber suplantado a otra persona a través de Internet	1 'NO' 2 'SI'
NO_COMPARTIR	No compartir el ordenador/*tablet*	1 'NO' 2 'SI'
NO_COMPARTIR_PADRES	No compartir el ordenador/*tablet* con los padres	1 'NO' 2 'SI'
NO_COMPARTIR_HERMANOS	No compartir el ordenador/*tablet* con los hermanos	1 'NO' 2 'SI'
NO_COMPARTIR_FAMILIARES	No compartir el ordenador/*tablet* con otros familiares	1 'NO' 2 'SI'
NO_LIMITES_RS	No limitar el acceso a los perfiles de redes sociales	1 'NO' 2 'SI'
NO_CONOCIMINETO_PADRES_RS	Los padres no tienen conocimiento de sus cuentas en redes sociales	1 'NO' 2 'SI'
NO_CONTROL_ORDENADOR	No control de los padres sobre el uso del ordenador/*tablet*	1 'NO' 2 'SI'
NO_CONTROL_MÓVIL	No control de los padres sobre el uso del móvil	1 'NO' 2 'SI'

2.4. Instrumento

El instrumento empleado para el presente trabajo es la encuesta electrónica "Hábitos de los menores en Internet". Se trata de una herramienta creada *ad hoc* por el Centro d para el estudio y prevención de la delincuencia para el proyecto financiado por la Diputación de

Alicante "Estudio sobre las distintas formas de violencia que sufren los menores a través de las nuevas tecnologías de la información y las comunicaciones". Esta encuesta tiene como objetivos conocer, por un lado, la prevalencia de victimización de cada una de las formas de violencia que sufren los menores a través de Internet; y, por otro, los hábitos adquiridos por los menores en el manejo de las tecnologías de la información y la comunicación. Permitiendo así establecer la relación entre las actividades cotidianas que realizan los menores en Internet y la probabilidad de cibervictimización.

Para crear la encuesta se procedió, en primer lugar, a elaborar una lista de ítems atendiendo a los objetivos propuestos en el estudio. Tras múltiples reuniones con expertos en metodología, cibervictimización y trabajo con menores, donde se discutió la adecuación de cada uno de los ítems así como su orden, se desarrolló una encuesta borrador.

Con el fin de determinar la viabilidad de la encuesta se procedió a hacer un estudio piloto con 100 menores de un centro de enseñanza secundaria de la provincia de Alicante, que simulaban las características de una muestra representativa. El pase de la encuesta se realizó en el propio centro y fue llevado a cabo por tres encuestadores debidamente formados para tal labor.

Tras la obtención de datos, se realizaron los análisis psicométricos propios para determinar la adecuación de las preguntas. Asimismo, se mantuvieron reuniones con los encuestadores con el fin de analizar los posibles inconvenientes que pudieran surgir durante el pase de encuestas. Tras comprobar la conveniencia de cada una de las

preguntas, así como su disposición, se procedió a desarrollar la encuesta definitiva, que puede consultarse en el anexo.

La encuesta está compuesta por cuatro tipo de preguntas. El primer tipo de preguntas se corresponden con variables sociodemográficas tales como el sexo, la edad, el colegio en el que estudian y el curso. El segundo tipo de preguntas tienen que ver con todas las formas de violencia sufrida por los menores a través de Internet (insultos, amenazas, suplantación de identidad, coacciones, acoso sexual, etc.). El tercer tipo de preguntas son referentes al uso de las distintas herramientas de comunicación personal que ofrece Internet (Mensajería instantánea, redes sociales, correo electrónico, foros, blogs, etc.). Por último, incluye una serie de preguntas que tienen que ver con las actividades cotidianas que, no siendo específicas del uso de Internet, si pueden mediatizar su uso. Como, por ejemplo, si tiene ordenador personal propio o debe compartirlo con otras personas, si posee un *smartphone* con tarifa de datos contratada, el control por parte de los padres sobre las horas y las actividades que realizan los menores en Internet, etc. Para el presente trabajo no se han utilizado la totalidad de los ítems incluidos, sino tan sólo aquellos que tienen que ver con los objetivos propuestos en el mismo, y que han quedado reflejados en el apartado "variables del estudio".

2.5. Procedimiento

Para la obtención de los datos se alojó la encuesta en un servidor de Internet a la que se podía acceder a través de un enlace. El procedimiento para que los alumnos contestaran la encuesta fue el

mismo en todos los centros. Tras convenir con la dirección de los centros la fecha y hora del pase de encuestas, dos encuestadores de los seis debidamente formados para tal labor, se trasladaban al centro y en la sala de ordenadores habilitaba la encuesta accediendo a ella a través de un enlace. Una vez preparados los ordenadores, se solicitaba a los menores que accedieran a la sala, destinando un ordenador para cada alumno. Una vez informados los estudiantes sobre la voluntariedad de la participación, así como de las cuestiones previas de funcionamiento, contestaban la encuesta y, al finalizar, los datos eran registrados en una base de datos en formato csv sin identificaciones personales. El tiempo medio de respuesta fue de 30 minutos.

3. Resultados

3.1. Análisis descriptivos

3.1.1. Análisis descriptivo de los menores víctimas de ciberacoso continuado no sexual de la provincia de Alicante

Con el objetivo de conocer la prevalencia de victimización de las diferentes formas de ciberacoso continuado medidas en el estudio, se procedió a realizar un análisis descriptivo de las variables dependientes, cuyos resultados se presentan a continuación.

De las cuatro formas de ciberacoso continuado medidas en el estudio, los resultados muestran que 469 de los 2038 participantes en el estudio, en algún momento de su vida, han sido insultados o ridiculizados de manera repetida a través de Internet o el móvil. Esto es, que el porcentaje de víctimas se sitúa en el 23% frente a un 77% que nunca ha sufrido esta forma de ciberacoso.

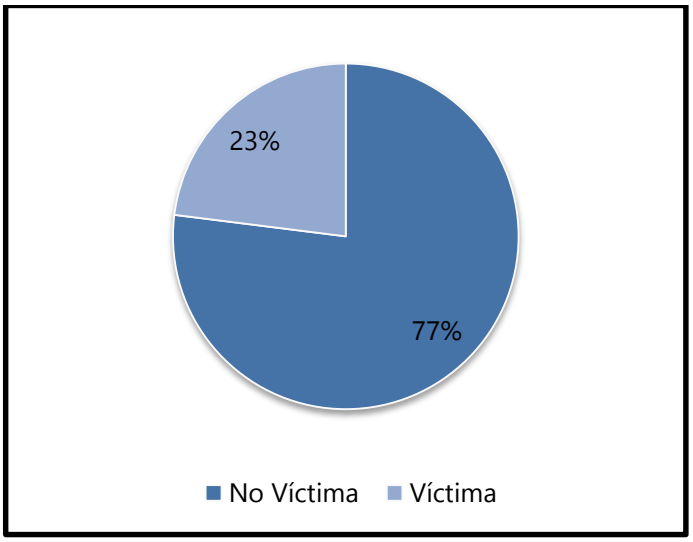


Ilustración 10. Prevalencia de cibervictimización por insultos continuados

Referente a la cibervictimización consistente en lanzar rumores o mentiras de manera continuada, el porcentaje de victimización se sitúa en el 21,5% (n=438) frente a un 78,5% (n=1600) que nunca lo ha padecido.

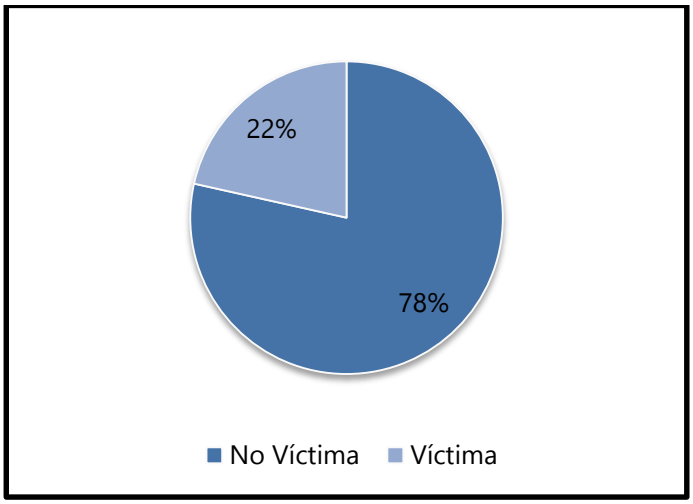


Ilustración 11. Prevalencia de cibervictimización por rumores o mentiras continuadas

El porcentaje de cibervictimización disminuye a un 14,4% (n=293) cuando se trata de haber sido acosado mediante el contacto repetido no deseado a través de Internet o el móvil habiendo solicitado previamente el cese de tal acción.

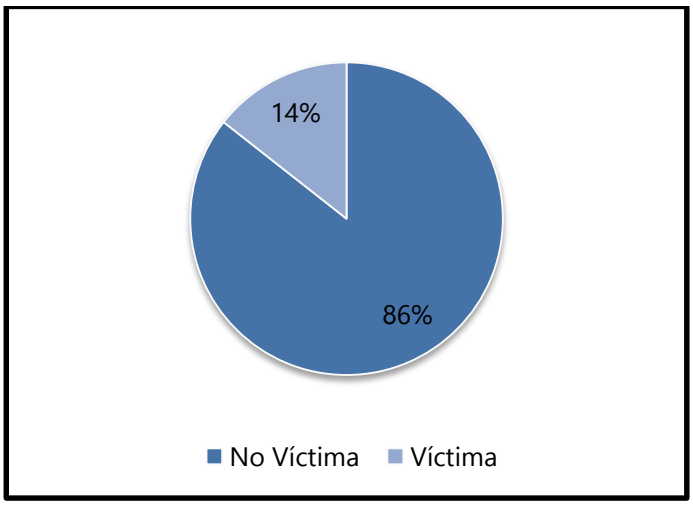


Ilustración 12. Prevalencia de cibervictimización por contacto repetido no deseado

Respecto a la última de las conductas de ciberacoso incluidas en el estudio, el haber sido marginado de manera repetida a través de Internet, el porcentaje de victimización se sitúa en 4,8% (n=293).

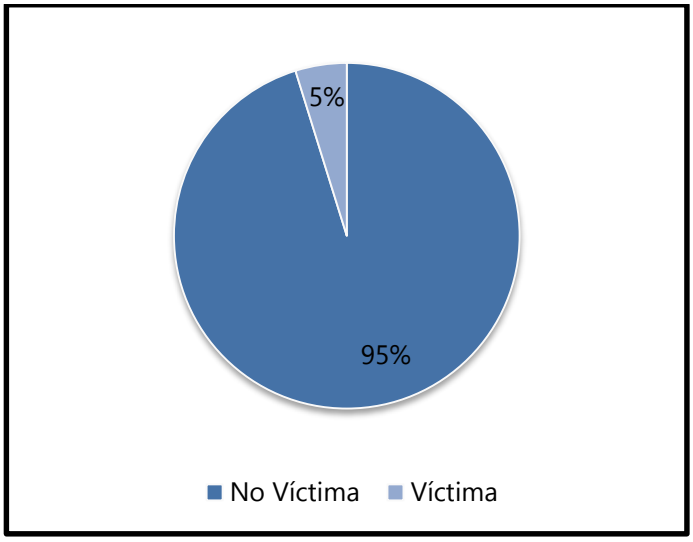


Ilustración 13. Prevalencia de cibervictimización por haber sido marginado de manera repetida

Agrupando las cuatro formas de victimización de manera conjunta, observamos que la conducta que con mayor frecuencia se repite es la de "insultos o haber sido ridiculizado", seguido de "rumores o mentiras", "contacto repetido no deseado" y "marginar".

3.1.2. Análisis descriptivos de las actividades cotidianas de los menores de la provincia de Alicante en Internet

Del mismo modo que en el apartado anterior, y con el objetivo de determinar las actividades cotidianas de los menores en el ciberespacio, se realizó en el análisis descriptivo de las variables independientes incluidas en el estudio, y que se presentan a continuación.

a. Ofrecer datos personales a través de Internet.

Los datos obtenidos reflejan que, de los menores participantes en la encuesta, un 35,1% admiten haber facilitado sus datos personales a través de Internet frente al 64,9% que niegan haberlos facilitado.

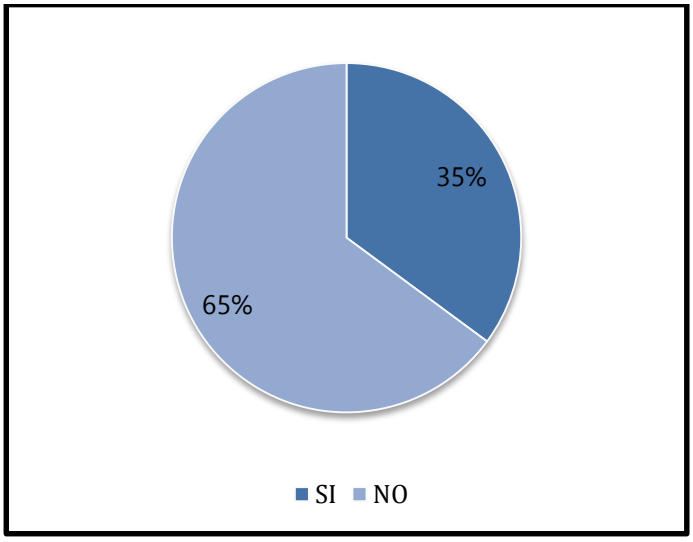


Ilustración 14. Ofrecer datos personales reales a través de Internet

b. Tipo de datos personales ofrecidos a través de Internet.

Constatado el hecho de que los menores facilitan sus datos personales reales a otras personas a través de Internet, el siguiente paso fue determinar el tipo de datos y en qué medida eran facilitados a través de Internet. Se puede observar en la siguiente ilustración cómo el nombre es el dato que se da con mayor facilidad (34,8%), seguido de los apellidos (27%) y la edad (26,2%). El número de teléfono es el cuarto dato más facilitado por los menores a través de Internet (20%), al igual que la dirección de correo electrónico, con un 19,2%. En menor medida se facilitan fotos propias que alcanza un porcentaje del 13,8%, así como indicar el nombre del centro donde se estudia, con un 12,9%, el estado civil (8,9%) y la ubicación desde donde se conecta (8,1%).

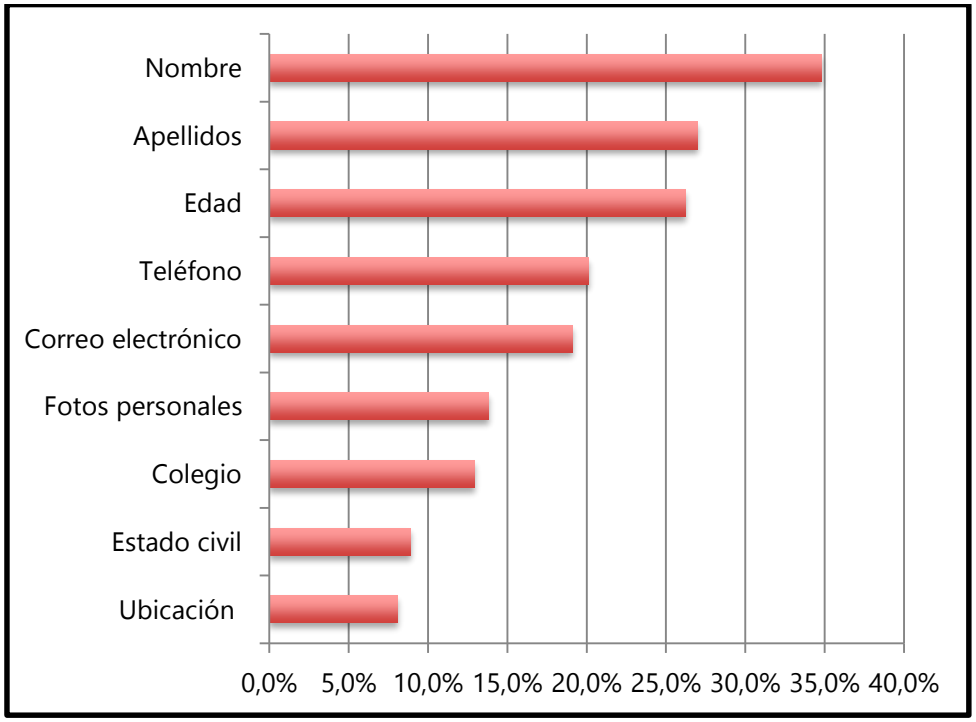


Ilustración 15. Tipo de datos personales facilitados por Internet

c. Medio empleado por los sujetos para ceder sus datos personales a otras personas.

Además del tipo de datos, se solicitó a los participantes que indicaran el medio a través del cual cedían tales datos. Los resultados arrojan que el 24,4% lo hace a través de aplicaciones como WhatsApp, Line, etc. Es decir, a través de herramientas de comunicación propias de la mensajería instantánea. En segundo lugar, se encuentra la transmisión de datos personales a través de las redes sociales (Facebook, Twitter, Tuenti, etc.) con un 20,5%, seguido del correo electrónico con un 9,2%. En menor medida, los facilitan a través de páginas de videojuegos *online* (3%), salas de chats (2,2%) y los foros (0,8%).

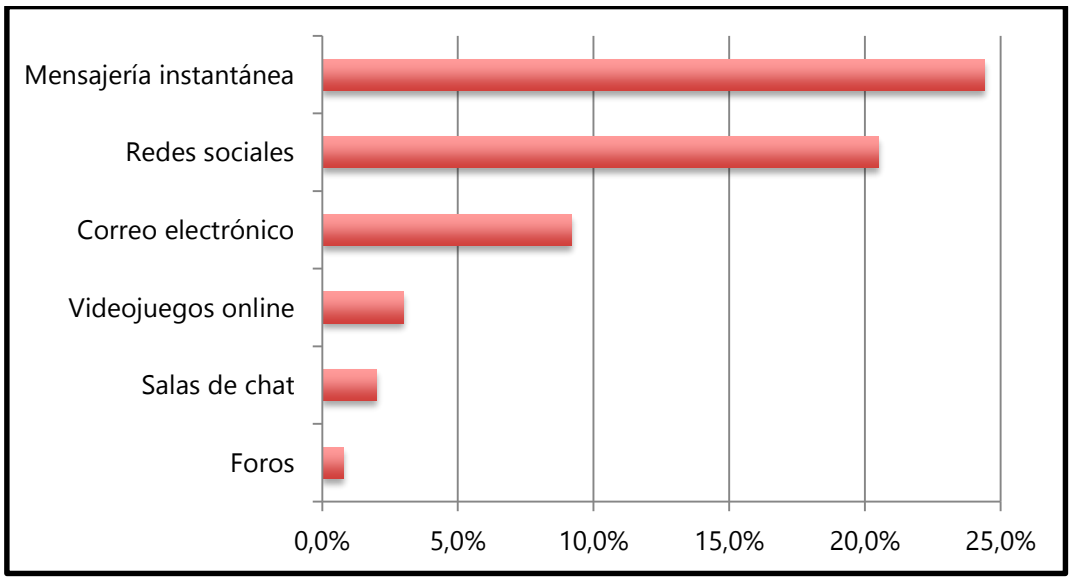


Ilustración 16. Medio empleado para ceder datos personales reales en Internet

d. Información contenida en el ordenador con el que se conectan a Internet.

Los resultados arrojan que el 49,1% de los participantes en el estudio guarda algún tipo de información o archivos en el ordenador con el que se conectan a Internet.

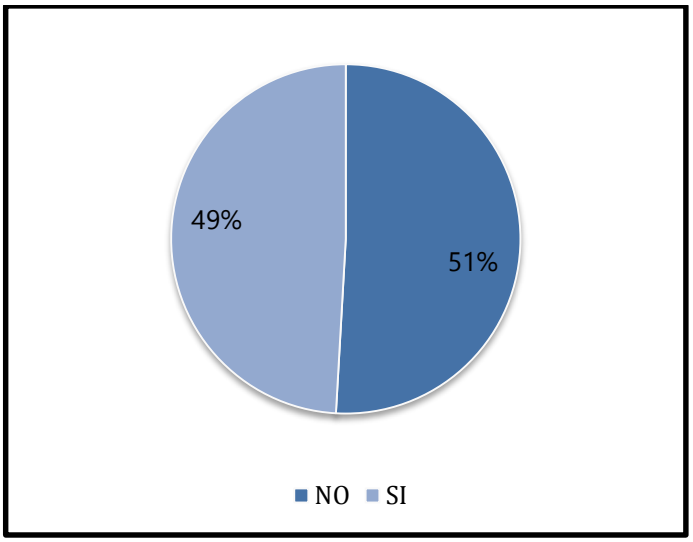


Ilustración 17. Guardar información o archivos en el ordenador con el que se conectan a Internet

Una vez que se constató el hecho de que los sujetos de la muestra guardan información personal en el ordenador con el navegaban en Internet, se procedió a preguntarles por el tipo. Los resultados obtenidos muestran que, en mayor medida, los sujetos guardan fotos personales, con un porcentaje de 40,8%, seguido de vídeos (18,9%), información personal e íntima (12,1%) y, en menor medida, fotos íntimas (3,1%).

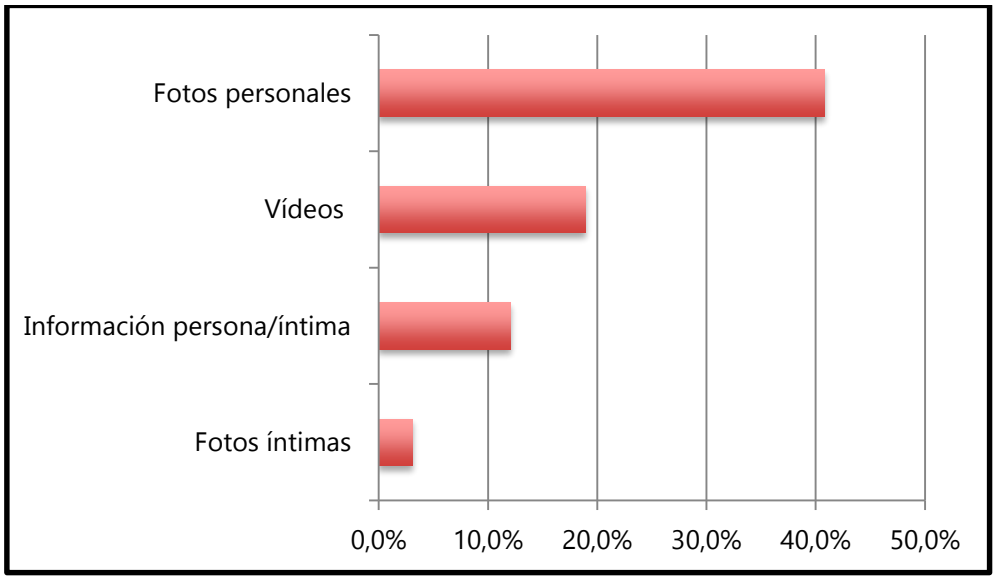


Ilustración 18. Tipo de información contenida en el ordenador con el que se conecta a Internet

e. Información contenida en el móvil con el que se conectan a Internet

Los participantes, sin embargo, guardan más información en el móvil que en el ordenador. El porcentaje es de 58,2% cuando se trata de dispositivos móviles frente al 49,1% del ordenador.

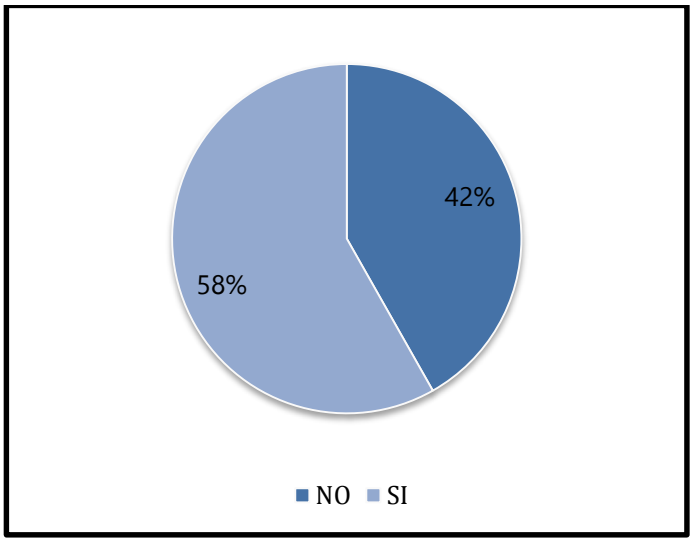


Ilustración 19. Guardar información o archivos en el móvil con el que se conectan a Internet

Del mismo modo que con el ordenador, se les ha preguntado el tipo de información contenida en el móvil con el que se conectan a Internet. De nuevo, el tipo de información que más guardan son fotos personales, pero en este caso el porcentaje es superior (50,3%). Del mismo modo, el resto de ítems también presentan porcentajes superiores: un 26,4% guarda vídeos en el móvil, un 16,8% guarda información personal o íntima, y, finalmente, llama la atención el porcentaje elevado de fotos íntimas que se sitúa en un 8,6%.

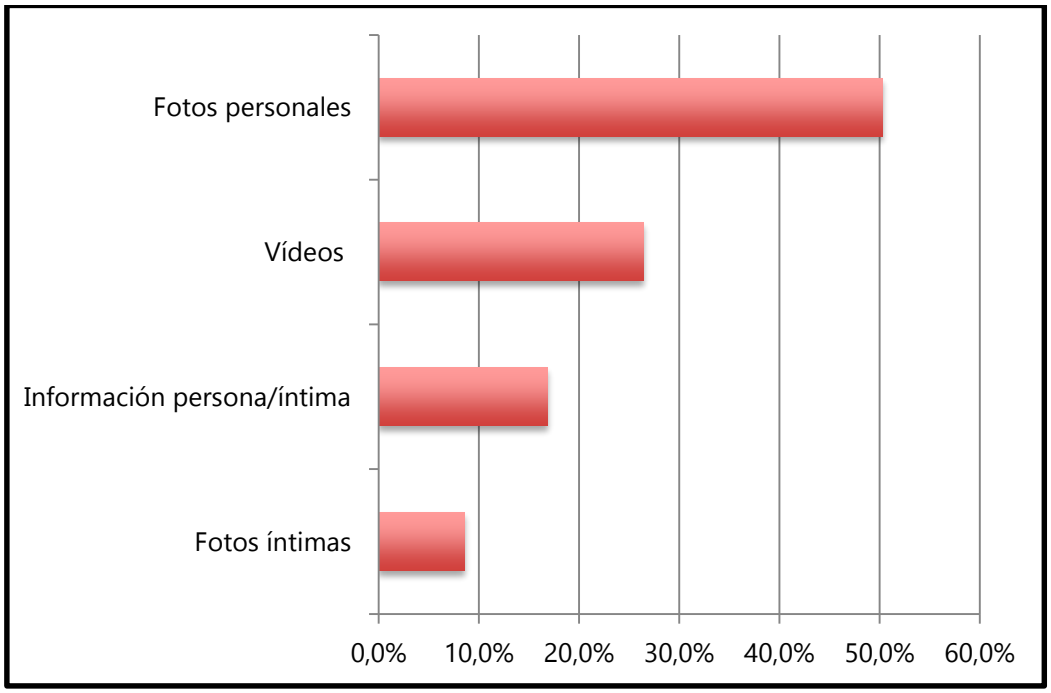


Ilustración 20. Tipo de información contenida en el ordenador con el que se conectan a Internet

f. Uso otorgado al móvil con el que se conectan a Internet

Los sujetos del estudio usan principalmente el teléfono móvil para contactar con personas conocidas (80%). Pero ese no es el único uso que otorgan, también observamos que un 21,9% de la muestra lo usa como medio para cotillear, un 16,1% para ligar y un 13,5% para conocer personas nuevas. Es decir, para contactar con desconocidos.

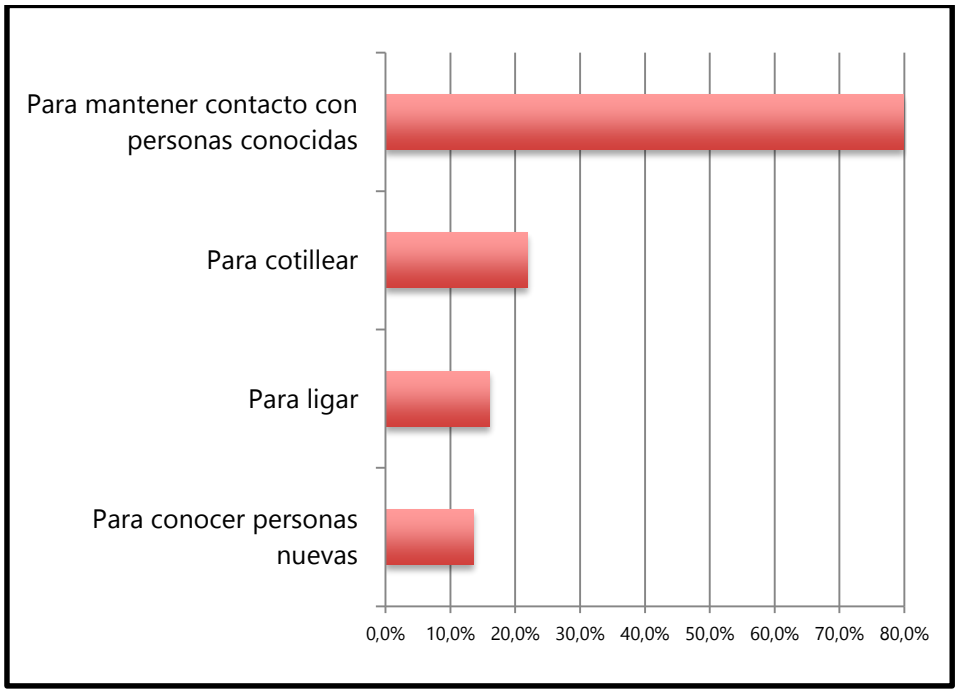


Ilustración 21. Uso otorgado al móvil

g. Número de correos electrónicos recibidos al día

Una de las herramientas de comunicación que ofrece Internet, y que es empleada por los jóvenes es el correo electrónico. Aproximadamente un 65% de la muestra hace uso de él. No obstante, los jóvenes no hacen un uso excesivo. Como se puede observar en la tabla de estadísticos, el percentil 50 se sitúa en el valor 2 (de 1 a 3 correos), concretamente en 1,78 correos, por lo que la mitad de muestra recibe menos de dos correos al día. Analizando los intervalos, observamos que el 35% recibe entre 1 y 3 correos al día, un 13% entre 4 y 7 correos, un 7% entre 8 y 15 correos, y sólo un 9% recibe más de 15 correos al día.

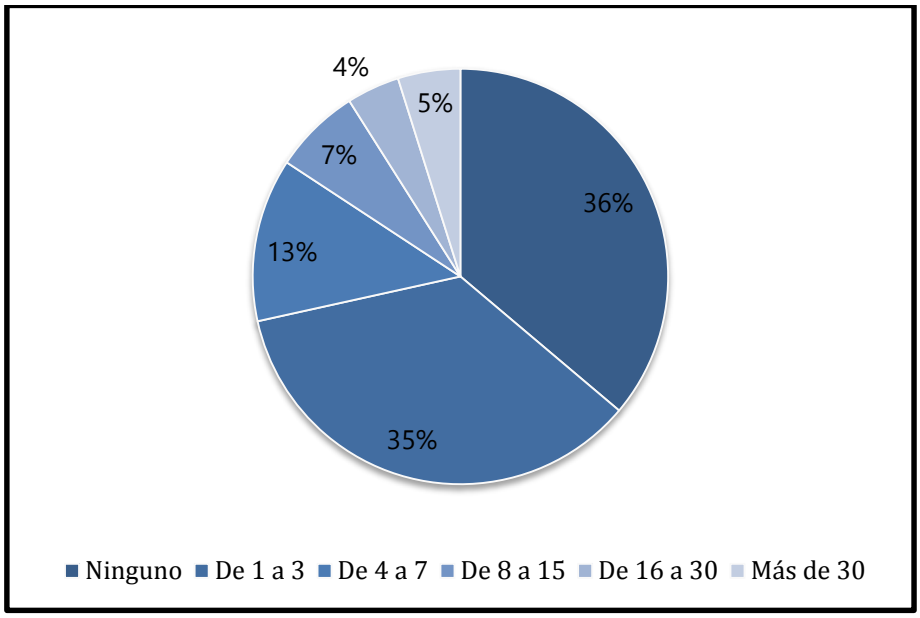


Ilustración 22. Número de correos recibidos al día

Tabla 11. Estadísticos de la variable número de correos recibidos al día

Estadísticos		
Desv. típ.		1,36
Varianza		1,86
Mínimo		1,00
Máximo		6,00
Percentiles	25	1,00
	50	2,00
	75	3,00

h. Horas a la semana dedicadas a chatear.

Otro de los medios que se ha convertido en popular entre los jóvenes, para la comunicación personal, son las salas de chat. Como se puede observar, sólo el 16% no chatea. El percentil 50 se sitúa en el valor 3, concretamente en 2,7 horas, por lo que podemos afirmar que el 50% de la muestra dedica unas 2,7 horas a chatear a la semana. Analizándolo a partir de los intervalos, se observa como el 29% chatea menos de 1 hora a la semana, un 25% chatea entre 1 y 3 horas, 15% entre 4 y 7 horas y el resto, un 15%, dedica más de 8 horas a la semana a chatear.

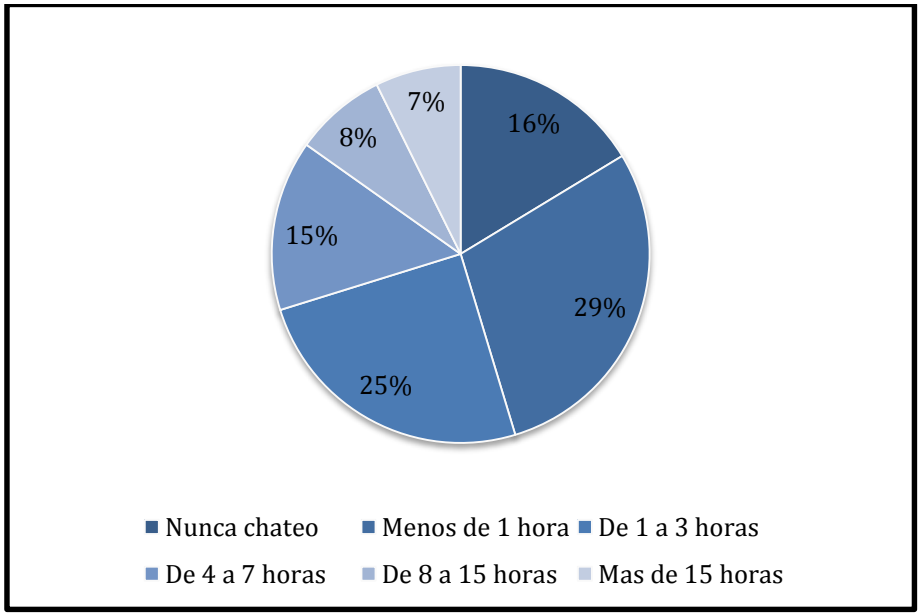


Ilustración 23. Horas a la semana dedicadas a chatear

Tabla 12. Estadísticos de la variable horas a la semana dedicadas a chatear

Estadísticos		
Desv. típ.		1,43
Varianza		2,06
Mínimo		1,00
Máximo		6,00
Percentiles	25	2,00
	50	3,00
	75	4,00

i. Horas al día dedicadas a las redes sociales.

Pero, de todos los medios actuales que dispone Internet para la comunicación personal, son las redes sociales los que más usan los jóvenes. Tal y como se demuestra en la gráfica, el 92% de los sujetos de la muestra usa las redes sociales. De forma concreta, algo más del 57% usa las redes sociales hasta tres horas al día. Hay un alto porcentaje, el 21%, que le dedica a las redes sociales entre 4 y 7 horas y un 14%, que le dedica más de 8 horas al día.

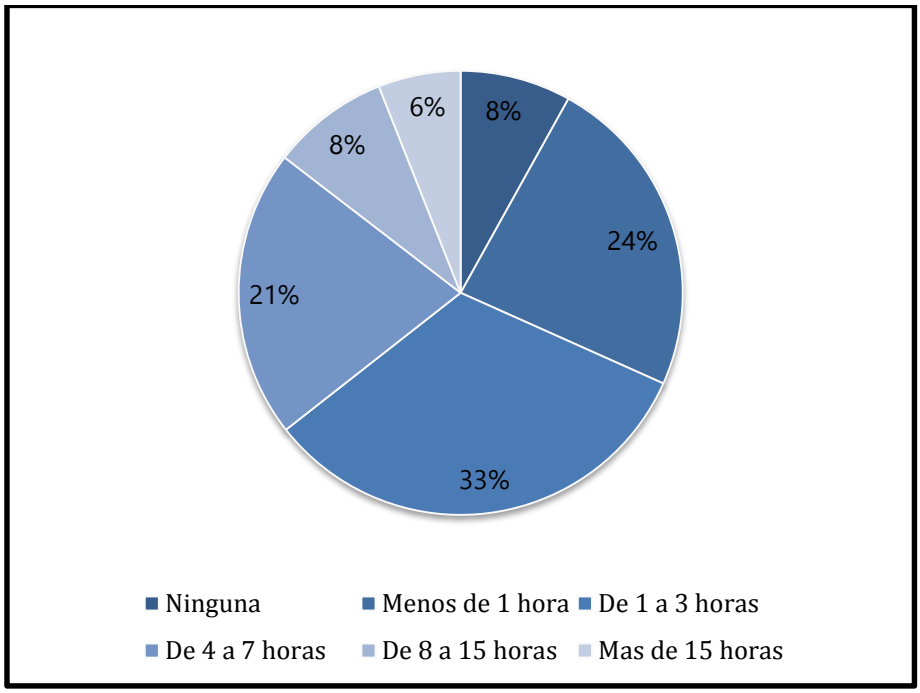


Ilustración 24. Horas al día dedicadas a las redes sociales

Tabla 13. Estadísticos de la variable horas al día dedicadas a las redes sociales

Estadísticos		
Desv. típ.		1,28
Varianza		1,63
Mínimo		1,00
Máximo		6,00
Percentiles	25	2,00
	50	3,00
	75	4,00

j. Número de cuentas abiertas de redes sociales usando datos personales reales.

Analizando el número de cuentas que los participantes en el estudio han abierto usando datos personales reales, observamos que el número varía de un perfil a otro en más de diez. Si observamos los datos de manera detallada, vemos que el 28% de la muestra tan sólo tiene un perfil, un 17,6% dos y un 18,2% tres. El resto de la muestra, un 36,2%, tiene más de cuatro perfiles.

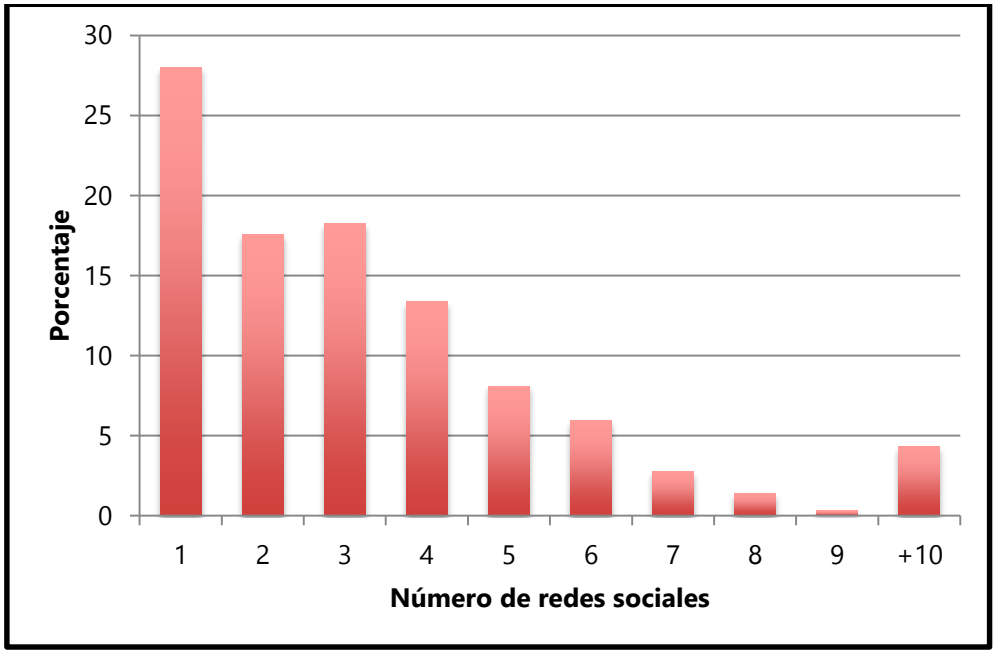


Ilustración 25. Número de cuentas abiertas de redes sociales usando datos reales

Tabla 14. Estadísticos de la variable número de cuentas de redes sociales

Estadísticos		
Desv. típ.		2,90
Varianza		5,25
Mínimo		1,00
Máximo		10,00
Percentiles	25	1,00
	50	3,00
	75	4,00

k. Uso empleado de las redes sociales.

La gran parte de los sujetos de la muestra usan las redes sociales como medio para mantener contacto con personas conocidas (87,5%). Del mismo modo, hay un 73,9% de la muestra que lo emplea como herramienta para quedar con los amigos y un 31,1% para organizar fiestas y actividades. Sin embargo, éstos no son los únicos usos que le dan a las redes sociales, también hay un 30,6% que las emplea para cotillear, un 26,1% para conocer a personas nuevas, es decir, desconocidos, un 26% que las usa para jugar y, finalmente, hay un 17,6% que las emplea como medio para ligar.

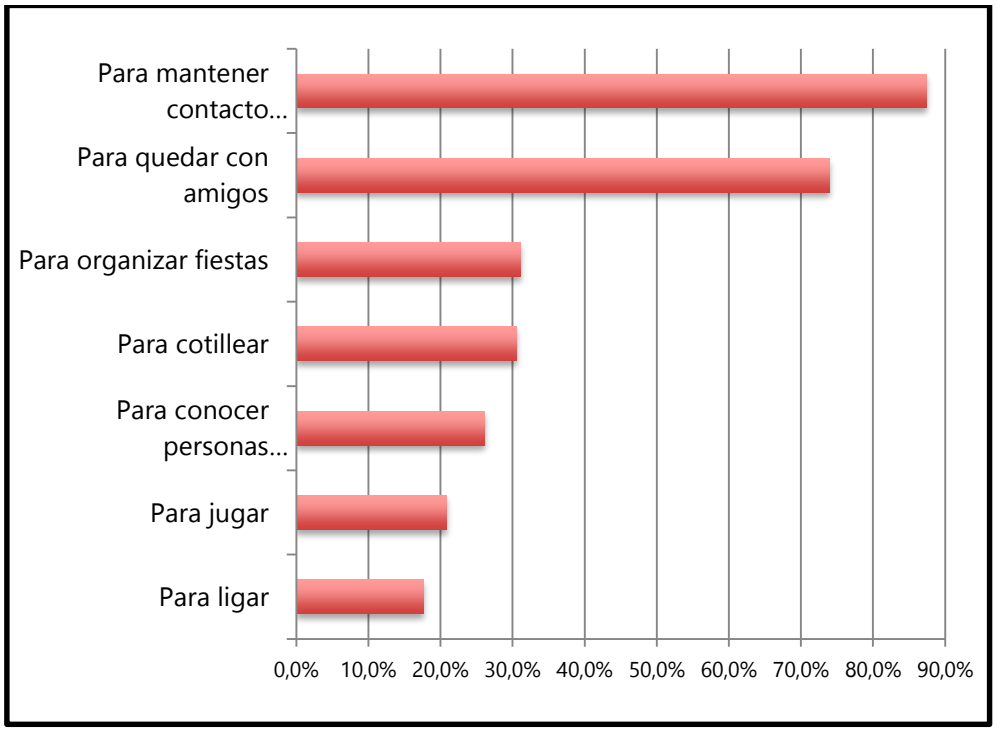


Ilustración 26. Uso empleado a las redes sociales

l. Personas que agregan a los perfiles de redes sociales.

Entre las personas que agregan los jóvenes a sus redes sociales encontramos que, casi la totalidad de ellos agregan a conocidos. De forma detallada, el 89,8% agrega a sus compañeros de clase, un 79,4% agrega a compañeros de otras clases (del colegio), un 64,1% a compañeros de actividades extraescolares, y un 43,2% agrega a amigos de sus amigos. Respecto a los familiares, un 56,6% agrega a sus hermanos, un 53,9% a otros familiares como tíos o primos y un 30,7% a los padres. Finalmente, un 30,7% agrega a desconocidos.

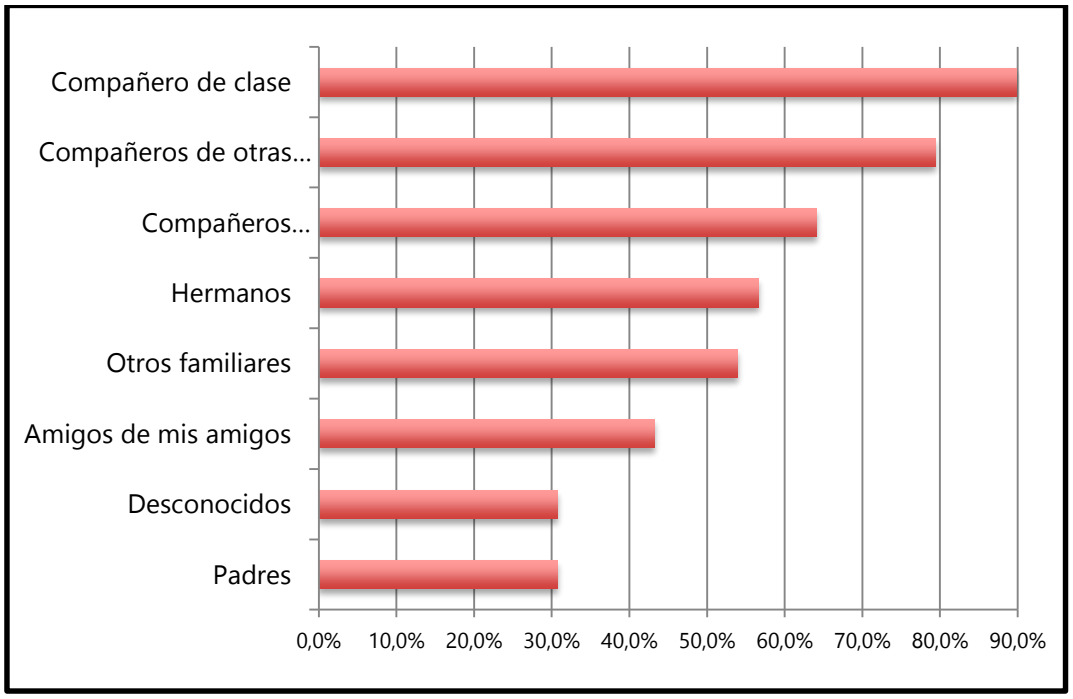


Ilustración 27. Personas que agregan a las redes sociales

m. Poseer un blog propio

Otra de las herramientas que ofrece Internet y que también es usada por los jóvenes, son los blogs. Sin embargo, esta herramienta es poco utilizada si se compara con otras antes mencionadas, pues tan sólo hacen uso de ella un 15% de la muestra.

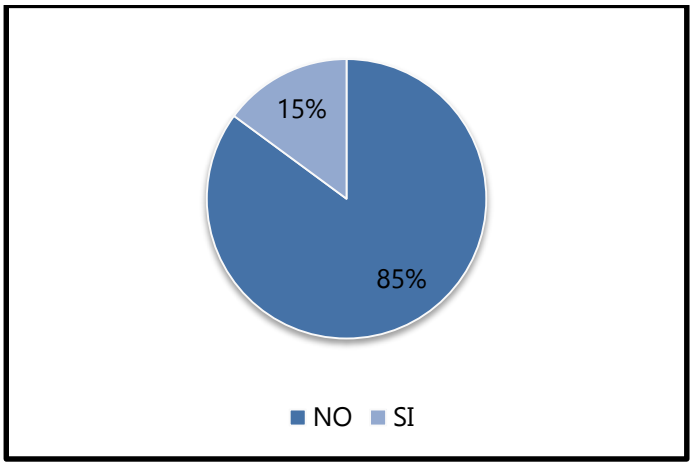


Ilustración 28. Poseer un blog propio

n. Escribir en blogs o foros ajenos

Del mismo modo, los jóvenes también escriben en blogs y foros creados por otras personas, pero vemos que el porcentaje de uso de esta forma de comunicación se sitúa en un 17%, similar a los que tienen un blog propio.

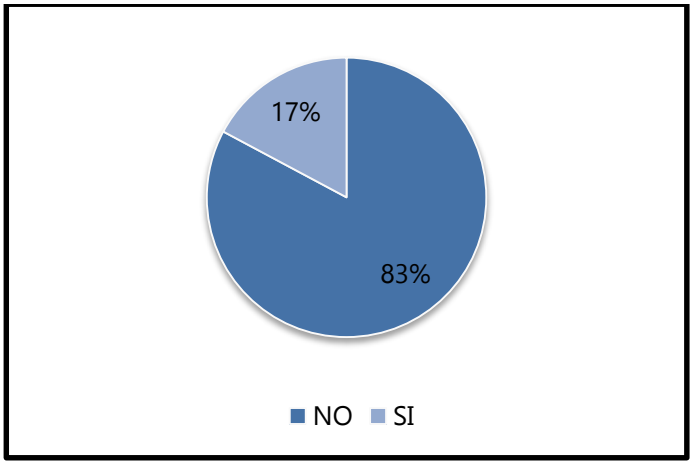


Ilustración 29. Escribir comentarios en blogs o foros ajenos

o. Realizar videoconferencias o videollamadas.

Respecto a la realización de videoconferencias o videollamadas, tan sólo un 26% de la muestra usa este medio para comunicarse con otras personas, de los cuales, un 16% lo emplea durante menos de una hora a la semana, un 7% entre una y tres horas, y tan sólo un 3% lo usa más de tres horas a la semana.

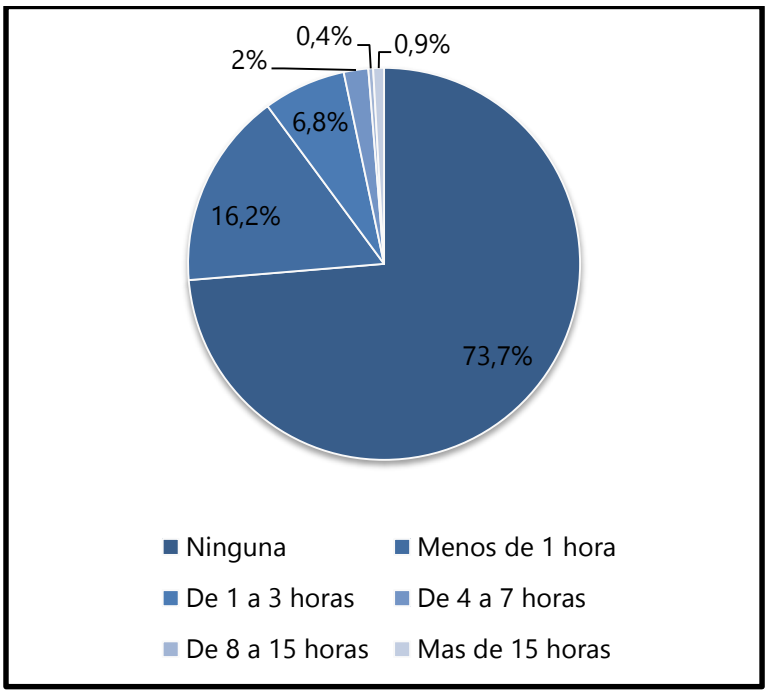


Ilustración 30. Horas a la semana dedicadas a hacer videoconferencias o videollamadas

Tabla 15. Estadísticos de la variable realizar videoconferencias o videollamadas

Estadísticos		
Desv. típ.		0,85
Varianza		0,73
Mínimo		1,00
Máximo		6,00
Percentiles	25	1,00
	50	1,00
	75	2,00

p. Horas a la semana dedicadas a jugar a videojuegos *online* con el ordenador.

Aproximadamente, el 53% de la muestra juega a videojuegos *online* a través del ordenador. De forma concreta, se puede observar como el 24% emplea menos de una hora a tal fin, frente a un 16% que lo hace entre una y tres horas, y un 13% que le dedica más de tres horas.

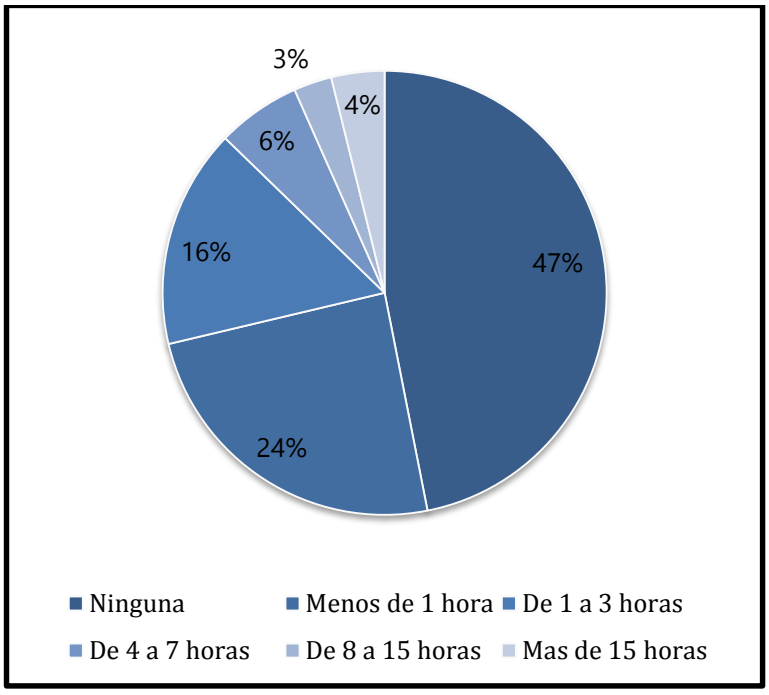


Ilustración 31. Horas a la semana dedicadas a jugar a videojuegos *online* con el ordenador

Tabla 16. Estadísticos de la variable horas dedicadas a jugar a videojuegos *online* con el ordenador

Estadísticos		
Desv. típ.		0,85
Varianza		0,73
Mínimo		1,00
Máximo		6,00
Percentiles	25	1,00
	50	1,00
	75	2,00

q. Horas a la semana dedicadas a jugar a videojuegos *online* con el móvil.

El porcentaje de jugadores aumenta cuando el medio empleado es el teléfono móvil. De forma concreta, el 30% de la muestra le dedica menos de una hora a la semana jugar, un 19% le dedica entre 1 y 3 horas, y un 15% le dedica más de 3 horas.

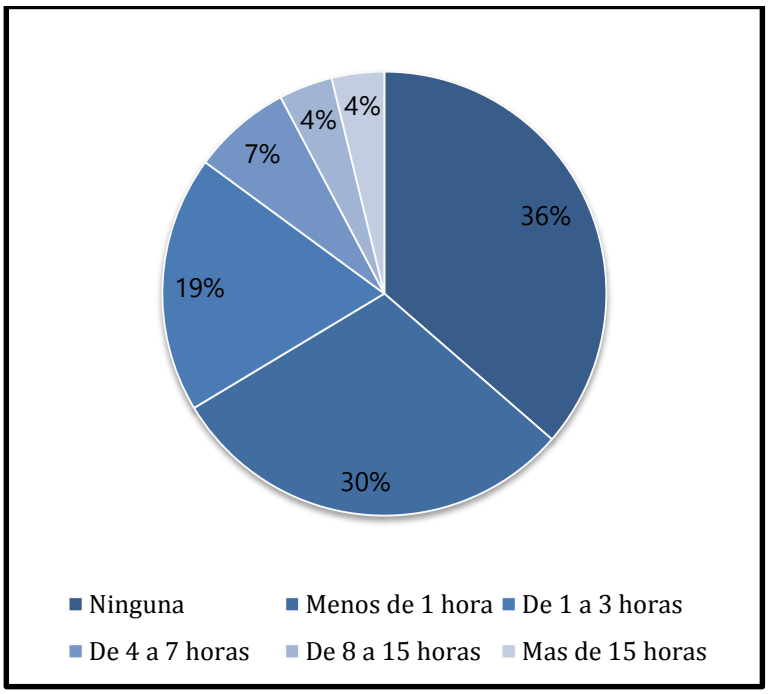


Ilustración 32. Horas a la semana dedicadas a jugar a videojuegos *online* con el móvil

Tabla 17. Estadísticos de la variable horas dedicadas a jugar a videojuegos *online* con el móvil

Estadísticos		
Desv. típ.		1,32
Varianza		1,75
Mínimo		1,00
Máximo		6,00
Percentiles	25	1,00
	50	2,00
	75	3,00

r. Chatear a través de los videojuegos *online.*

En muchas ocasiones los videojuegos *online* disponen de chats que permiten establecer comunicación entre los jugadores. En el presente estudio, el 27% de la muestra afirma que utiliza los videojuegos *online* para hablar (chatear) con otros jugadores.

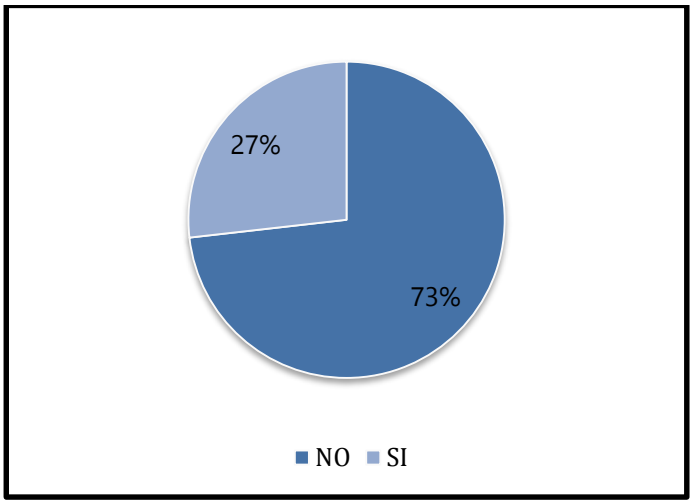


Ilustración 33. Chatear a través de videojuegos *online*

s. Contactar con desconocidos a través de Internet.

Una de las preguntas que se les realizó a los participantes fue si habían contactado con desconocidos a través de Internet. Como se puede observar en el gráfico, un 62% nunca ha contactado con desconocidos, mientras que un 38% si lo ha hecho.

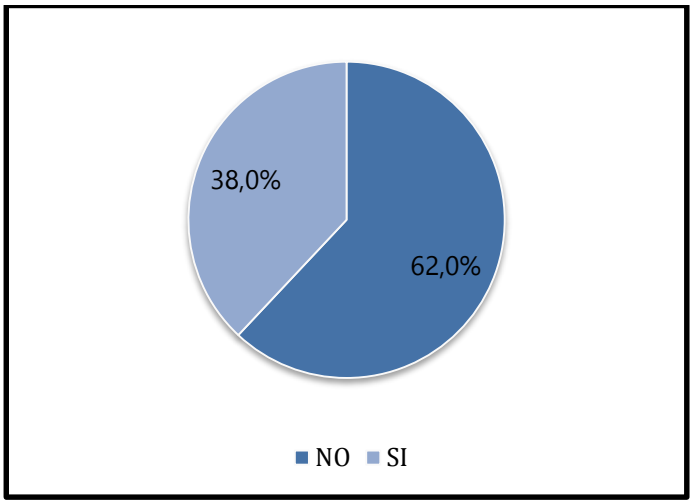


Ilustración 34. Contactar con desconocidos a través de Internet

t. Medio usado para contactar con desconocidos a través de Internet.

Tras haber constatado que los participantes en el estudio contactan con desconocidos a través de Internet, se le preguntó por el medio empleado para tal fin. Aunque no existe mucha diferencia entre las respuesta, un 10,5% ha contestado que lo ha hecho a través de mensajería instantánea, un 9,3% a través de los chats que ofrecen los videojuegos *online* y un 5,9% a través de salas de chat.

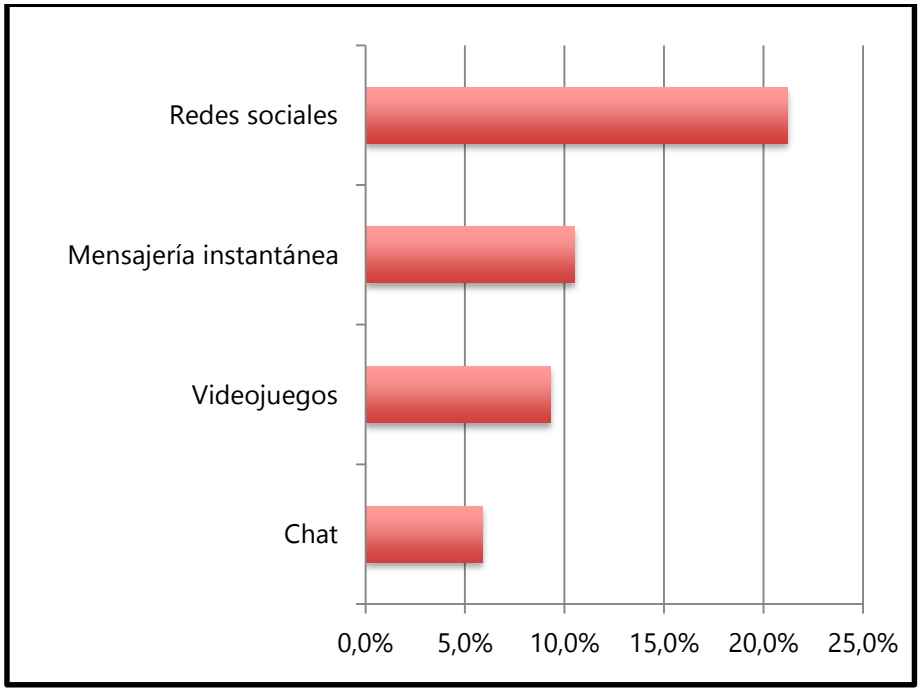


Ilustración 35. Medio usado para contactar con desconocidos a través de Internet

u. Motivo por el que contactan con desconocidos a través de Internet.

También se les preguntó por el motivo por el que contactan con desconocidos. El principal motivo es para mantener una relación de amistad (23,1%), pero también lo hacen para jugar (15,8%) y, en menor medida, para mantener relaciones sentimentales (6,3%).

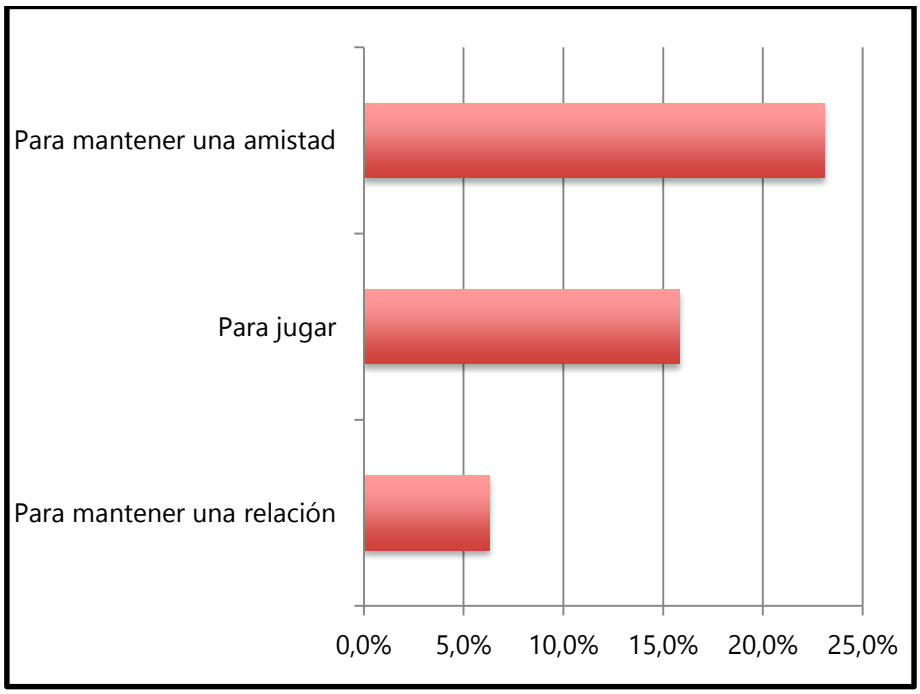


Ilustración 36. Motivo por el que contactan con desconocidos

v. Sexting.

También se le ha preguntado a los estudiantes por la práctica del *sexting.* El porcentaje de muestra que afirma haberse hecho alguna vez una foto o vídeo comprometido (íntimo), y después se lo ha

enviado a alguien a través de móvil o Internet, se sitúa en un 9%, frente a un 91% que nunca ha realizado esta práctica.

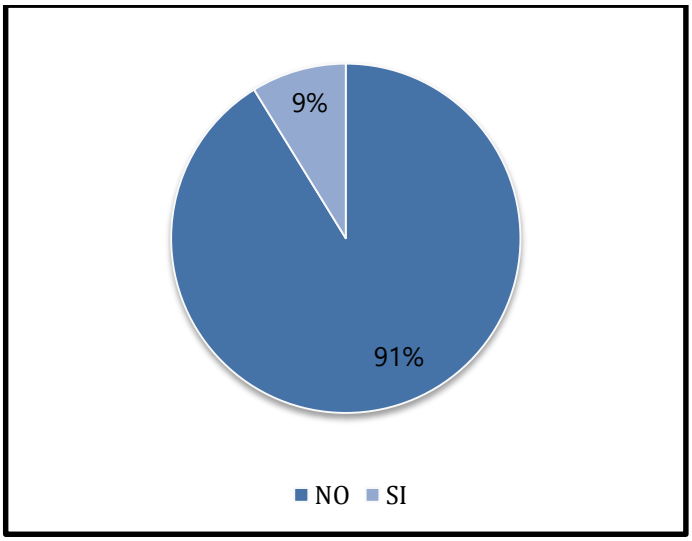


Ilustración 37. Sexting

w. Comportamiento desviado.

En otro orden, también se preguntó a los participantes en el estudio si habían realizado alguna vez conductas de ciberacoso, tanto en su forma continuada como con actos concretos. Los resultados arrojaron que un 28,7% de la muestra afirma haber acosado de manera continuada a alguna persona a través de Internet. De forma concreta, un 22,8% ha insultado o ridiculizado a alguien de forma repetida, un 9,5% ha difundido rumores o mentiras sobre alguien de forma repetida para hacerle daño, un 5,8% ha contactado con alguien de forma repetida a través de Internet tras haberle pedido esa persona que no

lo hiciera y, finalmente, un 4,7% ha utilizado Internet para marginar o excluir de manera continuada a alguien.

En cuanto al ciberacoso no continuado, se constata que es menos practicado por los sujetos de la muestra pues el porcentaje se sitúa en un 21%. Sin embargo, estas conductas, pese a que se realizan una sola vez, puede ser consideradas más graves pues pueden llegar a tener consecuencias mayores. Analizando los porcentajes de las conductas aisladas, observamos que el 11,9% ha difundido alguna vez información secreta o íntima de otra persona a través de Internet sin el consentimiento de la persona, un 11,5% ha amenazado alguna vez de forma grave a otra persona a través de Internet, un 7,1% ha suplantado la identidad de otra persona para hacerle daño al menos una vez; y, finalmente, un 1,7% ha obligado con violencia o intimidación a alguien a hacer algo que no quería a través de Internet o el móvil.

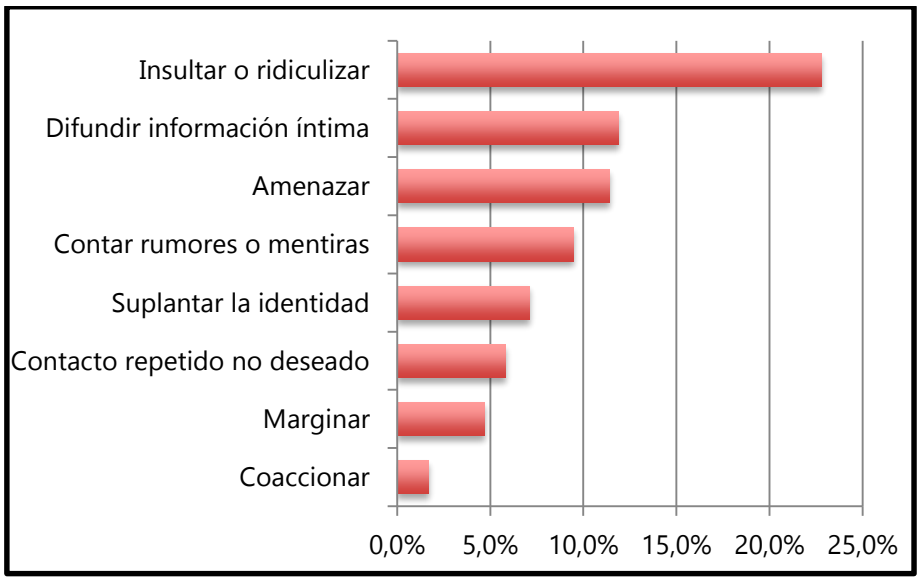


Ilustración 38. Comportamiento desviado

x. Compartir el ordenador con otras personas.

A los estudiantes se les preguntó acerca de si comparten el ordenador con otras personas. Los resultados muestran que el 24,9% de la muestra no comparte el ordenador, frente a un 60,5% que lo comparte con los padres, un 51,6% que lo comparte con los hermanos y un 7,3% que lo comparte con otros familiares.

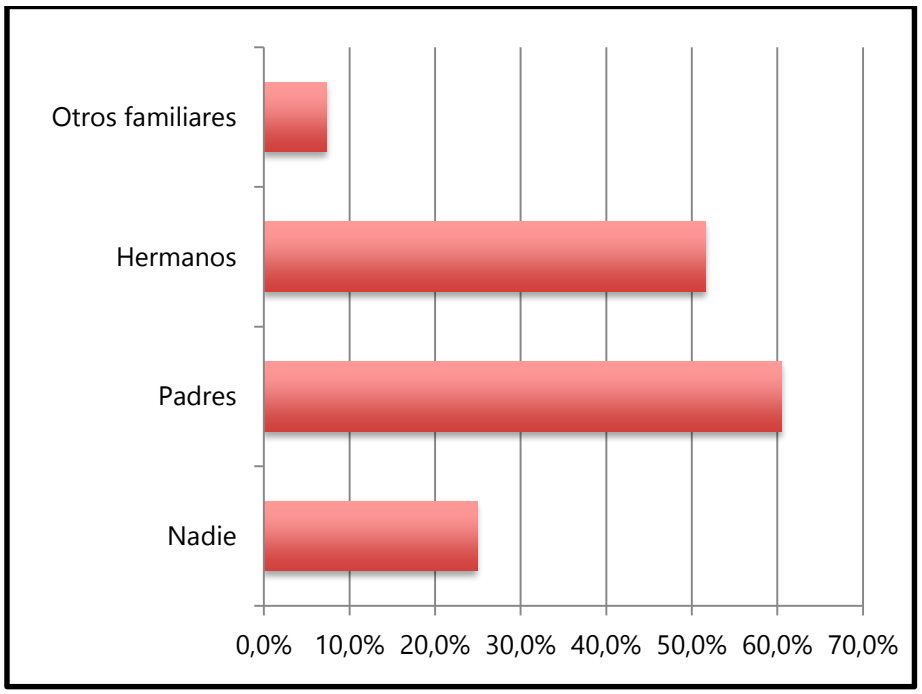


Ilustración 39. Compartir el ordenador

y. No limitar el acceso a los perfiles de redes sociales.

En cuanto a la limitación de acceso a los perfiles de redes sociales, el 78% de los sujetos de la muestra que usan redes sociales afirman que sí limitan el acceso a sus cuentas, frente a un 22% que no lo hace, de forma que cualquier persona puede acceder al contenido publicado en su perfil.

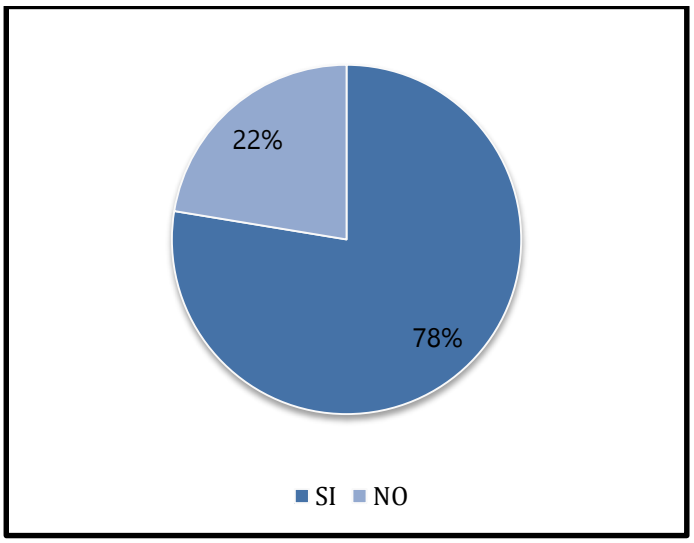


Ilustración 40. Limitar el acceso a las redes sociales

z. No comunicar a los padres el uso de las redes sociales.

Del mismo modo, también se le preguntó a los estudiantes que hacen uso de las redes sociales por el hecho de comunicar a los padres la tenencia de perfiles. El 98% de ellos contestó de manera afirmativa, es decir, que sus padres tienen conocimiento sobre la existencia de sus perfiles en redes sociales, frente a un 2% que no lo sabe.

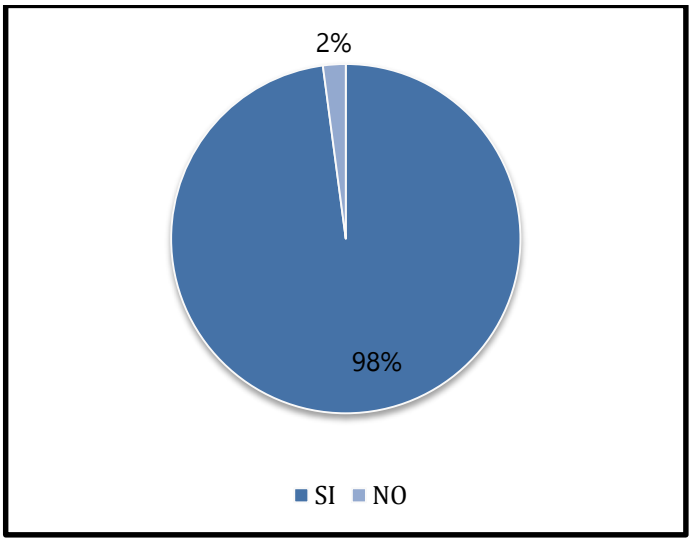


Ilustración 41. Comunicar a los padres el uso de las redes sociales

aa. No control de los padres sobre el uso del ordenador y del móvil.

Finalmente, se les preguntó a los estudiantes si los padres ejercían algún tipo de control sobre el uso que realizan del ordenador y del móvil. Los resultados muestran que se realiza un mayor control sobre el ordenador que sobre el móvil. No obstante, los porcentajes de control son inferiores a los de no control. Es decir, sólo un 27,3% afirma que sus padres controlan lo que realizan con el ordenador y un 17,7% lo que hacen con el móvil.

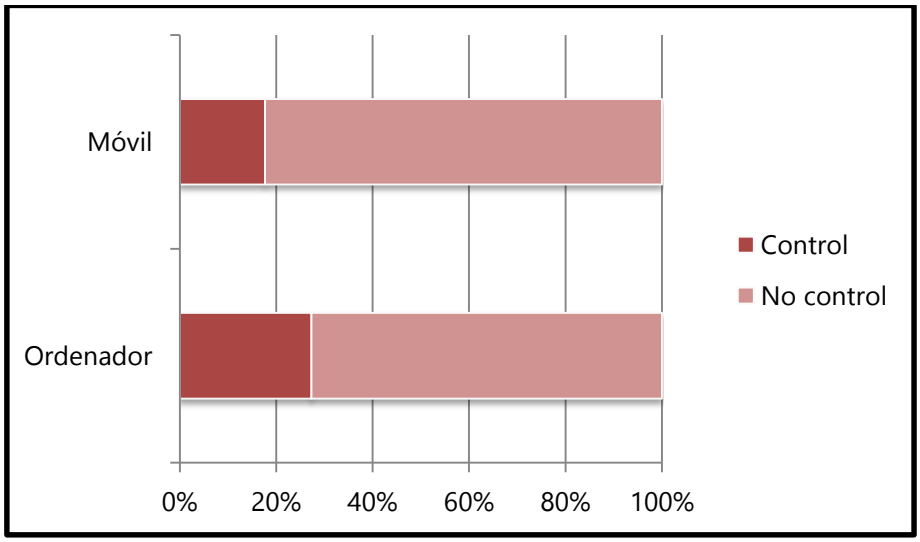


Ilustración 42. Control de los padres sobre el uso del ordenador y el móvil

3.2. Análisis de componentes principales

Dado que se cuenta con un número amplio de variables independientes, setenta y nueve en total, se optó por realizar un análisis de componentes principales para datos categóricos (CATPCA). El objetivo de este análisis es reducir el conjunto original de variables independientes a un conjunto más pequeño de componentes no correlacionadas que representen la mayor parte de la información encontrada en las variables originales. Con este análisis, adecuado para las variables categóricas o nominales, se pretende por un lado, encontrar una estructura interna de datos que se corresponda con la estructura teórica; y, por otro, convertir éstas variables en continuas usando el escalamiento óptimo. Esto es así debido a que un índice obtenido del primer componente principal puede interpretarse como la combinación lineal de los indicadores originales, y captura el máximo

de información posible, optimizando la proporción explicada del total de la varianza. Antes de realizar el análisis se optó por transformar las variables de naturaleza ordinal en variables dicotómicas con el objetivo de que todas las variables independientes tuviesen la misma estructura. El valor de referencia que se tomó como punto de corte para establecer las dos categorías fue la mediana. A continuación, se presentan las variables transformadas con las frecuencias y porcentajes de respuesta:

Tabla 18. Variables transformadas para el CATPCA

Variables transformadas	Categorías	Frecuencia	Porcentaje
Número de correos electrónicos recibidos al día	1. <3 correos	1458	71,5
	2. >3 correos	580	28,5
Horas a la semana dedicadas a chatear	1. <3 horas	1428	70,2
	2. >3 horas	606	29,8
Horas al día dedicadas a las redes sociales	1. <3 horas	1309	64,4
	2. >3 horas	723	35,6
Número de cuentas abiertas de redes sociales usando datos personales reales	1. <3 Cuentas	1277	68,2
	2. >3 Cuentas	595	31,8
Realizar videoconferencias o videollamadas	1. No	1505	73,8
	2. Si	533	26,2
Horas a la semana dedicadas a jugar a videojuegos *online* con el ordenador	1. <1 hora	1459	71,6
	2. >1 hora	579	28,4
Horas a la semana dedicadas a jugar a videojuegos *online* con el móvil	1. <1 hora	1360	66,7
	2. >1 hora	678	33,3

Las variables originales fueron agrupadas en once componentes de acuerdo al planteamiento teórico. Las tres primeras componentes hacen referencia a la introducción de bienes en el ciberespacio; es decir, agrupan todos los ítems relacionados con el hecho de hacer a un sujeto presente en el ciberespacio y de trasladar bienes del espacio físico al ciberespacio. Las seis componentes siguientes agrupan todos los ítems relacionados con la interacción; es decir, las acciones que realiza un usuario en el ciberespacio para comunicarse con otras personas y que le hacen más visible. Y finalmente, las dos últimas componentes hacen referencia a las actividades cotidianas que realizan los menores en el ciberespacio que posibilita que los padres y otros familiares puedan vigilar las acciones que realizan los menores, y otros sobre ellos, en Internet.

A continuación, se muestran los resultados obtenidos para las todas componentes principales.

3.2.1. Descripción de las componentes principales

1. Componente 1: Guardar

La primera componente denominada "Guardar", hace referencia a los bienes de un usuario que están disponibles en el ciberespacio y que, por lo tanto, son susceptibles de ataque por el hecho de guardarlos en los dispositivos con los que se conectan a Internet. Es decir, son las fotos, videos y demás información personal que se guarda en los móviles y los ordenadores con los que se conectan a Internet.

Esta componente está formada por ocho ítems, resume el 42,7% de la información contenida en las variables originales, y tiene un nivel de consistencia interna de 0,81.

Tabla 19. Resumen del modelo. Guardar

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,809	3,423	42,784
Total	,809	3,423	42,784

Tanto en la tabla como en la representación gráfica de saturación en componentes, se observa como la escala muestra unidimensionalidad presentando índices altos de saturación en todos los ítems en el componente principal, con puntuaciones mayores de 0,4.

Tabla 20. Saturación en componentes. Componente guardar

	Dimensión 1
Guardar en el ordenador/*tablet* fotos	,738
Guardar en el ordenador/*tablet* fotos íntimas	,476
Guardar en el ordenador/*tablet* videos	,721
Guardar en el ordenador/*tablet* videos	,580
Guardar en el móvil fotos	,745
Guardar en el móvil fotos íntimas	,491
Guardar en el móvil videos	,768
Guardar en el móvil información personal o íntima	,639

Normalización principal por variable.

Ilustración 43. Saturación en componentes. Guardar

2. Componente 2: Facilitar información personal real a través de Internet

La segunda componente hace referencia al tipo de información que los menores facilitan a través de Internet como el nombre, apellidos, fotos, etc. En total, esta nueva variable explica el 54,98% de la varianza de los diez ítems relativos a la información cedida por los menores y tiene una consistencia interna de 0,909.

Tabla 21. Resumen del modelo. Facilitar información personal real a través de Internet

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,909	5,498	54,982
Total	,909	5,498	54,982

Tal y como se puede observar en la tabla de saturación en componentes, todos los ítems presentan un índice de saturación alto, por encima de 0,5. La escala muestra unidimensionalidad para todas las medidas.

Tabla 22. Saturación en componentes. Facilitar información personal real a través de Internet

	Dimensión 1
He dado el nombre	,851
He dado los apellidos	,848
He dado el teléfono	,791
He dado fotos mías	,725
He dado el correo electrónico	,759
He dado el nombre del colegio	,718
He dado mi ubicación	,618
He dado mi dirección	,592
He dado mi edad	,827
He dado mi estado civil	,630

Normalización principal por variable.

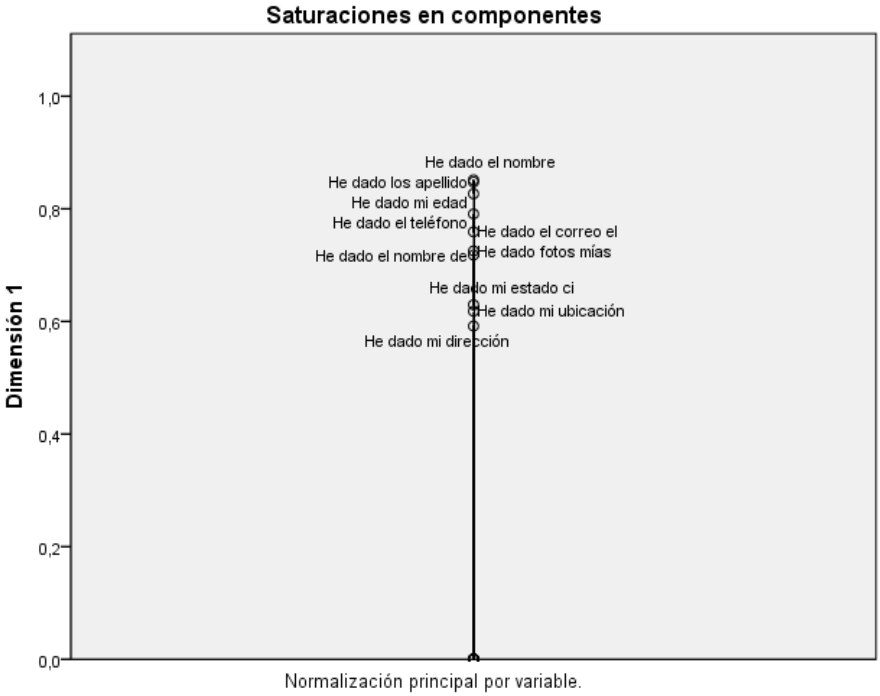


Ilustración 44. Saturación en componentes. Facilitar información personal real a través de Internet

3. Componente 3: Medios usados para facilitar información personal real

La tercera componente también hace referencia la introducción de datos en el ciberespacio, pero en esta ocasión relativo a los medios empleados para tal fin. En concreto, se han incluido cuatro de los seis ítems registrados inicialmente en la encuesta, ya que las opciones "facilitar datos personales reales a través de las salas de chat" y "facilitar datos personales reales a través de los foros" presentan frecuencias muy bajas, tal como se comprobó en el análisis exploratorio. La consistencia interna de la componente es de 0,610 y la varianza explicada es de un 46,1%.

Tabla 23. Resumen del modelo. Medios usados para facilitar información personal real

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,610	1,842	46,054
Total	,610	1,842	46,054

Tanto en la tabla, como en la representación gráfica, se puede comprobar la unidimensionalidad de la escala, y cómo todos los componentes saturan por encima de 0,6, salvo en el caso de ceder los datos a través de las páginas de videojuegos (cuyo valor alcanza 0,37, pero que se ha optado por mantener por su relevancia teórica).

Tabla 24. Saturación en componentes. Medios usados para facilitar información personal real

	Dimensión 1
Dar datos personales a través del correo electrónico	,657
Dar datos personales a través de la mensajería instantánea	,790
Dar datos personales a través de redes sociales	,802
Dar datos personales a través de páginas de videojuegos	,377

Normalización principal por variable.

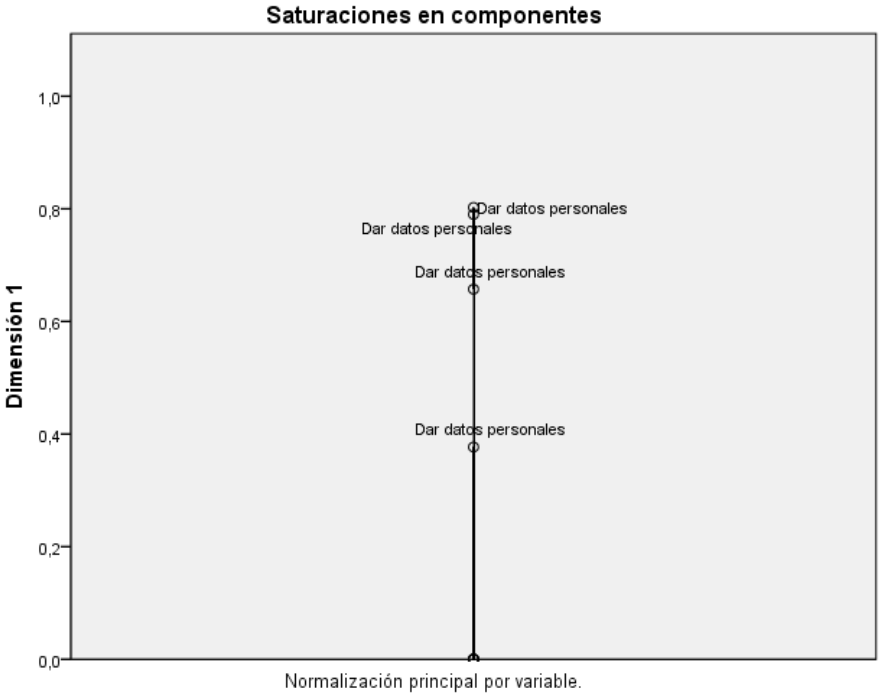


Ilustración 45. Saturación en componentes. Medios usados para facilitar información personal real

4. Componente 4: Comportamiento desviado en el ciberespacio

La cuarta componente se ha denominado comportamiento desviado en el ciberespacio porque aglutina todos los ítems relativos al ciberacoso continuado y no continuado, es decir, que los menores hayan insultado, marginado, contactado de manera repetida o ridiculizado a otra persona a través de la Red, y haber realizado amenazas, difundido información personal, coaccionado o suplantado la identidad con el ánimo de hacer daño. También se ha incluido en esta componente el hecho de haberse fotografiado o grabado en vídeo en situación comprometida, y después haberlo cedido a otra persona

a través de Internet (*sexting*). Esta componente explica el 35,5% de la varianza y tiene una consistencia interna de 0,772.

Tabla 25. Resumen del modelo. Comportamiento desviado en el ciberespacio

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,772	3,187	35,415
Total	,772	3,187	35,415

De acuerdo con la tabla de saturación de componentes y su representación gráfica, podemos observar la unidimensionalidad de la escala, y que todos los ítems tienen saturaciones altas (superiores a 0,5) salvo para la conducta de *sexting,* que se opta por mantener, dado que la literatura científica ha demostrado que se trata de un comportamiento que facilita la aparición de conductas de cibervictimización.

Tabla 26. Saturación en componentes. Comportamiento desviado en el ciberespacio

	Dimensión 1
Haber hecho *sexting* al menos una vez	,359
Haber insultado de manera repetida a través de Internet	,622
Haber contado rumores falsos sobre otra persona de manera repetida a través de Internet	,623
Haber contactado de manera repetida a otra persona a través de Internet tras haberle pedido que no lo hiciera	,574
Haber marginado de manera repetida a otra persona a través de Internet	,601
Haber difundido información personal de otra persona a través de Internet	,629
Haber amenazado a otra persona a través de Internet	,668
Haber coaccionado a otra persona a través de Internet	,591
Haber suplantado a otra persona a través de Internet	,634

Normalización principal por variable.

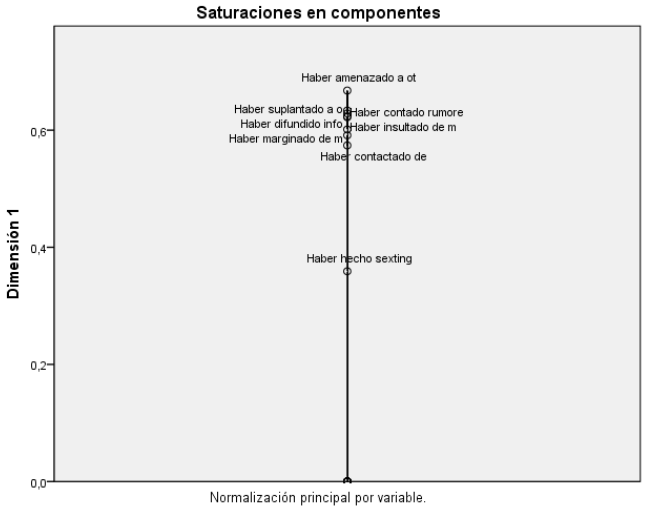


Ilustración 46. Saturación en componentes. Comportamiento desviado en el ciberespacio

5. Componente 5: Uso de herramientas de comunicación

La quinta componente reúne todos los ítems relativos al uso de herramientas de comunicación, tales como el uso del correo electrónico, salas de chat, redes sociales, foros, blogs, etc. La consistencia interna de la escala es 0,61 y la varianza explicada es de 20,41%.

Tabla 27. Resumen del modelo. Uso de herramientas de comunicación

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,610	2,245	20,406
Total	,610	2,245	20,406

La escala muestra unidimensionalidad como se puede ver en el gráfico y todos los ítems saturan por encima de 0,3.

Tabla 28. Saturación en componentes. Uso de herramientas de comunicación

	Dimensión 1
Recibir más de 3 correos al día	,422
Horas a la semana dedicadas a chatear	,493
Horas al día dedicadas a las redes sociales	,388
Número de cuentas abiertas usando datos reales	,310
Tener un blog propio	,361
Escribir comentarios en blog o foros ajenos	,513
Realizar videoconferencias o videollamadas	,505
Horas a la semana dedicadas a jugar a videojuegos *online* con el ordenador	,556
Horas a la semana dedicadas a jugar a videojuegos *online* con el móvil	,416
Chatear a través de videojuegos	,530
Usar las redes sociales para jugar	,405

Normalización principal por variable.

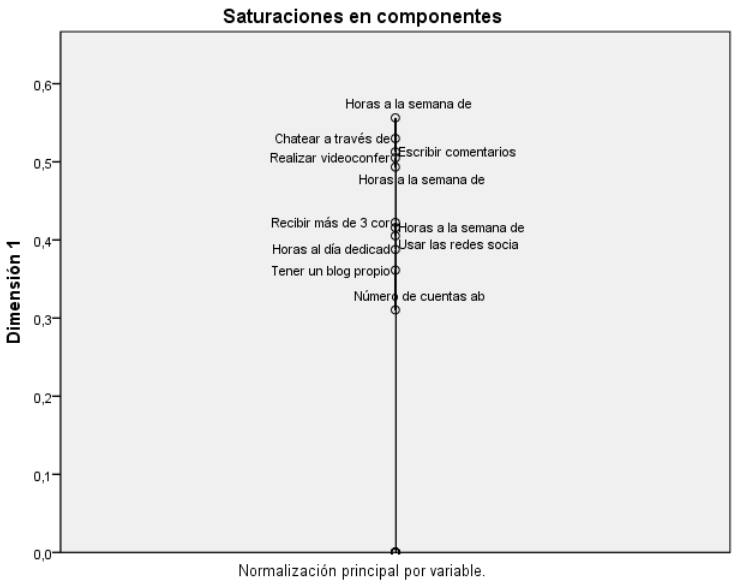


Ilustración 47. Saturación en componentes. Uso de herramientas de comunicación

6. Componente 6: Uso de las TIC para contactar con conocidos

La sexta componente está compuesta por todos los ítems que tienen que ver con el uso de las TIC, por parte de los menores, para mantener contacto con personas conocidas. Esta nueva variable resume el 40,3% de la información contenida de forma conjunta en los ocho ítems, y tiene un nivel de consistencia interna de 0,79.

Tabla 29. Resumen del modelo. Uso de las TIC para contactar con conocidos

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,788	3,221	40,260
Total	,788	3,221	40,260

Tanto en la tabla como en la representación gráfica de saturación en componentes, se observa como la escala muestra unidimensionalidad, presentando índices altos de saturación en todos los ítems en la componente principal, con valores superiores a 0,4. Es conveniente apuntar en este punto, que se ha prescindido de dos variables relativas al contacto con conocidos mediante videoconferencia dado que su saturación era inferior a 0,2.

Tabla 30. Saturación en componentes. Uso de las TIC para contactar con conocidos

	Dimensión 1
Usar el móvil para mantener contacto con conocidos	,418
Usar las redes sociales para organizar fiestas/actividades	,706
Usar las redes sociales para quedar con los amigos	,691
Uso de las redes sociales para mantener contacto con conocidos	,706
Agregar a las redes sociales a los compañeros de clase	,685
Agregar a las redes sociales a otros compañeros de otras clases	,706
Agregar a las redes sociales a compañeros de actividades extraescolares	,629
Agregar a las redes sociales a amigos de los amigos	,456

Normalización principal por variable.

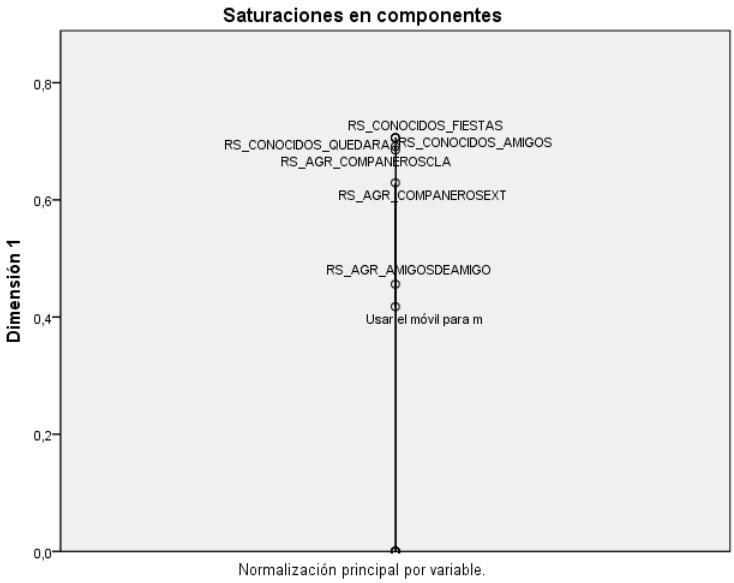


Ilustración 48. Saturación en componentes. Uso de las TIC para contactar con conocidos

7. Componente 7: Uso de las TIC para cotillear

La séptima componente está compuesta por dos ítems que muestran información de la intención de uso por parte de los menores del móvil y de las redes sociales para cotillear sobre otras personas. Esta componente tiene una consistencia interna de 0,8 y resume un 83,51% de la varianza explicada.

Tabla 31. Resumen del modelo. Uso de las TIC para cotillear

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,802	1,670	83,507
Total	,802	1,670	83,507

Ambos ítems quedan incluidos en la misma dimensión y sus saturaciones superan el 0,9.

Tabla 32. Saturación en componentes. Uso de las TIC para cotillear

	Dimensión 1
Usar el móvil para cotillear	,914
Usar las redes sociales para cotillear	,914

Normalización principal por variable.

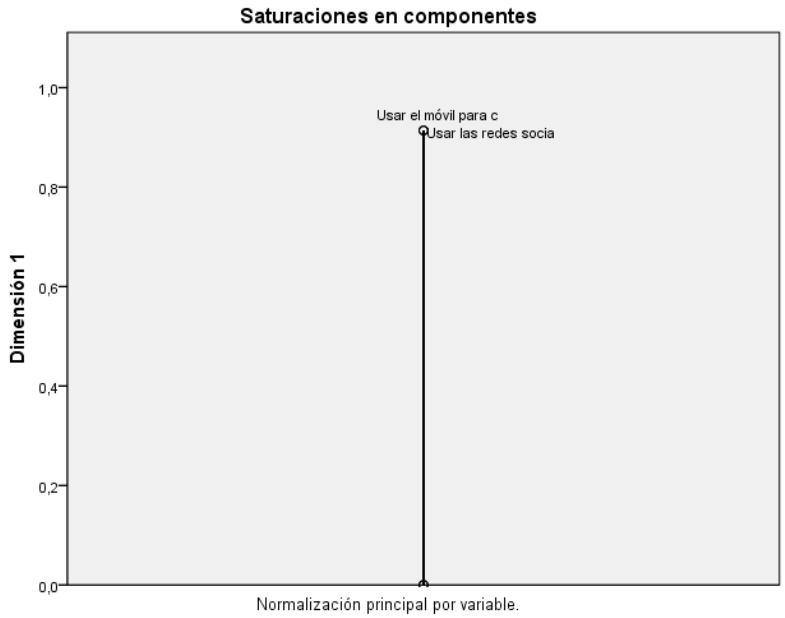


Ilustración 49. Saturación en componentes. Uso de las TIC para cotillear

8. Componente 8: Uso de las TIC para establecer relaciones sentimentales

La octava componente es similar a la anterior pero, en este caso, el objetivo es crear una variable numérica continua sobre el uso de las TIC por parte de los menores para establecer relaciones sentimentales. Esta componente explica el 85% de la varianza de las variables originales y tiene una consistencia interna de 0,82.

Tabla 33. Resumen del modelo. Uso de las TIC para establecer relaciones sentimentales

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,824	1,700	85,016
Total	,824	1,700	85,016

Los ítems incluidos tiene una saturación superior a 0,9 en la componente como se muestra en la siguiente tabla.

Tabla 34. Saturación en componentes. Uso de las TIC para establecer relaciones sentimentales

	Dimensión
	1
Usar las redes sociales para ligar	,922
Usar el móvil para ligar	,922

Normalización principal por variable.

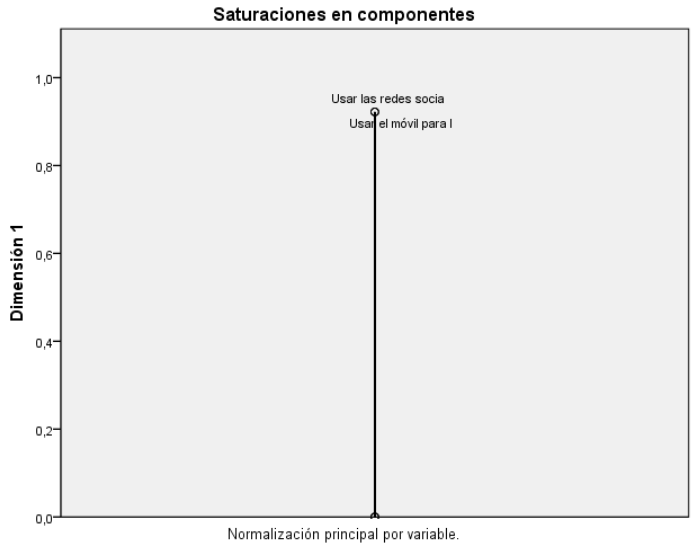


Ilustración 50. Saturación en componentes. Uso de las TIC para establecer relaciones sentimentales

9. Componente 9: Uso de las TIC para contactar con desconocidos

La novena componente reúne todos los ítems que hacen referencia al uso de las TIC por parte de los menores para conocer a personas nuevas, o lo que es lo mismo, para conocer a desconocidos. Incluye tanto las herramientas empleadas para tal fin, como los motivos que les llevan a tal acción. Esta componente explica el 33,9% de la varianza y tiene una consistencia interna de 0,78.

Tabla 35. Resumen del modelo. Uso de las TIC para contactar con desconocidos

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,783	3,391	33,906
Total	,783	3,391	33,906

La mayoría de ítems que la componen tienen una saturación superior a 0,4 salvo dos, usar el móvil para conocer personas nuevas y usar las salas de chat para conocer a personas nuevas, en las que sus saturaciones son cercanas a 0,4 (concretamente, 0,398 y 0,381 respectivamente).

Tabla 36. Saturación en componentes. Uso de las TIC para contactar con desconocidos

	Dimensión 1
Usar el móvil para conocer personas nuevas	,398
Usar las redes sociales para conocer personas nuevas	,485
Contactar con desconocidos a través de Internet	,898
Contactar con desconocidos a través de mensajería instantánea	,548
Contactar con desconocidos a través de redes sociales	,736
Contactar con desconocidos a través de chat	,381
Contactar con desconocidos a través de videojuegos *online*	,450
Contactar con desconocidos para mantener una amistad	,725
Contactar con desconocidos para mantener una relación	,426
Contactar con desconocidos para jugar	,542

Normalización principal por variable.

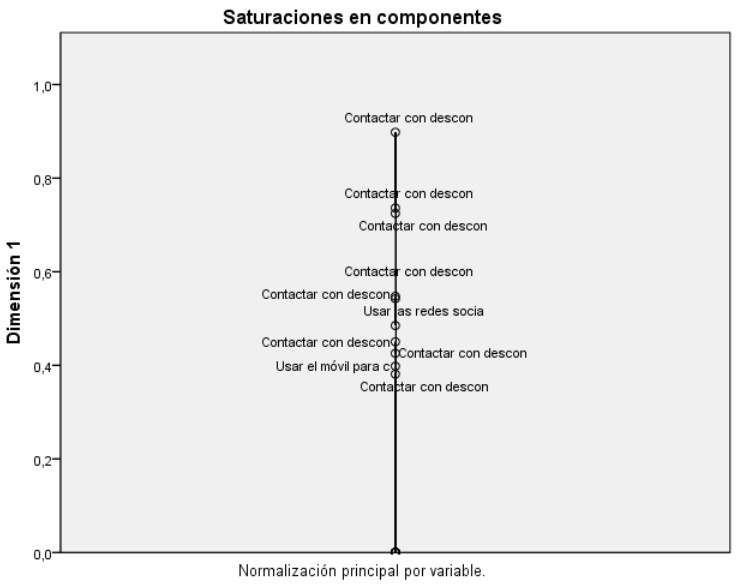


Ilustración 51. Saturación en componentes. Uso de las TIC para contactar con desconocidos

10. Componente 10: No agregar a los familiares a las redes sociales

En décimo lugar, se ha configurado la componente "no agregar a los familiares a las redes sociales". Esta componente, incluida como elemento de protección, está compuesta por tres ítems que hacen referencia a agregar como "amigos" en las redes sociales a los padres, los hermanos y otros familiares que, como se ha relatado en apartados anteriores, puede ejercer control sobre la actividades de los menores en el ciberespacio, concretamente, en las redes sociales. La consistencia interna es de 0,69 y la varianza explicada es de 61,96%.

Tabla 37. Resumen del modelo. No agregar a los familiares a las redes sociales

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,693	1,859	61,955
Total	,693	1,859	61,955

Los ítems incluidos en esta componente muestran unidimensionalidad, y además saturan por encima de 0,7.

Tabla 38. Saturación en componentes. No agregar a los familiares a las redes sociales

	Dimensión
	1
No agregar a los hermanos a las redes sociales	,767
No agregar a otros familiares a las redes sociales	,799
Agregar a sus padres a las redes sociales	,795

Normalización principal por variable.

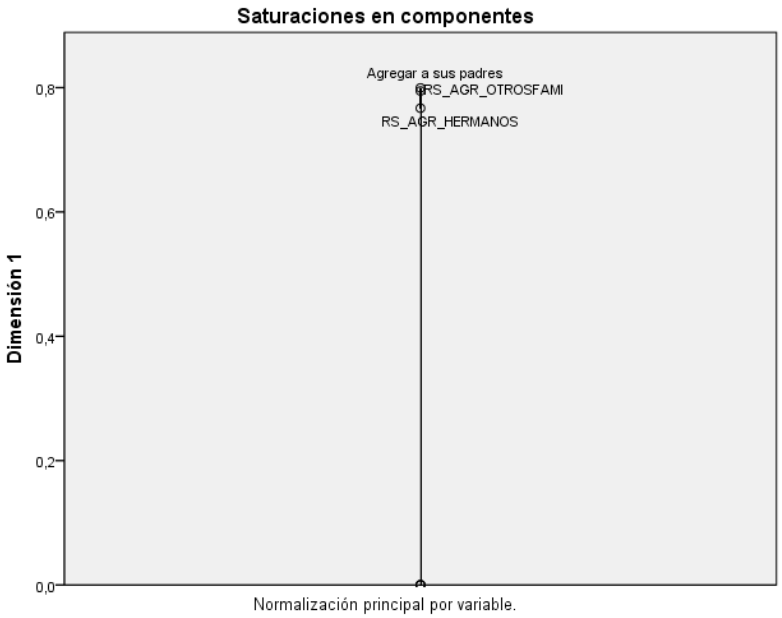


Ilustración 52. Saturación en componentes. No agregar a los familiares a las redes sociales

11. Componente 11: No control

La última componente también incluye ítems relativos a la vigilancia ejercida por los padres sobre el actuar cotidiano de los menores en Internet. De forma concreta, tres de los cinco ítems incluidos analizan el hecho de compartir con otras personas el ordenador con el que navegan por Internet y los otros dos respecto al control que ejercen sobre los menores en cuanto al uso del móvil y del ordenador con el que navegan en Internet. Esta componente resume el 47,4% de la información contenida y tiene un nivel de consistencia interna de 0,723.

Tabla 39. Resumen del modelo. No control

		Varianza explicada	
Dimensión	Alfa de Cronbach	Total (Autovalores)	% de la varianza
1	,723	2,371	47,42
Total	,723	2,371	47,42

Respecto a la saturación de los ítems observamos valores altos, salvo los relativos al control ejercido sobre el uso del ordenador y el móvil que, si bien se encuentran por debajo de 0,4, ambos son relevantes desde un punto de vista teórico.

Tabla 40. Saturación en componentes. No supervisión

	Dimensión 1
No compartir el ordenador/*tablet*	,961
No compartir el ordenador con los padres	,847
No compartir el ordenador/tablet con los hermanos	,744
No control sobre el uso del ordenador	,332
No control sobre el uso del móvil	,259

Normalización principal por variable.

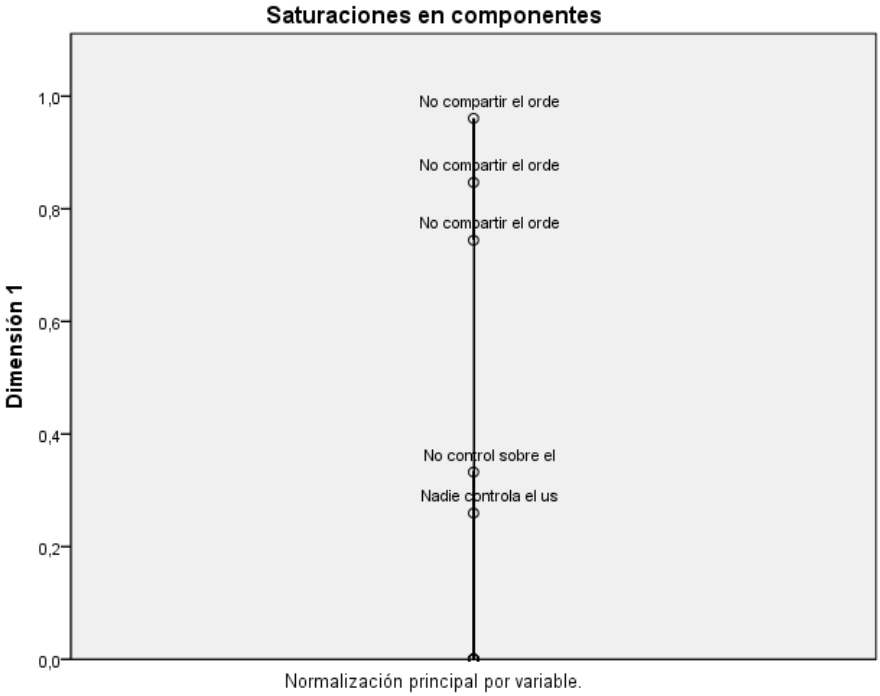


Ilustración 53. Saturación en componentes. No supervisión

3.2.2. Análisis descriptivo de las componentes principales

Tras la creación de las componentes principales, se procedió a hacer los análisis descriptivos de las mismas, cuyos resultados se muestran a continuación.

Las puntuaciones obtenidas en las componentes han sido transformadas a puntuaciones T, con media 50 y desviación típica 10. El motivo de la transformación radica en que todas las variables estén en la misma unidad de medida. Lo que, además, facilita la interpretación y la comparación de las puntuaciones.

Como se desprende de la tabla, la media de las puntuaciones es 50, y la desviación típica es de 10 debido a la transformación de las puntuaciones originales. Los valores de la mediana oscilan entre 45 y 47, quedando por debajo de las medias, por lo que podemos afirmar que los datos presentan una distribución asimetría positiva, salvo en la variable "interacción con conocidos", en la que la mediana presenta un valor superior, pero muy cercano a la media. Esto viene a confirmar que los sujetos de la muestra tienden a realizar en menor medida los comportamientos de riesgo medido, salvo excepción de la interacción con conocidos. Analizando los percentiles, observamos que el 75% de las puntuaciones son cercanas a la media y a su vez al límite mínimo, pero encontramos que un 25% de los sujetos obtienen puntuaciones muy altas, es decir, atendiendo a la literatura, tenemos un grupo de sujetos que en mayor medida llevan a cabo conductas de riesgo en el ciberespacio.

Tabla 41. Descriptivos de las componentes principales

	GUAR.	DAR	MEDIO DAR	COMP. DESV.	HERRA.	CONO.	COTIL.	LIGAR	DESCO.	AGREG.	NO CONTR.
N Válidos	2038	2038	2038	2038	2038	2038	2038	2038	2038	2038	2038
Media	50	50	50	50	50	50	50	50	50	50	50
Me	45,88	43,62	43,86	44,82	47,81	51,04	43,47	45,11	45,29	46,42	47,04
Mo	41,5	43,62	43,86	44,82	36,94	63,36	43,47	45,11	42,04	37,79	43,31
D.T.	10,00	10,00	10,00	10,00	10,00	10,00	10,00	10,00	10,00	10,00	10,97
Var.	100,05	100,05	100,05	100,05	100,05	100,05	100,05	100,05	100,05	100,05	120,26
Asim.	1,17	1,41	1,5	2,94	0,76	-0,68	1,09	1,75	0,98	0,13	0,75
ET asim.	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05	0,05
Curtosis	0,76	0,83	1,26	10,36	0,10	-0,03	-0,55	1,38	-0,11	-1,40	-0,52
ET curtosis	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11	0,11
Mínimo	41,5	43,62	43,86	44,82	36,94	26,36	43,47	45,11	42,04	37,79	36,12
Máximo	83,98	80,89	89	111,42	87,49	63,36	68,57	74,09	88,75	64,02	74,39
P_{25}	41,49	43,62	43,86	44,82	42,06	45,61	43,47	45,11	42,03	37,79	43,31
P_{50}	45,88	43,62	43,86	44,82	47,80	51,04	43,47	45,11	45,29	46,42	47,04
P_{75}	55,95	57,27	54,63	51,40	56,51	59,29	55,35	45,11	57,87	55,69	56,90

Asimismo, en este punto se analiza a través de la prueba de Kolmorov-Smirnov la distribución de las puntaciones obtenidas para las componentes. Como se puede observar en la siguiente tabla, todos los valores obtenidos indican que no se puede aceptar la hipótesis nula de que las variables se comportan conforme a la Ley de Normalidad. Por tanto, se concluye que ninguna de las puntuaciones obtenidas para cada una de las componentes se distribuye de forma normal, pese a que los datos descriptivos y los gráficos apuntaban lo contrario.

Tabla 42. Prueba de Kolmogorov-Smirnov para una muestra

	GUAR.	DAR	MEDIO DAR	COMP. DESV.	HERRA.	CONO.	COTIL.	LIGAR	DESCO.	AGREG.	NO CONTR.
Z de K-S	10,351	17,045	18,114	14,642	4,327	4,101	18,639	21,508	12,89	8,404	9,105
Sig.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000

La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

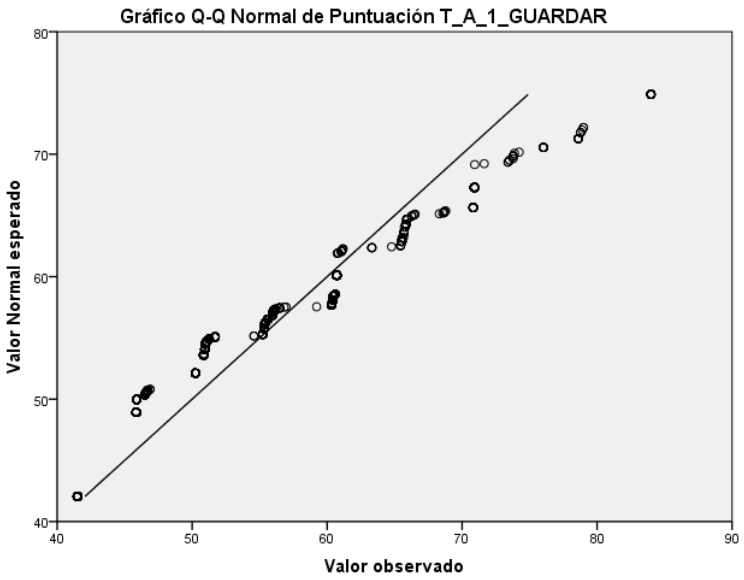


Ilustración 54. Gráfico Q-Q Normal de Puntuación. Componente Guardar

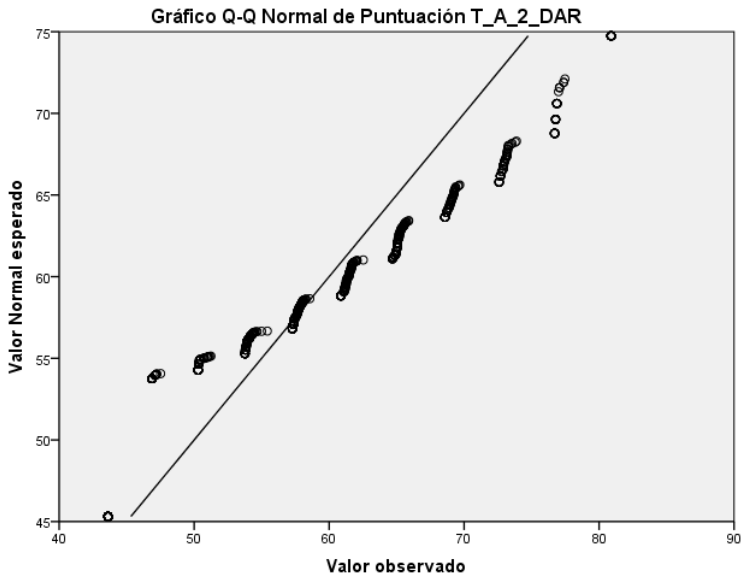


Ilustración 55. Gráfico Q-Q Normal de Puntuación. Facilitar información personal real a través de Internet

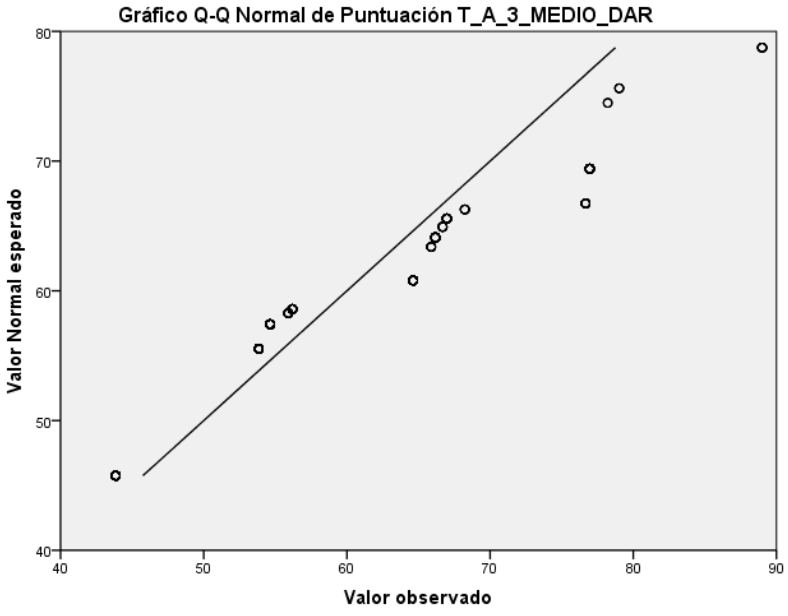


Ilustración 56. Gráfico Q-Q Normal de Puntuación. Medios usados para facilitar información personal real

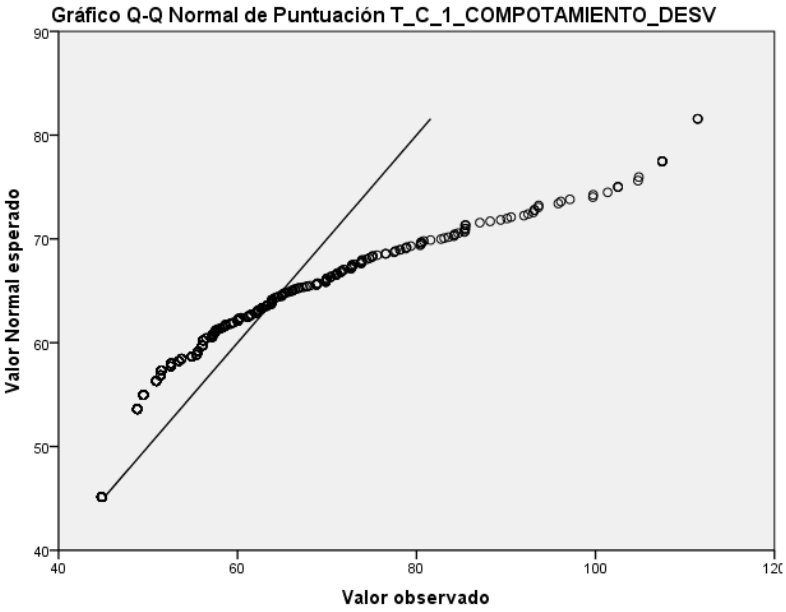


Ilustración 57. Gráfico Q-Q Normal de Puntuación. Comportamiento desviado en el ciberespacio

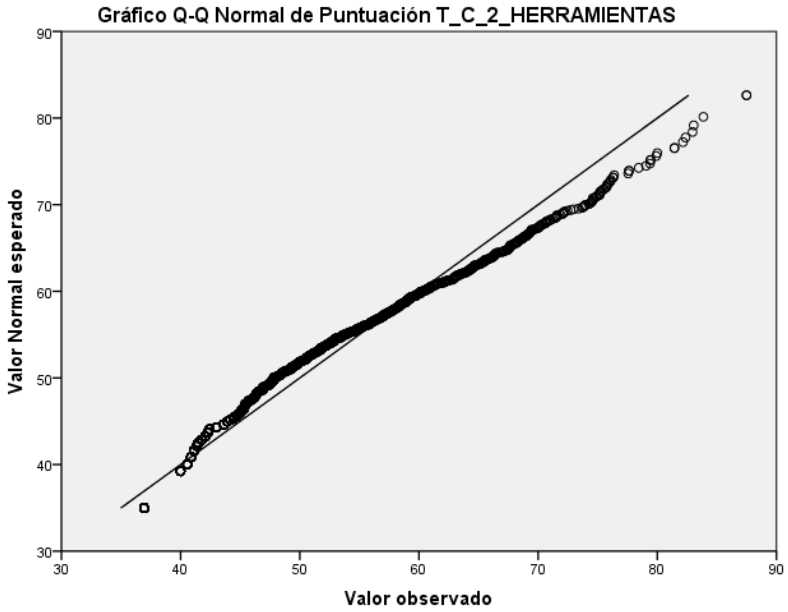


Ilustración 58. Gráfico Q-Q Normal de Puntuación. Uso de herramientas de comunicación

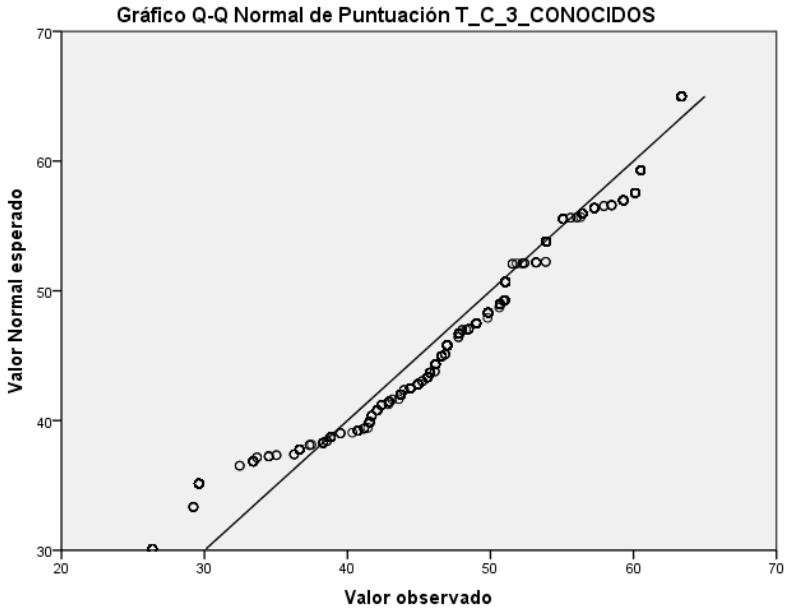


Ilustración 59. Gráfico Q-Q Normal de Puntuación. Uso de las TIC para contactar con conocidos

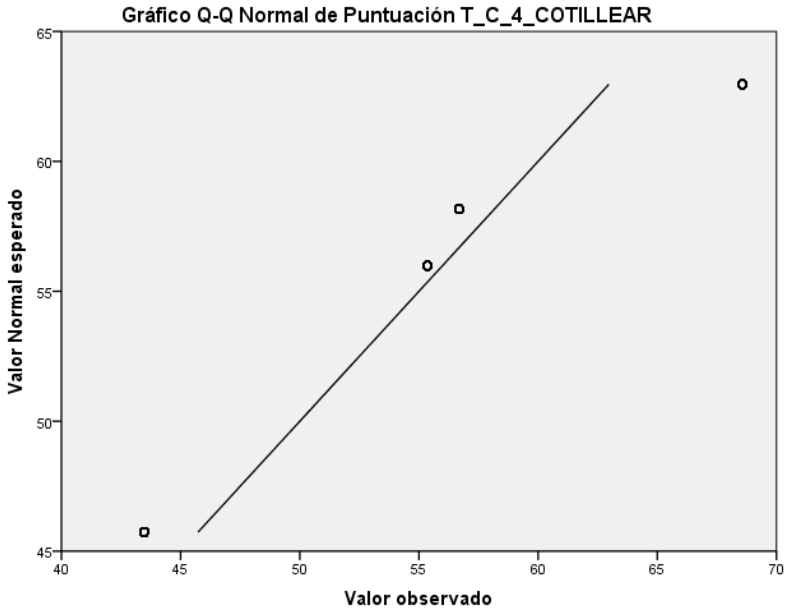


Ilustración 60. Gráfico Q-Q Normal de Puntuación. Uso de las TIC para cotillear

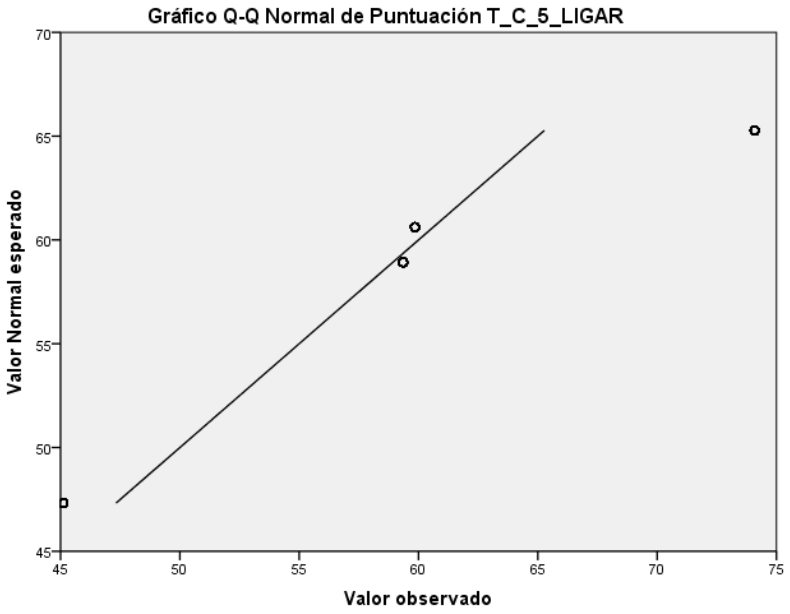


Ilustración 61. Gráfico Q-Q Normal de Puntuación. Uso de las TIC para establecer relaciones sentimentales

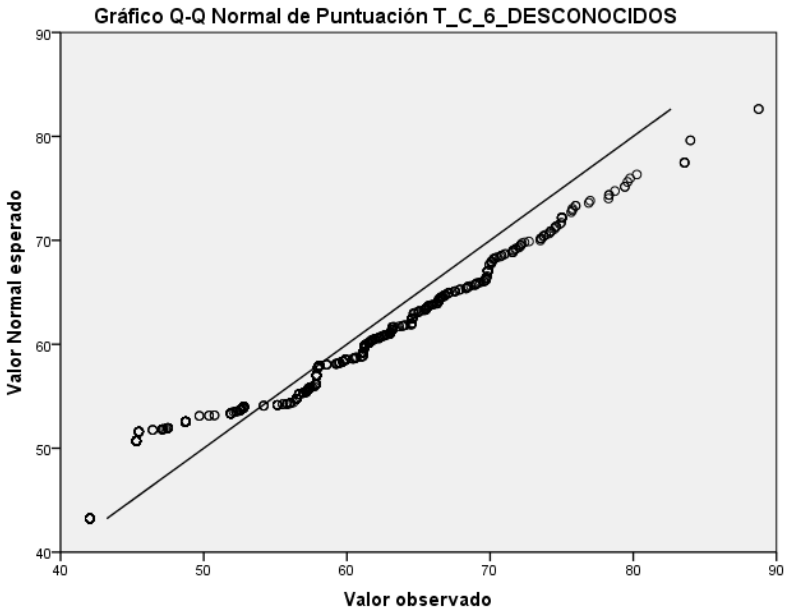


Ilustración 62. Gráfico Q-Q Normal de Puntuación. Uso de las TIC para contactar con desconocidos

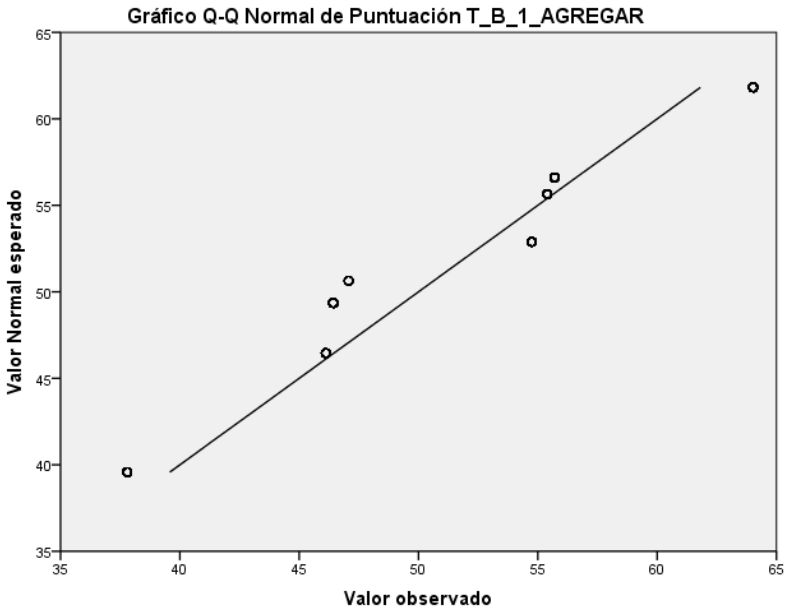


Ilustración 63. Gráfico Q-Q Normal de Puntuaciones. No agregar a los familiares a las redes sociales

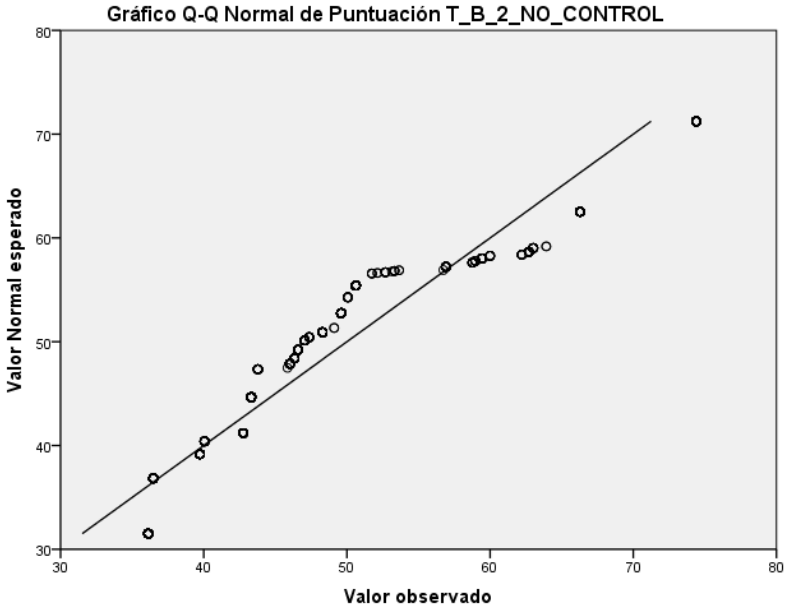


Ilustración 64. Gráfico Q-Q Normal de Puntuación. No control

3.2.3. Análisis factorial de las componentes principales

En este punto se ha realizado un análisis factorial que nos permite conocer cómo se agrupan las variables y establecer la validez de constructo. Es una técnica de reducción de la dimensionalidad de los datos. Su propósito último consiste en buscar el número mínimo de dimensiones capaces de explicar al máximo de información contenida en los datos. De esta forma, podremos comprobar si las variables independientes creadas a partir del CATPCA se agrupan en tres factores de acuerdo a las hipótesis planteadas.

Como se muestra en la tabla de la varianza total explicada, las variables se agrupan entre tres factores. El primero de ellos explica un total del 16,6% de la varianza total. El segundo un 15,6%. Y, finalmente, el tercero explica un 9,1% de la varianza. La suma de los tres factores nos muestra que se llega a explicar un 41,2% de la varianza total.

Tabla 43. Análisis factorial: Varianza total explicada

	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción			Suma de las saturaciones al cuadrado de la rotación		
Factor	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
1	3,070	27,911	27,911	2,543	23,122	23,122	1,822	16,563	16,563
2	1,419	12,895	40,806	1,015	9,224	32,345	1,715	15,593	32,155
3	1,283	11,660	52,466	,978	8,895	41,241	,999	9,085	41,241
4	,966	9,330	61,796						
5	,955	8,684	70,480						
6	,771	7,011	77,492						
7	,606	5,512	83,004						
8	,592	5,380	88,384						
9	,569	5,176	93,559						
10	,490	4,456	98,016						
11	,218	1,984	100,000						

Método de extracción: Mínimos cuadrados no ponderados.

Analizando la matriz de factores, vemos que se agrupan de acuerdo al planteamiento inicial. El primer factor sería el de "introducción", donde se agrupan las variables guardar información personal en los dispositivos con los que se conectan a Internet (GUARDAR), facilitar información personal a otros usuarios a través de Internet (DAR), y el medio empleado para facilitar esa información (MEDIO DAR).

El segundo factor incluye las variables de interacción. Estas variables son: realizar comportamientos desviados en la Red (COMPORTAMIENTO_DESV.), hacer un mayor uso de las herramientas de comunicación (HERRAMIENTAS), usar las TIC para mantener el contacto con personas conocidas (CONOCIDOS), usar las TIC para cotillear (COTILLEAR), usar las TIC para ligar (LIGAR) y contactar con desconocidos (DESCONOCIDOS).

El último hace referencia a la vigilancia familiar experimentada por porte de los familiares. En este caso, las variables incluidas son no agregar a familiar a las redes sociales (AGREGAR) y la falta de supervisión (NO CONTROL), que como se ha explicado en apartados anteriores, incluye no compartir el ordenador con otros familiares y no ser controlado de manera específica por los padres.

Tabla 44. Análisis factorial: Matriz de factores rotados

	Factor		
	1	2	3
GUARDAR	,416	,347	,008
DAR	,803	,178	-,059
MEDIO DAR	,917	,107	-,045
COMPOTAMIENTO_DESV	,166	,333	-,175
HERRAMIENTAS	,197	,298	,042
CONOCIDOS	,155	,556	,157
COTILLEAR	,096	,625	-,093
LIGAR	-,060	,606	-,134
DESCONOCIDOS	,325	,448	-,089
AGREGAR	,062	,144	,931
NO CONTROL	,053	,102	,189

Método de extracción: Mínimos cuadrados no ponderados.

Método de rotación: Normalización Varimax con Kaiser.

a. La rotación ha convergido en 5 iteraciones.

De acuerdo con lo visto, podemos concluir que los datos muestran una estructura semejante a la planteada en el modelo teórico. Entre las actividades medidas de los menores en el ciberespacio, se pueden distinguir aquellas cuyo propósito es la interacción con otras personas, las relativas a la introducción de bienes al ciberespacio, y las de vigilancia por parte de la familia.

3.3. Análisis bivariados

3.3.1. Análisis de las conductas de ciberacoso continuado por sexo y edad

El objetivo de este apartado es analizar la relación entre las variables dependientes incluidas en el estudio y las variables demográficas, para intentar determinar si existen diferencias en la victimización por ciberacoso continuado por sexo y por edad.

a. Diferencias por sexo

Para cumplir con el objetivo propuesto de determinar si existen diferencias significativas en la victimización por sexo se empleó el test Chi-Cuadrado de Pearson, dada la naturaleza cualitativa de las variables. También se tuvo en cuenta el valor de la *Odd Ratio* para determinar la probabilidad de que el evento victimización suceda, contra la que no suceda, dependiendo del sexo.

a.1. Relación entre la victimización por insultos y el sexo

Comparando la cibervictimización por insultos entre chicos y chicas observamos que hay un porcentaje mayor de chicas (57,5%) víctimas que de chicos (42,4%) y que además esa diferencia es significativa (χ^2 =15,8; p=0,000), de forma que los chicas tienen un 60,3% más de probabilidades de ser víctimas que los chicos (OR=1,524).

Tabla 45. Tabla de contingencia: Víctimas de insultos por sexo

			¿En algún momento de tu vida alguien te ha insultado o ridiculizado repetidamente a través de Internet o del móvil?		
			VÍCTIMA	NO VÍCTIMA	Total
Sexo	Chica	Recuento	270	739	1009
		% dentro de Sexo	26,8%	73,2%	100,0%
		% dentro de V_Insulto	57,6%	47,1%	49,5%
	Chico	Recuento	199	830	1029
		% dentro de Sexo	19,3%	80,7%	100,0%
		% dentro de V_Insulto	42,4%	52,9%	50,5%
Total		Recuento	469	1569	2038
		% dentro de Sexo	23,0%	77,0%	100,0%
		% dentro de V_Insulto	100,0%	100,0%	100,0%

Tabla 46. Pruebas de chi-cuadrado: Víctimas de insulto por sexo

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	15,832[a]	1	,000		
Corrección por continuidad[b]	15,415	1	,000		
Razón de verosimilitudes	15,874	1	,000		
Estadístico exacto de Fisher				,000	,000
Asociación lineal por lineal	15,824	1	,000		
N de casos válidos	2038				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 232,20.

b. Calculado sólo para una tabla de 2x2.

Tabla 47. Estimación de riesgo: Víctimas de insulto por sexo

		Intervalo de confianza al 95%	
	Valor	Inferior	Superior
Razón de las ventajas para Sexo (Chico / Chica)	1,524	1,237	1,877
Para la cohorte ¿En algún momento de tu vida alguien te ha insultado o ridiculizado repetidamente a través de Internet o del móvil? = VÍCTIMA	1,384	1,178	1,626
Para la cohorte ¿En algún momento de tu vida alguien te ha insultado o ridiculizado repetidamente a través de Internet o del móvil? = NO VÍCTIMA	,908	,866	,952
N de casos válidos	2038		

a.2. Relación entre la victimización por rumores y el sexo

En cuanto a la victimización por rumores, observamos que de nuevo el porcentaje de chicas víctima es superior al de los chicos (52,5% y 47,5%, respectivamente). Sin embargo, esta diferencia por sexo no es significativa (χ^2=2,01; p=0,156).

Tabla 48. Tabla de contingencia: Víctimas de rumores por sexo

			¿Alguien ha contado rumores o mentiras sobre ti de forma repetida para hacerte daño a través de Internet o del móvil?		
			VÍCTIMA	NO VÍCTIMA	Total
Sexo	Chica	Recuento	230	779	1009
		% dentro de Sexo	22,8%	77,2%	100,0%
		% dentro de V_Rumores	52,5%	48,7%	49,5%
	Chico	Recuento	208	821	1029
		% dentro de Sexo	20,2%	79,8%	100,0%
		% dentro de V_Rumores	47,5%	51,3%	50,5%
Total		Recuento	438	1600	2038
		% dentro de Sexo	21,5%	78,5%	100,0%
		% dentro de V_Rumores	100,0%	100,0%	100,0%

Tabla 49. Pruebas de chi-cuadrado: Víctimas de rumores por sexo

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	2,011[a]	1	,156		
Corrección por continuidad[b]	1,861	1	,172		
Razón de verosimilitudes	2,012	1	,156		
Estadístico exacto de Fisher				,161	,086
Asociación lineal por lineal	2,010	1	,156		
N de casos válidos	2038				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 216,85.

b. Calculado sólo para una tabla de 2x2.

Tabla 50. Estimación de riesgo: Víctimas de rumores por sexo

		Intervalo de confianza al 95%	
	Valor	Inferior	Superior
Razón de las ventajas para Sexo (Chico / Chica)	1,165	,943	1,440
Para la cohorte ¿Alguien ha contado rumores o mentiras sobre ti de forma repetida para hacerte daño a través de Internet o del móvil? = VÍCTIMA	1,128	,955	1,332
Para la cohorte ¿Alguien ha contado rumores o mentiras sobre ti de forma repetida para hacerte daño a través de Internet o del móvil? = NO VÍCTIMA	,968	,925	1,013
N de casos válidos	2038		

a.3. Relación entre la victimización por contacto repetido no deseado y el sexo

Respecto al contacto repetido no deseado, también son las chicas quienes experimentan más esta forma de cibervictimización. Observamos que el porcentaje de chicas víctimas es de 63,1% frente 36,9% de chicos. Esta diferencia es además significativa, tal y como muestran los resultados (χ^2=25,43; p=0,000). Encontrando que las chicas tienen un 66% más de probabilidades de sufrir esta forma de victimización que los chicos (OR=1,915).

Tabla 51. Tabla de contingencia: Víctimas de contacto repetido por sexo

			¿Alguien ha contactado contigo repetidamente a través de Internet o el móvil tras haberle pedido que no lo hiciera?		
			VÍCTIMA	NO VÍCTIMA	Total
Sexo	Chica	Recuento	185	824	1009
		% dentro de Sexo	18,3%	81,7%	100,0%
		% dentro de V_Contacto	63,1%	47,2%	49,5%
	Chico	Recuento	108	921	1029
		% dentro de Sexo	10,5%	89,5%	100,0%
		% dentro de V_Contacto	36,9%	52,8%	50,5%
Total		Recuento	293	1745	2038
		% dentro de Sexo	14,4%	85,6%	100,0%
		% dentro de V_Contacto	100,0%	100,0%	100,0%

Tabla 52. Pruebas de chi-cuadrado: Víctimas de contacto repetido por sexo

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	25,434[a]	1	,000		
Corrección por continuidad[b]	24,801	1	,000		
Razón de verosimilitudes	25,674	1	,000		
Estadístico exacto de Fisher				,000	,000
Asociación lineal por lineal	25,421	1	,000		
N de casos válidos	2038				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 145,06.

b. Calculado sólo para una tabla de 2x2.

Tabla 53. Estimación de riesgo: Víctimas de contacto repetido por sexo

		Intervalo de confianza al 95%	
	Valor	Inferior	Superior
Razón de las ventajas para Sexo (Chico / Chica)	1,915	1,483	2,471
Para la cohorte ¿Alguien ha contactado contigo repetidamente a través de Internet o el móvil tras haberle pedido que no lo hiciera? = VÍCTIMA	1,747	1,401	2,179
Para la cohorte ¿Alguien ha contactado contigo repetidamente a través de Internet o el móvil tras haberle pedido que no lo hiciera? = NO VÍCTIMA	,912	,880	,946
N de casos válidos	2038		

a.4. Relación entre la victimización por marginación y el sexo

Similares resultados se obtienen para la última forma medida de ciberacoso continuado: haber sido marginado. El porcentaje de chicas víctimas es superior al de chicos, 63,3% frente a un 36,7%. De nuevo, podemos afirmar que esta diferencia entre grupos es significativa (χ^2=7,79; p=0,005) y, por lo tanto, las chicas tienen más probabilidades (64%) de sufrir esta forma de victimización que los chicos (OR=1,806).

Tabla 54. Tabla de contingencia: Víctima de marginación por sexo

			¿Alguien ha utilizado Internet o el móvil para marginarte o excluirte de manera continuada?		
			VÍCTIMA	NO VÍCTIMA	Total
Sexo	Chica	Recuento	62	947	1009
		% dentro de Sexo	6,1%	93,9%	100,0%
		% dentro de V_Marginar	63,3%	48,8%	49,5%
	Chico	Recuento	36	993	1029
		% dentro de Sexo	3,5%	96,5%	100,0%
		% dentro de V_Marginar	36,7%	51,2%	50,5%
Total		Recuento	98	1940	2038
		% dentro de Sexo	4,8%	95,2%	100,0%
		% dentro de V_Marginar	100,0%	100,0%	100,0%

Tabla 55. Pruebas de chi-cuadrado: Víctimas de marginación por sexo

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	7,793[a]	1	,005		
Corrección por continuidad[b]	7,226	1	,007		
Razón de verosimilitudes	7,876	1	,005		
Estadístico exacto de Fisher				,007	,003
Asociación lineal por lineal	7,789	1	,005		
N de casos válidos	2038				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 48,52.

b. Calculado sólo para una tabla de 2x2.

Tabla 56. Estimación de riesgo: Víctimas de marginación por sexo

		Intervalo de confianza al 95%	
	Valor	Inferior	Superior
Razón de las ventajas para Sexo (Chico / Chica)	1,806	1,186	2,749
Para la cohorte ¿Alguien ha utilizado Internet o el móvil para marginarte o excluirte de manera continuada? = VÍCTIMA	1,756	1,176	2,624
Para la cohorte ¿Alguien ha utilizado Internet o el móvil para marginarte o excluirte de manera continuada? = NO VÍCTIMA	,973	,954	,992
N de casos válidos	2038		

A modo de resumen, el análisis bivariado entre las variables dependientes y la variable sexo muestra que las chicas son las que en mayor medida sufren el ciberacoso continuado. Siendo estadísticamente diferente para las conductas insultar o ridiculizar de manera repetida, el contacto repetido no deseado, y para la conducta de marginar.

b. Diferencias por edad

Del mismo modo que con la variable sexo, en este punto se analizan las posibles diferencias que puedan existir en el ciberacoso continuado teniendo en cuenta la edad de los sujetos de la muestra.

Antes de realizar los análisis por edad, es necesario apuntar que la edad ha sido agrupada en tres categorías: el primer grupo está conformado por los sujetos que tienen entre 12 y 13 años; el segundo grupo lo conforman los sujetos que tienen entre 14 y 15 años; y el tercer grupo por el resto de sujetos, es decir, los que tienen entre 16 y 18 años. Realizando esta clasificación, el primer grupo está compuesto por 647 sujetos (31,7%), el segundo grupo por 721 (35,4%) y el tercero por 670 (32,9%).

Tabla 57. Frecuencia y porcentaje de la edad agrupada

EDAD	Frecuencia	Porcentaje
12-13	647	31,7
14-15	721	35,4
16-18	670	32,9
Total	2038	100,0

Con el fin de contrastar la uniformidad de las frecuencias obtenidas para cada uno de los grupos de edad, es decir, para determinar si existe el mismo número de víctimas en los tres grupos de edad establecidos, se ha optado por usar el test Chi-cuadrado de Pearson.

b.1. Relación entre la victimización por insultos y la edad

Comparando el número de víctimas de insulto para cada uno de los grupos de edad observamos que el número total de víctimas se distribuye de forma similar en los tres grupos: el 32,2% tiene entre 12 y 13 años, el 34,5% tiene entre 14 y 15 años y el 33,3% tiene entre 16 y 18 años.

Tabla 58. Víctima de insultos por edad

	¿En algún momento de tu vida alguien te ha insultado o ridiculizado repetidamente a través de Internet o del móvil? VÍCTIMA	
EDAD	Frecuencia	Porcentaje
12-13	151	32,20%
14-15	162	34,50%
16-18	156	33,30%
Total	469	100,0%

El estadístico chi-cuadrado viene a confirmar que el número de víctimas se distribuye igual en los tres grupos (χ^2=0,388; p=0,824) y que por lo tanto, no podemos afirmar que exista una relación ente la edad y la victimización por insultos.

Tabla 59. Estadísticos de contraste. Víctima insultos por edad

	Notas
Chi-Cuadrado	0,388
gl	2
Sig.	0,824

b.2. Relación entre la victimización por rumores y la edad

Cuando comparamos el número de víctimas por rumores o mentiras en los tres grupos de edad observamos que, al igual que sucedía con las víctimas de insulto, las frecuencias se distribuyen igual para los tres grupos. El grupo que más víctimas presenta es el compuesto por jóvenes entre 14 y 15 años con un 35,8%, seguido del grupo de los que tienen entre 16 y 18 años con un 34,7% y, finalmente, el grupo con menor número de víctimas es el que lo conforman los menores entre 12 y 13 años con un 29,5%.

Tabla 60. Víctima de rumores por edad

	¿Alguien ha contado rumores o mentiras sobre ti de forma repetida para hacerte daño a través de Internet o del móvil? VÍCTIMA	
EDAD	Frecuencia	Porcentaje
12-13	129	29,5%
14-15	157	35,8%
16-18	152	34,7%
Total	438	100,0%

El estadístico chi-cuadrado confirma que las frecuencias de victimización se distribuyen uniformemente para las tres grupos (χ^2=3,055; p=0,217) y por lo tanto no existen diferencias en la victimización en relación a la edad.

Tabla 61. Estadísticos de contraste. Víctima rumores por edad

	Notas
Chi-Cuadrado	3,055
gl	2
Sig.	0,217

b.3. Relación entre la victimización por contacto repetido no deseado y la edad

En la tabla que se presenta a continuación, se observa como el mayor número de víctimas por contacto repetido no deseado se sitúa en el grupo con mayor edad (16-18 años) con un 46,1%. El segundo grupo con mayor número de víctimas es el grupo conformado por menores de entre 14 y 15 años con un 30% y el grupo que menos víctimas presenta es el conformado por los más pequeños de la muestra con un 23,9%.

Tabla 62. Víctima de contacto repetido por edad

	¿Alguien ha contactado contigo repetidamente a través de Internet o el móvil tras haberle pedido que no lo hiciera? VÍCTIMA	
EDAD	Frecuencia	Porcentaje
12-13	70	23,9%
14-15	88	30,0%
16-18	135	46,1%
Total	469	100,0%

Al comprobar la uniformidad de las puntuaciones observamos que no se distribuyen igual (χ^2=23,065; p=0,000) por lo tanto podemos afirmar que existe una relación entre la edad y la victimización por

contacto repetido no deseado, de manera que a mayor edad más probabilidades de sufrir este tipo de victimización.

Tabla 63. Estadísticos de contraste. Víctima insultos por edad

	Notas
Chi-Cuadrado	23,065
gl	2
Sig.	0,000

b.4. Relación entre la victimización por marginación y la edad

Comparando los porcentajes de victimización por la conducta de marginar en los tres grupos de edad, observamos que se comporta de forma contraria a la conducta de contacto repetido no deseado. En este caso los porcentajes disminuyen con la edad. Así, en el grupo compuesto por los que tienen entre 12 y 13 años el porcentaje se sitúa en un 40,8%, seguido del grupo de 14 y 15 años con un porcentaje de 32,7% y del grupo de entre 16 y 18 años.

Tabla 64. Víctima de marginación por edad

	¿Alguien ha utilizado Internet o el móvil para marginarte o excluirte de manera continuada? VÍCTIMA	
EDAD	Frecuencia	Porcentaje
12-13	40	40,8%
14-15	32	32,7%
16-18	26	26,5%
Total	469	100,0%

Sin embargo, las pruebas de contraste confirma que el número de víctimas de distribuye de manera uniforme entre los tres grupos (χ^2=3,02; p=0,221) y por lo tanto no hay relación entre la edad y esta forma de victimización.

Tabla 65. Estadísticos de contraste. Víctima insultos por edad

	Notas
Chi-Cuadrado	3,02
gl	2
Sig.	0,221

A modo de resumen, podemos concluir que no hay relación entre la edad y las distintas formas de victimización por ciberacoso continuado, salvo en el caso del contacto repetido no deseado, donde a mayor edad más víctimas se concentran.

3.3.2. Análisis de la relación entre las conductas de ciberacoso continuado y las actividades cotidianas de los menores en el ciberespacio

Con el objetivo de determinar si las "víctimas" llevan a cabo actividades cotidianas en el ciberespacio distintas al grupo de "no víctimas", o dicho de otro modo, para determinar si las puntuaciones obtenidas en las variables independientes son estadísticamente significativas entre el grupo de las "víctimas" y el de las "no victimas" para las cuatro formas de ciberacoso continuado medidas, se optó por emplear la prueba no paramétrica *U* de Mann Whitney dado que ninguna de las variables independientes presentó una distribución normal. Asimismo, se empleó el estadístico *d* de Cohen para determinar el tamaño del efecto de las diferencias encontradas que

permite concluir sobre la magnitud de las diferencias y por consiguiente, de su relevancia.

a. Victimización por insultos

Como se muestra en la tabla, para todas las variables las víctimas de insultos puntúan más que las no víctimas. Podemos observar como las diferencias entre los grupos es estadísticamente significativa para todas las variables salvo para la variable "no control" entendiendo por tanto, que las víctimas experimentan el mismo control que las no víctimas ($p>0,5$). Sin embargo, aunque parecen existir diferencias significativas entre el grupo de víctimas de insultos y no víctimas, dado el tamaño del efecto podemos concluir que las puntuaciones no son tan diferentes, en su mayoría son pequeñas (d<0,5) (Morales, 2012), salvo para las variables "comportamiento desviado" y "contacto desconocidos no deseado" donde encontramos que las diferencias son moderadas (d>0,5), es decir, las víctimas de insultos tienen un mayor comportamiento desviado y contactan más con desconocidos que las "no víctimas".

Tabla 66. Comparación entre cibervictimización por insultos y las variables independientes

Variables Independientes	Grupos	Media	DT	Mediana	Rango promed.	*U* M-W	Sig.	d
GUARDAR	Víctima	52,62	11,26	50,23	1153,98			
	No víctima	49,22	9,46	45,85	979,30	304860,0	0,000	0,3
DAR	Víctima	53,13	11,67	43,62	1171,02			
	No víctima	49,06	9,25	43,62	974,21	296867,5	0,000	0,4
MEDIO DAR	Víctima	52,46	10,70	43,86	1154,01			
	No víctima	49,27	9,67	43,86	979,29	304846,0	0,000	0,3
COMPORT. DESVIADO	Víctima	54,79	13,06	49,47	1290,03			
	No víctima	48,57	8,37	44,82	938,63	241050,5	0,000	0,6
HERRAMIENTAS	Víctima	52,75	10,11	51,16	1188,17			
	No víctima	49,18	9,82	47,09	969,08	288822,5	0,000	0,3
CONTACTO CONOCIDOS	Víctima	52,79	9,18	53,90	1190,76			
	No víctima	49,17	10,09	50,66	968,31	287608,0	0,000	0,3
COTILLEAR	Víctima	53,14	11,21	43,47	1169,49			
	No víctima	49,06	9,41	43,47	974,67	297586,5	0,000	0,4
LIGAR	Víctima	52,43	11,77	45,11	1116,16			
	No víctima	49,27	9,29	45,11	990,61	322599,0	0,000	0,3
CONTACTO DESCONO.	Víctima	53,96	10,88	55,51	1237,71			
	No víctima	48,82	9,41	42,04	954,27	265592,0	0,000	0,5
AGREGAR	Víctima	51,41	10,11	54,74	1098,70			
	No víctima	49,58	9,93	46,42	995,82	330784,0	0,001	0,2
NO CONTROL	Víctima	50,26	11,24	46,59	1028,78			
	No víctima	49,85	10,89	47,04	1016,73	363578,5	0,695	0,1

b. Victimización por rumores

Lo mismo sucede en la victimización por rumores. Encontramos que existen diferencias significativas (p<0,1) entre las puntuaciones de las víctimas y las no víctimas para todas las variables con excepción de la falta de control. Sin embargo, de nuevo encontramos que las diferencias, a pesar de ser significativas, son bajas de acuerdo al tamaño del efecto, aunque son mayores que las encontradas en la victimización por insultos. Donde se encuentran diferencias moderadas es en las variables "ligar", "contacto con desconocidos" y "comportamiento desviado", esta última con una diferencia incluso mayor (*d=0,7)*. Podemos concluir en este punto que las víctimas de rumores contactan más con desconocidos, usan las tecnologías de la información y la comunicación para ligar y para realizar ciberataques en mayor medida que los sujetos que no han sufrido esta forma de victimización.

Tabla 67. Comparación entre cibervictimización por rumores y las variables independientes

Variables Independientes	Grupos	Media	DT	Mediana	Rango promed.	*U* M-W	Sig.	d
	Víctima	52,29	10,89	50,24	1142,74			
GUARDAR	No víctima	49,37	9,65	45,85	985,76	296419,5	0,000	0,32
	Víctima	53,36	11,87	43,62	1178,21			
DAR	No víctima	49,08	9,22	43,62	976,05	280883,5	0,000	0,4
	Víctima	52,80	11,02	43,86	1167,18			
MEDIO DAR	No víctima	49,23	9,57	43,86	979,07	285714,0	0,000	0,3
COMPORT.	Víctima	55,54	13,46	50,91	1324,53			
DESVIADO	No víctima	48,48	8,20	44,82	936,00	216799,0	0,000	0,7
	Víctima	52,92	10,43	51,17	1189,57			
HERRAMIENTAS	No víctima	49,20	9,73	47,32	972,94	275907,5	0,000	0,32
	Víctima	53,55	8,96	53,90	1239,05			
CONTACTO CONOCIDOS	No víctima	49,03	10,06	50,66	959,40	254235,5	0,000	0,44
	Víctima	53,64	11,35	43,47	1191,45			
COTILLEAR	No víctima	49,00	9,36	43,47	972,43	275087,5	0,000	0,4
	Víctima	53,71	12,39	45,11	1168,70			
LIGAR	No víctima	48,98	8,98	45,11	978,66	285050,0	0,000	0,5
	Víctima	53,81	11,01	52,80	1228,88			
CONTACTO DESCONO.	No víctima	48,96	9,45	42,04	962,18	258690,5	0,000	0,5
	Víctima	51,31	10,18	54,74	1093,21			
AGREGAR	No víctima	49,64	9,93	46,42	999,32	318115,0	0,002	0,2
	Víctima	50,44	11,46	46,81	1037,18			
NO CONTROL	No víctima	49,81	10,83	47,04	1014,66	342657,0	0,475	0,1

c. Victimización por contacto repetido no deseado

También encontramos que las víctimas por contacto repetido no deseado puntúan de manera significativa en todas las variables de actividades cotidianas salvo en dos relativas a la vigilancia familiar experimentada, no agregar a los familiares a las redes sociales y no tener control sobre el uso de las TIC. No obstante, dado el tamaño del efecto, encontramos que las diferencias son bajas para las variables "medio empleado para ofrecer datos personales reales", "uso de herramientas de comunicación", "uso de las TIC para establecer comunicaciones con conocidos" y "uso de las TIC para ligar". En cambio, las diferencias son moderadas para las variables "guardar", "dar datos personales reales", "comportamiento desviado", "uso de las TIC para cotillear" y "uso de las TIC para contactar con desconocidos". En otras palabras, podemos afirmar que las víctimas por contacto repetido no deseado guardan más información en los sistemas con los que se conectan a Internet, facilitan más información personal real a otras personas a través de Internet, realizan más comportamientos desviados, usan más las TIC para cotillear a otras personas y para contactar con desconocidos.

Tabla 68. Comparación entre cibervictimización por contacto repetido no deseado y las variables independientes

Variables Independientes	Grupos	Media	DT	Mediana	Rango promedi.	*U* M-W	Sig.	d
GUARDAR	Víctima	54,47	11,30	50,97	1265,34			
	No víctima	49,25	9,57	45,85	978,22	183612,0	0,000	0,5
DAR	Víctima	54,73	12,21	50,34	1250,43			
	No víctima	49,21	9,36	43,62	980,73	187980,5	0,000	0,5
MEDIO DAR	Víctima	53,47	10,70	53,84	1221,21			
	No víctima	49,42	9,76	43,86	985,63	196541,5	0,000	0,4
COMPORT. DESVIADO	Víctima	55,90	13,50	51,49	1350,43			
	No víctima	49,01	8,92	44,82	963,93	158679,5	0,000	0,6
HERRAMIEN-TAS	Víctima	53,23	10,26	51,70	1213,38			
	No víctima	49,46	9,86	47,54	986,95	198835,5	0,000	0,42
CONTACTO CONOCIDOS	Víctima	53,17	8,72	53,90	1204,77			
	No víctima	49,47	10,11	51,04	988,39	201358,0	0,000	0,44
COTILLEAR	Víctima	54,06	11,26	55,35	1217,11			
	No víctima	49,32	9,61	43,47	986,32	197743,5	0,000	0,5
LIGAR	Víctima	52,97	12,07	45,11	1137,44			
	No víctima	49,50	9,53	45,11	999,70	221086,0	0,000	0,3
CONTACTO DESCONO.	Víctima	55,06	10,99	57,32	1299,31			
	No víctima	49,15	9,57	42,04	972,52	173657,0	0,000	0,63
AGREGAR	Víctima	50,96	10,27	54,74	1072,59			
	No víctima	49,84	9,95	46,42	1010,59	240087,0	0,087	0,11
NO CONTROL	Víctima	51,07	11,70	48,30	1073,92			
	No víctima	49,76	10,83	46,59	1010,36	239697,5	0,085	0,2

d. Victimización por marginar

En cambio, para la última forma de ciberacoso medida, solo encontramos diferencias significativas (p<0,001) para tres de las once variables independientes incluidas. Las variables que muestran una puntuación mayor en el grupo de los sujetos que afirman haber sido marginado a través de las TIC son las que hacen referencia al comportamiento desviado, al mayor uso de herramientas de comunicación y al contacto con desconocidos. Aunque de nuevo, estas diferencias son bajas.

Tabla 69. Comparación entre cibervictimización por marginar y las variables independientes

Variables Independientes	Grupos	Media	DT	Mediana	Rango promed.	*U* M-W	Sig.	d
GUARDAR	Víctima	51,56	10,13	50,24	1124,52	84768,0	0,059	0,21
	No víctima	49,92	9,99	45,88	1014,19			
DAR	Víctima	50,59	10,06	43,62	1070,72	90040,5	0,304	0,1
	No víctima	49,97	10,00	43,62	1016,91			
MEDIO DAR	Víctima	51,81	11,03	43,86	1106,68	86516,5	0,072	0,2
	No víctima	49,91	9,94	43,86	1015,10			
COMPORT. DESVIADO	Víctima	53,90	13,48	49,47	1223,36	75082,0	0,000	0,4
	No víctima	49,80	9,76	44,82	1009,20			
HERRAMIEN-TAS	Víctima	53,40	10,59	52,07	1219,00	75509,0	0,001	0,42
	No víctima	49,83	9,94	47,77	1009,42			
CONTACTO CONOCIDOS	Víctima	51,46	9,69	53,90	1110,42	86149,5	0,116	0,2
	No víctima	49,93	10,01	51,04	1014,91			

	Víctima	50,98	10,90	43,47	1052,62			
COTILLEAR	No víctima	49,95	9,96	43,47	1017,83	91814,5	0,492	0,11
	Víctima	51,77	11,62	45,11	1083,28			
LIGAR	No víctima	49,91	9,91	45,11	1016,28	88809,5	0,122	0,2
	Víctima	52,85	9,95	52,23	1205,56			
CONTACTO DESCONO.	No víctima	49,86	9,99	42,04	1010,10	76826,5	0,001	0,33
	Víctima	50,23	10,11	46,42	1033,41			
AGREGAR	No víctima	49,99	10,00	46,42	1018,80	93697,0	0,806	0,1
	Víctima	49,70	11,82	46,59	987,01			
NO CONTROL	No víctima	49,96	10,92	47,04	1021,14	91876,0	0,573	0,02

3.3.3. Análisis de las variables independientes por sexo y edad

a. Diferencias por sexo

Con el objetivo de averiguar si las chicas y los chicos realizan las mismas ciberactividades cotidianas, es decir, para comprobar si las puntuaciones obtenidas en las variables independientes son iguales en ambos grupos, se utilizó la prueba *U* de Mann Whitney. También se utilizó la prueba *d* de Cohen para determinar el tamaño del efecto.

Se puede comprobar en la siguiente tabla como las chicas guardan más información en los sistemas con los que se conectan a la Red, facilitan más información personal real a través de Internet a otras personas, usan más medios para ceder esa información, agregan menos a sus familiares a las redes sociales, contactan más con conocidos y emplean más las TIC para cotillear que los chicos (p<0,05).

No obstante, de acuerdo al tamaño del efecto, estas diferencias son bajas (*d*<0,5).

En cambio, los chicos son menos controlados, se comportan de manera más desviada, usan más herramientas de comunicación, emplean más las TIC para ligar y contactan con más desconocidos que las chicas. Pero también estas diferencias son bajas salvo en el mayor uso de herramientas de comunicación y el uso de las TIC para ligar (*d>0,5*).

Tabla 70. Comparación de las puntuaciones de las variables independientes por sexo

Variables Independientes	Grupos	Media	DT	Mediana	Rango promedio	*U* M-W	Sig.	d
	Chica	51,18	10,01	50,24	1096,33			
GUARDAR	Chico	48,84	9,87	45,85	944,16	441606,0	0,000	0,32
	Chica	50,81	10,46	43,62	1060,95			
DAR	Chico	49,20	9,47	43,62	978,86	477308,5	0,000	0,11
	Chica	50,60	9,84	43,86	1060,95			
MEDIO DAR	Chico	49,41	10,13	43,86	978,86	477055,5	0,000	0,11
COMPORT.	Chica	49,22	8,21	44,82	985,18			
DESVIADO	Chico	50,77	11,44	44,82	1053,16	493648,5	0,027	-0,1
	Chica	47,84	8,99	46,19	994,25			
HERRAMIENTAS	Chico	52,11	10,48	51,02	1044,26	392175,5	0,000	-0,55
	Chica	50,36	9,51	51,04	893,68			
CONTACTO CONOCIDOS	Chico	49,64	10,46	51,04	1142,88	509081,0	0,448	0,11
COTILLEAR	Chica	51,70	10,77	43,47	1029,46	437726,5	0,000	0,33

	Chico	48,34	8,88	43,47	1009,73			
	Chica	47,92	7,90	45,11	1100,18			
LIGAR	Chico	52,04	11,35	45,11	940,39	428427,5	0,000	-0,54
	Chica	49,45	9,69	42,04	983,89			
CONTACTO DESCONO.	Chico	50,54	10,27	45,29	1054,42	483196,0	0,004	-0,11
	Chica	50,74	9,99	46,42	1060,95			
AGREGAR	Chico	49,27	9,97	46,42	978,86	475628,0	0,001	0,11
	Chica	49,25	10,64	46,59	1062,61			
NO CONTROL	Chico	50,63	11,24	48,30	977,22	484498,0	0,009	-0,1

b. Diferencias por edad

Para comprobar la posible existencia de diferencias significativas entre los distintos grupos de edad se empleó en primer lugar la prueba de Kruskal-Wallis. En segundo lugar se utilizó la prueba de *U* de Mann-Whitney para estudiar entre qué grupos se producían esas diferencias. En esta segunda prueba se utilizó la corrección de Bonferroni, resultado de dividir el valor de significación bilateral (0,05) entre 3 (número de grupos), para dar como resultado el valor de 0,01, por encima del cual no se consideran significativos los resultados. También se calculó el estadístico *d* de Cohen para comprobar el tamaño del efecto de las comparaciones dos a dos.

Respecto a la acción de guardar archivos en los dispositivos con los que se conecta a Internet, observamos que a mayor edad guardan mayor número de archivos. Tal y como se muestra en la tabla, existen diferencias significativas entre los tres grupos (H=167,96; p=0,000). Las comparaciones dos a dos nos muestran que estas diferencias

significativas se replican para las tres comparaciones (*p=0,000*), sin embargo, se puede ver claramente que la mayor diferencia se sitúa entre el grupo de los más pequeños y el de los más mayores (*d=0,71*), siendo las otras dos comparaciones bajas (*d<0,5*).

La misma situación se repite para la variable facilitar datos personales reales. Existen diferencias significativas entre los tres grupos pero las diferencias son pequeñas salvo para la comparación entre grupo de 12-13 años y el de 16-18 años (*d*=-0,61).

Situación parecida ofrece la variable medios usados para facilitar información personal real. Observamos que sigue la misma tendencia, a mayor edad más puntuación obtienen en esta variable. Existen diferencias entre los grupos, concretamente entre el primer grupo (12-13 años) con los otros dos, no así entre los grupos de mayor edad (14-15 y 16-18años). Sin embargo, las diferencias encontradas son muy pequeñas (*d<0,*39).

También se han encontrado diferencias significativas en el comportamiento desviado de los tres grupos. Observamos como a mayor edad más conductas desviadas practican, encontrando diferencias significativas en las comparaciones dos a dos aunque todas ellas son bajas, siendo la más grande entre el grupo de los más pequeños (12-13 años) y el de los más mayores (16-18años).

Situación parecida a la variable medios usados para facilitar información personal real presenta la variable que mide el mayor uso de herramientas de comunicación que ofrece Internet. De nuevo a mayor edad mayor es el uso de las herramientas de comunicación, encontrando diferencias significativas entre los grupos (*H*=13,33;

p=0,001). Y estas diferencias vienen determinadas por la comparación entre el grupo de los más pequeños (12-13 años) con los otros dos grupos pero de nuevo estas diferencias son muy bajas (*d*<0,2).

Siguiendo con la variable emplear las TIC para mantener el contacto con conocidos, observamos también que a mayor edad mayores puntuaciones y que además existen diferencias significativas entre los tres grupos (*H*=67,85; *p*=0,000). Concretamente, las diferencias vienen determinadas por la comparación entre el grupo de los más pequeños con los otros dos y no entre los dos compuestos por los más mayores. Y a diferencia de lo que ocurría con el resto de variables, en este punto si encontramos diferencias moderadas (*d*=0,5) cuando se compara el grupo de los más pequeños (12-13) con los más mayores (16-18 años).

En el caso del uso de las TIC para cotillear, se repite el hecho de que a mayor edad más puntuación obtienen y que además existen diferencias significativas entre los grupos (*H*=105,2; *p*=0,000). En las comparaciones dos a dos todas resultan significativas (*p*=0,000), pero el cálculo del tamaño del efecto indica que la mayor diferencia se produce entre el grupo de los más pequeños (12-13 años) y el grupo de los más mayores (16-18 años), siendo ésta moderada (*d*=0,58).

En cuanto al empleo de las TIC para ligar, observamos que a mayor edad mayores puntuaciones. Existen diferencias entre los grupos (*H*=21,5; *p*=0,000), y que éstas vienen determinadas por la comparación entre el grupo compuesto por estudiantes de 12 y 13 años con los otros dos (*p*<0,01), aunque las diferencias son pequeñas (d<0,3).

También observamos como el contacto con desconocidos se practica en mayor medida cuanto mayor es la edad de los sujetos de la muestra. Encontramos diferencias significativas entre los grupos (H=79,1; p=0,000) y de nuevo vienen determinadas al comparar el grupo de los más pequeños (12-13 años) con los otros dos (14-15 y 16-18 años) y la mayor diferencia se presenta al compararlo con el grupo de los más mayores (16-18 años) pero es moderada (d=0,5).

En cuanto a la variable no agregar a familiares a las redes sociales, observamos que la distribución es distinta a las variables anteriores. Son el grupo de los más mayores (16-18 años) los que menos agregan, seguido de los más pequeños (12-13 años), siendo por tanto el grupo de los que tienen entre 14 y 15 años los que más agregan a familiares. Observamos también que existen diferencias entre los grupos pero estas se producen entre el grupo de los que tienen entre 14 y 15 años con los otros dos grupos. Sin embargo, estas diferencias son muy pequeñas (d<0,2).

Finalmente, observamos que a mayor edad menos control ejercen sobre ellos, existiendo diferencias significativas entre los grupos. Concretamente, las diferencias se reflejan entre el grupo de los más jóvenes con los otros dos, no existiendo diferencias entre los grupos de los más mayores. No obstante, de nuevo las diferencias son muy pequeñas (d<0,3).

Tabla 71. Comparación de las puntuaciones de las variables independientes por grupos de edad

Variable Independiente	Edad	Rango promedio	*H* K-W	Sig.	Comparación Grupos	*U* de M-W	Sig.	d
GUARDAR	12-13	805			1-2	179354,0	0,000	-0,42
	14-15	1037,89	167,955	0,000	1-3	131854,5	0,000	-0,71
	16-18	1206,85			2-3	200902,0	0,000	-0,28
DAR	12-13	870,52			1-2	193220,5	0,000	-0,42
	14-15	1040,46	95,923	0,000	1-3	160379,5	0,000	-0,63
	16-18	1140,8			2-3	216627,5	0,000	-0,23
MEDIO DAR	12-13	904,36			1-2	201559,5	0,000	-0,26
	14-15	1041,09	58,427	0,000	1-3	173934,0	0,000	-0,39
	16-18	1107,46			2-3	225415,5	0,014	-0,13
COMPORTAMIENTO DESVIADO	12-13	878,21			1-2	197557,5	0,000	-0,26
	14-15	1035,03	86,962	0,000	1-3	161017,5	0,000	-0,38
	16-18	1139,22			2-3	217047,5	0,000	-0,11
HERRAMIENTAS	12-13	951,65			1-2	213315,0	0,006	-0,12
	14-15	1038,38	13,330	0,001	1-3	192775,5	0,001	-0,19
	16-18	1064,7			2-3	235219,0	0,398	-0,07
CONTACTO CONOCIDOS	12-13	868,94			1-2	190427,5	0,000	-0,36
	14-15	1054,3	67,850	0,000	1-3	162151,5	0,000	-0,49
	16-18	1127,44			2-3	223808,0	0,017	-0,14
COTILLEAR	12-13	877,97			1-2	200085,0	0,000	-0,31
	14-15	1021,14	105,172	0,000	1-3	158330,5	0,000	-0,58
	16-18	1154,41			2-3	209557,5	0,000	-0,27
LIGAR	12-13	963,58			1-2	219856,5	0,007	-0,16
	14-15	1022,4	21,453	0,000	1-3	193951,0	0,000	-0,27

	16-18	1070,38			2-3	230241,5	0,042	-0,11
CONTACTO DESCONOCIDOS	12-13	865,6			1-2	188679,5	0,000	-0,37
	14-15	1058,94	79,139	0,000	1-3	161735,0	0,000	-0,49
	16-18	1125,68			2-3	225406,5	0,024	-0,12
AGREGAR	12-13	1055,53			1-2	207504,0	0,000	0,20
	14-15	940,18	21,500	0,000	1-3	214317,0	0,718	-0,04
	16-18	1070,07			2-3	210082,5	0,000	-0,24
NO CONTROL	12-13	926,36			1-2	205300,5	0,000	-0,19
	14-15	1046,11	25,243	0,000	1-3	184423,5	0,000	-0,29
	16-18	1080,81			2-3	232775,5	0,238	-0,10

Analizadas una a una las variables de las actividades cotidianas en los tres grupos de edad, podemos concluir que la tendencia es que a mayor edad más actividades de riesgo practican y menos vigilancia experimentan. En la mayoría de los casos, se han encontrado diferencias estadísticamente significativas entre los grupos, principalmente al comparar el grupo de los más jóvenes (12-13 años) con el de los más mayores (16-18 años). Sin embargo, la tendencia ha sido encontrar diferencias muy pequeñas salvo contadas excepciones. Estas variables que han presentado mayores diferencias han sido las relacionadas con introducir información al ciberespacio, concretamente, guardar información en los dispositivos con lo que se conectan a Internet y facilitar información personal a través de la Red, y las de interacción, especialmente, las relativas a contactar con conocidos en el ciberespacio, hacer uso de las TIC para cotillear y contactar con desconocidos.

3.3.4. Distribución de las variables independientes entre los menores no víctimas de ciberacoso

Como último paso en el análisis de la distribución de las dimensiones en la muestra, se estudió la distribución percentil de la mismas en el grupo de casos que no afirmaron haber sido víctima de ninguna de las conductas consideradas. El objetivo de este análisis es la obtención de una puntuación normativa en estas variables que podemos considerar como comportamiento usual de las TIC por parte de los adolescentes. El conocimiento del uso habitual nos permitirá estudiar en el grupo de víctimas la existencia de puntuaciones diferentes o anómalas que puedan ser los factores que subyacen al proceso de victimización.

A nivel general, se puede observar que las distribuciones entre los tres grupos de edad son similares hasta alcanzar el percentil 75, donde se encuentran diferencias. El patrón habitual es que a mayor edad, mayor uso hacen de las TIC. Así, en la variable guardar, el percentil 95 se sitúa en el grupo de los chicos en 60,71, que es la misma puntuación que obtienen los chicos entre 16 y 18 años en el percentil 75. Por tanto, el uso excesivo de guardar cosas en los sistemas con los que se conectan a Internet no será el mismo cuando hagamos referencia al grupo de los más pequeños que de los más mayores. Analizando los valores entre ambos sexos, se observa que las puntuaciones son iguales entre los chicos y las chicas en el grupo de 16 a 18 años pero es superior para el grupo de chicas en las otras edades.

Los baremos por tanto, serán distintos dependiendo de la edad y el sexo. Aunque hay algunas variables donde no se encuentran diferencias, como es el caso del uso de las TIC para ligar. En otras la variación es muy amplia, como en el caso del uso de las TIC para cotillear donde se observa que en el grupo de los chicos, hay una diferencia de 12 puntos entre los más pequeños y los más mayores, y esa diferencia se amplía hasta 23 puntos cuando las comparaciones por edad se hacen entre las chicas.

Tabla 72. Distribución del uso de las TIC por sexo y edad

			PERCENTILES						
VARIABLES INDEPENDIENTES	SEXO	EDAD	5	10	25	50	75	90	95
GUARDAR	Chico	12-13	41,50	41,50	41,50	41,50	46,70	55,40	60,71
		14-15	41,50	41,50	41,50	45,85	55,33	60,71	66,29
		16-18	41,50	41,50	41,50	50,24	60,71	65,91	70,91
	Chica	12-13	41,50	41,50	41,50	41,50	50,24	60,71	65,70
		14-15	41,50	41,50	41,50	50,24	60,43	65,70	70,91
		16-18	41,50	41,50	45,85	50,94	60,71	70,91	70,91
DAR	Chico	12-13	43,62	43,62	43,62	43,62	43,62	57,57	61,43
		14-15	43,62	43,62	43,62	43,62	53,85	64,88	68,98
		16-18	43,62	43,62	43,62	43,62	61,46	69,65	76,70
	Chica	12-13	43,62	43,62	43,62	43,62	43,62	61,57	69,25
		14-15	43,62	43,62	43,62	43,62	57,88	65,58	73,07
		16-18	43,62	43,62	43,62	43,62	61,29	72,88	76,78
MEDIO DAR	Chico	12-13	43,86	43,86	43,86	43,86	43,86	64,62	66,58
		14-15	43,86	43,86	43,86	43,86	53,84	65,00	76,67
		16-18	43,86	43,86	43,86	43,86	55,97	66,97	76,96

	Chica	12-13	43,86	43,86	43,86	43,86	43,86	64,62	66,17
		14-15	43,86	43,86	43,86	43,86	56,19	64,62	73,76
		16-18	43,86	43,86	43,86	43,86	64,62	66,17	76,46
COMPORTAMIENTO DESVIADO	Chico	12-13	44,82	44,82	44,82	44,82	48,79	56,06	63,56
		14-15	44,82	44,82	44,82	44,82	51,40	66,21	75,50
		16-18	44,82	44,82	44,82	48,79	56,06	68,80	79,56
	Chica	12-13	44,82	44,82	44,82	44,82	44,82	55,57	63,29
		14-15	44,82	44,82	44,82	44,82	50,91	60,71	69,63
		16-18	44,82	44,82	44,82	44,82	54,88	61,15	69,81
HERRAMIENTAS	Chico	12-13	36,94	36,94	42,28	47,77	57,77	66,34	71,33
		14-15	36,94	40,87	45,31	51,63	58,89	65,29	68,89
		16-18	36,94	39,99	44,95	51,36	61,49	69,39	74,58
	Chica	12-13	36,94	36,94	40,56	45,47	51,92	59,43	66,32
		14-15	36,94	36,94	40,87	46,28	52,89	60,01	65,51
		16-18	36,94	36,94	42,06	47,20	52,63	60,11	66,04
CONTACTO CONOCIDOS	Chico	12-13	26,36	26,36	40,72	47,80	53,90	60,50	63,36
		14-15	29,60	37,81	46,15	51,04	60,50	63,36	63,36
		16-18	29,60	38,35	46,94	53,54	60,50	63,36	63,36
	Chica	12-13	26,36	29,60	42,08	49,42	53,90	60,50	63,36
		14-15	29,60	38,84	45,94	51,04	57,60	63,36	63,36
		16-18	36,76	42,08	46,97	51,04	60,50	63,36	63,36
COTILLEAR	Chico	12-13	43,47	43,47	43,47	43,47	43,47	55,35	68,57
		14-15	43,47	43,47	43,47	43,47	52,38	68,57	68,57
		16-18	43,47	43,47	43,47	43,47	55,35	68,57	68,57
	Chica	12-13	43,47	43,47	43,47	43,47	43,47	68,57	68,57
		14-15	43,47	43,47	43,47	43,47	68,57	68,57	68,57

		16-18	43,47	43,47	43,47	55,35	68,57	68,57	68,57
LIGAR	Chico	12-13	45,11	45,11	45,11	45,11	45,11	74,09	74,09
		14-15	45,11	45,11	45,11	45,11	59,35	74,09	74,09
		16-18	45,11	45,11	45,11	45,11	59,85	74,09	74,09
	Chica	12-13	45,11	45,11	45,11	45,11	45,11	45,11	59,35
		14-15	45,11	45,11	45,11	45,11	45,11	59,85	74,09
		16-18	45,11	45,11	45,11	45,11	45,11	59,85	74,09
CONTACTO DESCONOCIDOS	Chico	12-13	42,04	42,04	42,04	42,04	52,56	61,28	64,56
		14-15	42,04	42,04	42,04	45,47	57,87	66,33	69,85
		16-18	42,04	42,04	42,04	50,03	61,31	68,89	71,95
	Chica	12-13	42,04	42,04	42,04	42,04	48,73	57,87	64,40
		14-15	42,04	42,04	42,04	42,04	57,87	65,00	69,84
		16-18	42,04	42,04	42,04	45,29	58,08	65,52	69,83
AGREGAR	Chico	12-13	37,79	37,79	37,79	54,74	64,02	64,02	64,02
		14-15	37,79	37,79	37,79	46,12	54,74	64,02	64,02
		16-18	37,79	37,79	37,79	46,42	55,39	64,02	64,02
	Chica	12-13	37,79	37,79	37,79	50,91	64,02	64,02	64,02
		14-15	37,79	37,79	37,79	46,42	55,39	64,02	64,02
		16-18	37,79	37,79	46,12	54,74	64,02	64,02	64,02
NO CONTROL	Chico	12-13	36,12	36,47	42,76	46,59	53,64	66,28	66,28
		14-15	36,12	38,76	43,31	48,95	62,69	66,28	74,39
		16-18	36,12	36,12	43,31	49,60	66,28	66,28	74,39
	Chica	12-13	36,12	36,47	40,05	46,02	50,62	66,28	66,28
		14-15	36,12	36,47	43,31	47,04	50,62	66,28	66,28
		16-18	36,12	36,12	43,31	47,20	66,28	66,28	74,39

3.3.5. Relación entre las variables independientes

Finalmente, dentro de los análisis bivariados se analiza la relación entre las variables independientes. A simple vista, se puede observar que todas las relaciones entre las variables resultan ser significativas, a pesar de que los valores de correlación son bajos. Esto puede ser causado por el número amplio de la muestra. En este sentido, resultan significativas las relaciones entre las variables "agregar a familiares" y "no control" con las de interacción y las de introducción, pero los valores de la correlación son inferiores a 0,10. Por lo tanto, la mayor o menor protección del menor no guarda relación con interactuar más ni con introducir bienes personales al ciberespacio. Concretamente, las únicas correlaciones que no han resultado ser significativas son las de la variables agregar, en relación a las variables no control, comportamiento desviado, ligar y el contacto con desconocidos.

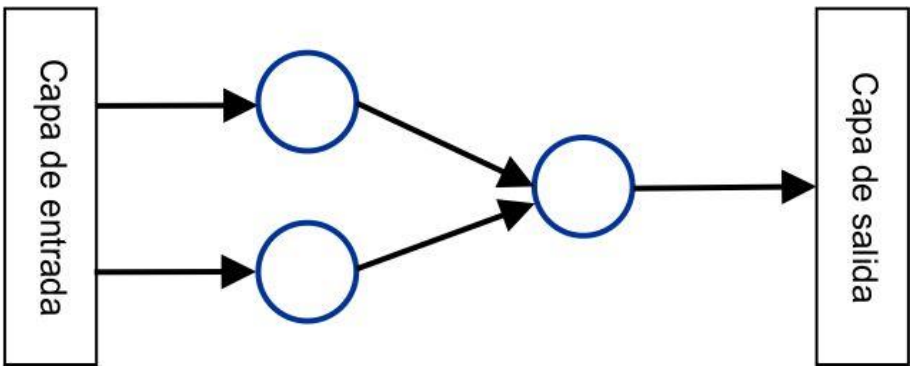
El resto de variables, todas relacionan entre sí, siempre de manera positiva. Lo que indica que los que más interaccionan, son a su vez los que más introducen bienes personales al ciberespacio. Aunque también se puede observar que las correlaciones son altas (entorno al 0,3) salvo dos excepciones. La correlación más alta (Rho=0,91) se encuentra entre facilitar datos personales a través de Internet y el número de medios empleados para facilitar información, entendiendo por tanto que, cuanta más información se facilita, más medios se emplean para ello. La otra excepción la encontramos entre el contacto con conocidos y el uso de las TIC para cotillear (Rho=0,43). De forma, que los que más emplean las TIC para contactar con conocidos, también las usan más para cotillear.

Tabla 73. Correlaciones entre las componente principales

	GUA.	DAR	MEDIO	AGRE.	NO CONT.	COM. DESV.	HERRA	CONO.	COTIL.	LIGAR
GUARDAR	1 .									
DAR	,294** 0,000	1 .								
MEDIO	,282** 0,000	,909** 0,000	1 .							
AGREGAR	,117** 0,000	,052* 0,018	,069** 0,002	1 .						
NO CONTOL	,057* 0,011	,057** 0,010	,057* 0,011	-0,097 0,000	1 .					
COMPOR. DESV.	,266** 0,000	,262** 0,000	,224** 0,000	-0,005 0,817	,096** 0,000	1 .				
HERRAMIE.	,184** 0,000	,210** 0,000	,209** 0,000	,120** 0,000	,107** 0,000	,287** 0,000	1 .			
CONOC.	,314** 0,000	,270** 0,000	,265** 0,000	,231** 0,000	0,014 0,532	,272** 0,000	,283** 0,000	1 .		
COTILLEAR	,302** 0,000	,206** 0,000	,185** 0,000	,076** 0,001	,088** 0,000	,285** 0,000	,157** 0,000	,429** 0,000	1 .	
LIGAR	,157** 0,000	,112** 0,000	,095** 0,000	0,015 0,493	,083** 0,000	,304** 0,000	,239** 0,000	,354** 0,000	,347** 0,000	1 .
DESCON.	,274** 0,000	,378** 0,000	,354** 0,000	0,031 0,158	,091** 0,000	,384** 0,000	,360** 0,000	,318** 0,000	,266** 0,000	,315** 0,000

4. Modelo predictivo de ciberacoso continuado no sexual de menores

Finalmente, se ha optado por crear un modelo predictivo que permita determinar los comportamientos de los menores que influyen en el proceso de victimización. Para ello se ha creado una Red Neuronal Artificial (RNA), que es un tipo de modelado de datos que se basa en el sistema de propagación de las redes neuronales biológicas. Son muchas las arquitecturas que puede adoptar una RNA. La más simple está formada por una capa de entrada donde se encuentran las "neuronas sensitivas", que se encargan exclusivamente de recibir información de entrada y propagarla hacia la siguiente capa o capa de salida.



Para que una neurona sensitiva se active y envíe información a las siguiente capa, ésta deber recibir (al igual que en las redes biológicas) un mínimo de información tal que supere el umbral de activación de dicha neurona. Una vez que la neurona ha sido activada, esta envía la información a la capa de salida. Entre estas neuronas existe una fuerza de conexión que vendrá determinada por el entrenamiento de la red y que denominamos peso. Los pesos pueden ser positivos (la neurona se activa) o negativos (la neurona se inhibe). Cuanto mayor es el peso mayor es la aportación de la variable al modelo, sin embargo en las RNA no tienen un rango de medida definido por lo que es difícil cuantificar la aportación de cada neurona a la salida. Si la información que llega desde la neurona sensitiva tiene suficiente energía para activar el umbral de la neurona de salida, entonces ésta emitirá una respuesta. Sin embargo esta cuestión varía en función de la arquitectura seleccionada.

La arquitectura empleada para el presente trabajo es del tipo "perceptrón multicapa". Es decir, se trata de una red neuronal artificial formada por múltiples capas. Cada capa está formada por una colección de neuronas que, de acuerdo a su ubicación en la RNA, recibe un nombre:

- Capa de entrada: recibe las señales de entrada de la red
- Capas ocultas: son capas que no tienen contacto con el medio exterior, sus elementos pueden tener diferentes conexiones y estas son las que determinan las diferentes tipologías de la red
- Capa de salida: recibe la información de la capa oculta y transmite la respuesta al medio exterior

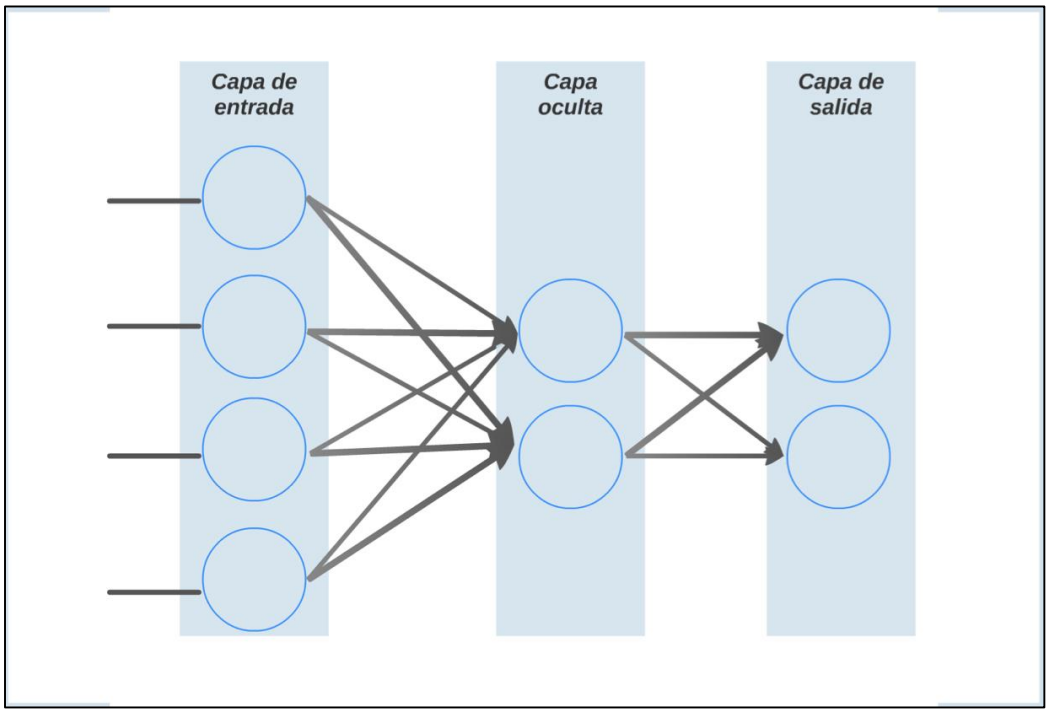


Ilustración 65. Ejemplo perceptrón

Este modelo permite que el peso y el umbral de las neuronas sean ajustables. Para ellos es necesario entrenar la red mediante el entrenamiento supervisado, que consiste en la modificación de los pesos a partir de las salidas de la red: cuando la salida se corresponde con el valor esperado no hay modificación de pesos, pero si la salida no se corresponde con el valor esperado se corrigen los pesos. Esta forma de corregir el error es denominado aprendizaje de *backpropagation*.

A continuación se describen los pasos que se han seguido para la construcción de un modelo de red neuronal capaz de discriminar entre "víctimas" y "no víctimas" de ciberacoso continuado.

4.1. Variables en el modelo

La **variable dependiente** se ha definido como la presencia o ausencia de victimización. Los sujetos que se identificaron como víctimas de algunas de las cuatro conductas de victimización señaladas (insultos, rumores, contacto repetido o marginar) fueron codificados con el valor 1 ("Víctima"), mientras que al resto de los sujetos se le asignó el valor 0 ("No víctima"). Se consideró la posibilidad de crear una variable que cuantificara el número de conductas sufridas que oscilara entre 0 "no haber sufrido ninguna" y 4 "haber sufrido las cuatro formas de victimización". Sin embargo, en los análisis previos se observó que las puntuaciones en las variables independientes no discriminaban entre esta categorización y por eso se optó por categorizar la variable en 1="víctima" y 0="no víctima".

Las **variables independientes** introducidas en el modelo fueron previamente categorizadas para diferenciar entre puntuaciones altas y bajas, y así poder discriminar una mayor interacción en el ciberespacio, mayor introducción de bienes y una menor protección. Las variables fueron estandarizadas con el grupo de las no víctimas pero teniendo en cuenta además el sexo y la edad de los sujetos, dado que los análisis anteriores habían demostrado que los chicos y las chicas no hacen el mismo uso y además también varía con la edad. Se estableció como punto de corte el valor obtenido en el percentil 70.

4.2. Preparación de la muestra

La muestra fue dividida en tres grupos: entrenamiento, validación y generalización. El grupo de entrenamiento es usado durante la etapa de aprendizaje, donde se van modificando los pesos para minimizar el error cometido entre la salida obtenida por la red y la salida esperada por el usuario. Con el fin de evitar un problema de sobreajuste, se usa un grupo de validación que permite controlar el proceso de aprendizaje. Y finalmente, el grupo "generalización" es empleado para evaluar la eficacia del sistema construido, es decir, para comprobar la validez predictiva del modelo.

La muestra de entrenamiento está formada por el 49,95% de la muestra total (n=1.018). Con el objetivo de que la red no sobreaprendiera a clasificar los casos de "no víctima", puesto que es el grupo mayoritario, se optó por extraer el mismo número de "víctimas" que de "no víctimas" (n=509 para cada grupo). La muestra de validación está compuesta por el 10% del total de la muestra (n=204). Y a diferencia de lo que se hizo con la muestra de entrenamiento, se optó por dejar el porcentaje real de "víctimas" y "no víctimas" para estimar el error de la red en un contexto muestral real. Finalmente, la muestra de generalización incluye los casos no representados en el entrenamiento y validación. Está compuesta por el 40% de la muestra total (n=816).

Tabla 74. División de la muestra para la construcción de la red

Total	Victima	782	38,4%
	No victima	1.256	61,6%
	Total	2.038	100%
Entrenamiento	Victima	509	50%
	No victima	509	50%
	% de la muestra total	1.018	49.95%
Validación	Víctima	78	38,2%
	No victima	126	61,8%
	% de la muestra total	204	10,01%
Generalización	Víctima	195	23.9%
	No victima	621	76.01%
	% de la muestra total	816	40.04%

Para la clasificación de los casos en función de los tres grupos se creó una nueva variable denominada "partición". Los casos incluidos en la muestra de entrenamiento se codifican con el valor 1, los casos destinados a la prueba de validación se codifican con el valor 0 y finalmente, los casos incluidos en la muestra de generalización se codifican con el valor -1.

La selección de los casos a cada grupo se realizó de forma aleatoria con los comandos de submuestreo del SPSS. A continuación se muestra la sintaxis del proceso de división de la muestra:

Muestreo entrenamiento:

```
DATASET ACTIVATE Conjunto_de_datos1.
DATASET CLOSE entrenamiento.
SORT CASES BY ID (A).
* Asistente de muestreo.
CSPLAN SAMPLE
  /PLAN FILE='H:\Nat_Internet\planperceptron.csplan'
  /PLANVARS SAMPLEWEIGHT=SampleWeight_Final_
  /PRINT PLAN
  /DESIGN STRATA=VICTIMIZACION_DIC
  /METHOD TYPE=SIMPLE_WOR ESTIMATION=DEFAULT
  /SIZE VALUE=509
  /STAGEVARS
INCLPROB(InclusionProbability_1_)
CUMWEIGHT(SampleWeightCumulative_1_)
POPSIZE(PopulationSize_1_)
SAMPSIZE(SampleSize_1_) RATE(SamplingRate_1_) WEIGHT(SampleWeight_1_).


DATASET DECLARE  entrenamiento.
CSSELECT
  /PLAN FILE='H:\Nat_Internet\planperceptron.csplan'
  /CRITERIA STAGES=1 SEED=RANDOM
  /CLASSMISSING EXCLUDE
  /SAMPLEFILE OUTFILE='entrenamiento'
  /PRINT SELECTION.
```

Muestreo validación:

```
CSPLAN ANALYSIS
 /PLAN FILE='H:\Nat_Internet\seleccion.csaplan'
 /PLANVARS ANALYSISWEIGHT=VICTIMIZACION_DIC
  /SRSESTIMATOR TYPE=WOR
  /PRINT PLAN
  /DESIGN
  /ESTIMATOR TYPE=WR.

* Asistente de muestreo.
CSPLAN SAMPLE
  /PLAN FILE='H:\Nat_Internet\planperceptronvalidacion.csplan'
  /PLANVARS SAMPLEWEIGHT=SampleWeight_Final_
  /PRINT PLAN MATRIX
  /DESIGN STRATA=VICTIMIZACION_DIC
  /METHOD TYPE=SIMPLE_WOR ESTIMATION=DEFAULT
  /SIZE MATRIX=VICTIMIZACION_DIC;1 78;0 126
  /STAGEVARSINCLPROB(InclusionProbability_1_)
        CUMWEIGHT(SampleWeightCumulative_1_)POPSIZE(PopulationSize_1_)
        SAMPSIZE(SampleSize_1_)                    RATE(SamplingRate_1_)
        WEIGHT(SampleWeight_1_).
DATASET DECLARE  validacion.
CSSELECT
  /PLAN FILE='H:\Nat_Internet\planperceptronvalidacion.csplan'
  /CRITERIA STAGES=1 SEED=RANDOM
  /CLASSMISSING EXCLUDE
  /SAMPLEFILE OUTFILE='validacion'
  /PRINT SELECTION.
```

Muestreo generalización:

```
GET FILE='H:\Base_Nat_Recod_edad_sexo.sav'.
DATASET NAME Conjunto_de_datos4 WINDOW=FRONT.
ADD FILES /FILE=*
  /FILE='Conjunto_de_datos3'
         /RENAME  (InclusionProbability_1_  muestreo  PopulationSize_1_
       PrimarioÚltimo SampleSize_1_ SampleWeight_1_ SampleWeight_Final_
       SampleWeightCumulative_1_ SamplingRate_1_=d0 d1 d2 d3 d4 d5 d6
       d7 d8)
  /DROP=d0 d1 d2 d3 d4 d5 d6 d7 d8.
EXECUTE.
DATASET CLOSE entrenamiento.
* Identificar casos duplicados.
SORT CASES BY ID(A).
MATCH FILES
  /FILE=*
  /BY ID
  /FIRST=PrimarioPrimero
  /LAST=PrimarioÚltimo.
DO IF (PrimarioPrimero).
COMPUTE  SecuenciaCoincidencia=1-PrimarioÚltimo.
ELSE.
COMPUTE  SecuenciaCoincidencia=SecuenciaCoincidencia+1.
END IF.
LEAVE  SecuenciaCoincidencia.
FORMATS  SecuenciaCoincidencia (f7).
COMPUTE  InDupGrp=SecuenciaCoincidencia>0.
SORT CASES InDupGrp(D).
MATCH FILES
  /FILE=*
  /DROP=PrimarioPrimero InDupGrp SecuenciaCoincidencia.
       VARIABLE LABELS  PrimarioÚltimo 'Indicador de cada último caso
       de coincidencia como primario'.
VALUE LABELS  PrimarioÚltimo 0 'Caso duplicado' 1 'Caso primario'.
VARIABLE LEVEL  PrimarioÚltimo (ORDINAL).
FREQUENCIES VARIABLES=PrimarioÚltimo.
EXECUTE.
RECODE muestreo (MISSING=-1).
EXECUTE.
DATASET ACTIVATE Conjunto_de_datos3.
ADD FILES /FILE=*
       /RENAME (InclusionProbability_1_ PopulationSize_1_ SampleSize_1_
       SampleWeight_1_  SampleWeight_Final_  SampleWeightCumulative_1_
       SamplingRate_1_=d0 d1 d2 d3 d4 d5 d6)
  /FILE='Conjunto_de_datos4'
  /DROP=d0 d1 d2 d3 d4 d5 d6.
EXECUTE.
```

4.3. Entrenamiento de la red

El trabajo con perceptrones multicapa implica la realización de sucesivas simulaciones del modelo con el fin de estimar de forma probabilística el valor de los coeficientes (o pesos) del modelo. La red ha sido entrenada en línea, o lo que es lo mismo, los casos han sido

introducidos uno a uno en el modelo lo que implica la modificación de pesos con cada caso incorrectamente clasificado. El algoritmo de optimización es el de pendiente de gradiente con una tasa de aprendizaje inicial de 0,5 y una reducción de la tasa de aprendizaje por época de 1. Se han llevado a cabo 100 simulaciones con la misma semilla aleatoria para la inicialización de los pesos de la red. El aprendizaje de la red se ha detenido cuando no se ha producido un cambio en los pesos en más de una época.

Para la selección del modelo se ha tenido en cuenta los siguientes criterios: tasa global de clasificación, tasa de verdaderos positivos, tasa de verdaderos negativos, tasa de falsos positivos, tasa de falsos negativos, tasa global de acierto y tasa global de error.

4.4. Resultados

El modelo ha quedado configurado con una capa de entrada compuesta por veintidós unidades más la neurona sesgo. Las veintidós unidades corresponden a los dos estados posibles de cada una de las 11 variables independientes consideradas. A su vez, cada neurona se conecta con la capa oculta que está compuesta por 9 unidades de procesamiento, más la neurona de sesgo. La función de activación de esta capa es sigmoide dado que es la función más ajustada para el caso de salidas dicotómicas.

$$sig\ (c) = \frac{1}{1 + \ e^{-c}}$$

Y finalmente, las unidades de procesamiento se conectan con la capa de salida que está compuesta por dos unidades, que se corresponde a los dos estados posibles de la variable victimización (1=Victima; 0 = No Victima). La función de activación de esta capa es la función softmax que maximiza las salidas dicotómicas de la red.

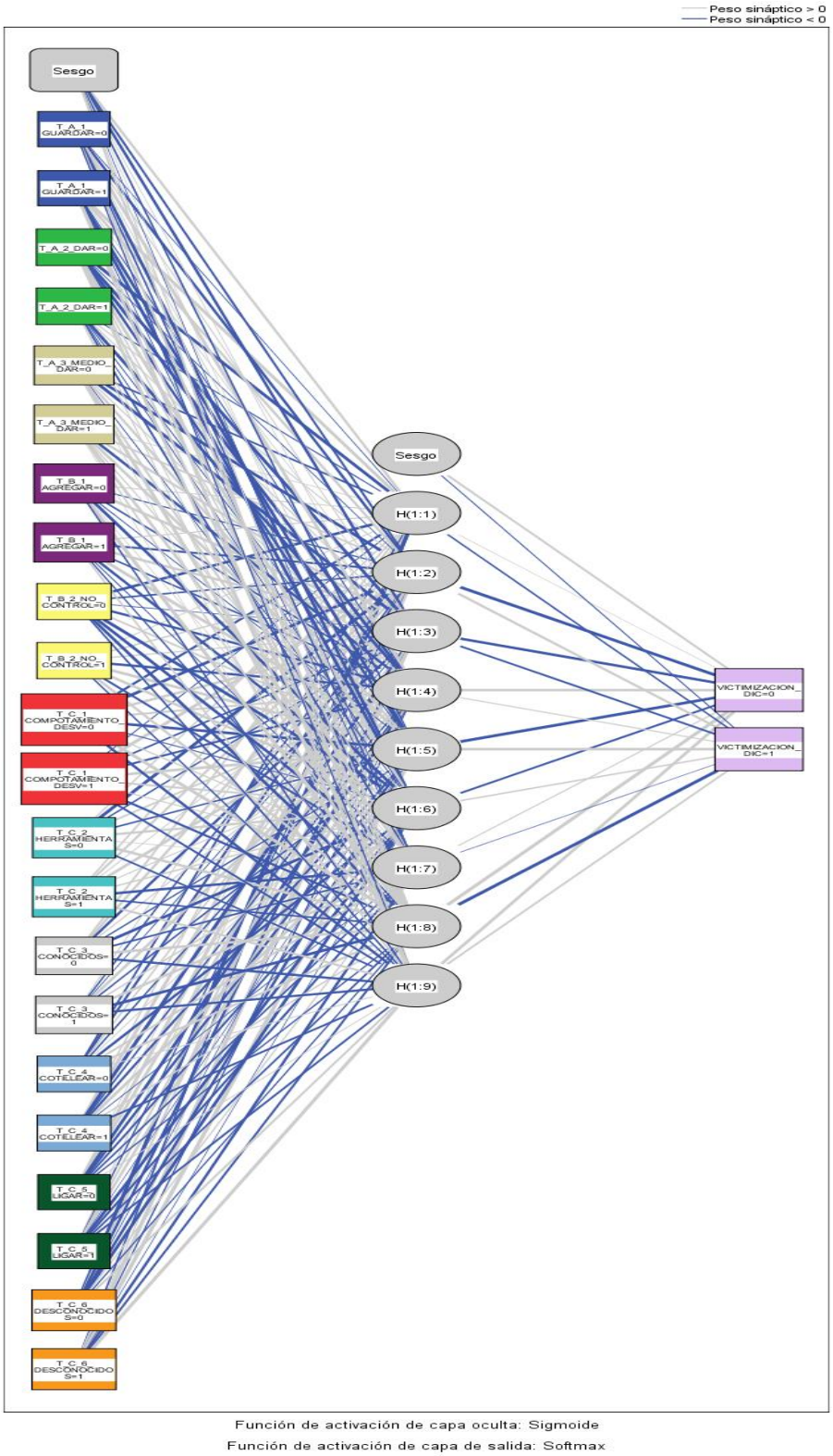


Ilustración 66. Diagrama de red

Como se puede observar en la tabla del resumen del modelo, el error cuadrático promedio obtenido en la fase de entrenamiento es de 592,762 con una tasa de clasificaciones incorrectas del 29%. El error se reduce en la muestra de validación hasta 123,484 con una tasa de errores de clasificación del 31,9%. En la fase de generalización, la tasa de clasificaciones incorrectas se mantiene en 31,9%.

Tabla 75. Resumen del modelo

Entrenamiento	Error de entropía cruzada	592,762
	Porcentaje de pronósticos incorrectos	29,0%
	Regla de parada utilizada	1 pasos consecutivos sin disminución del error
	Tiempo de entrenamiento	00:00:01,035
Prueba	Error de entropía cruzada	123,484
	Porcentaje de pronósticos incorrectos	31,9%
Reserva	Porcentaje de pronósticos incorrectos	31,9%

Variable dependiente: Victimización

a. Los cálculos del error se basan en la muestra de prueba.

La red obtiene unos buenos índices de clasificación correcta. Como se puede observar en la siguiente tabla, es capaz de clasificar correctamente el 68,1% de los casos. El modelo clasifica mejor a las "víctimas" que a las "no víctimas", aunque la diferencia no es grande. De forma concreta, la tasa de válidos positivos (clasificar correctamente

como víctima cuando un sujeto ha sufrido algún tipo de las agresiones medidas) es de 69,2%, mientras que la tasa de válidos negativos (clasificar correctamente como no víctima cuando un sujeto no ha sufrido ningún tipo de las agresiones medidas) es de 67,8%.

Tabla 76. Clasificación

		Pronosticado		
Muestra	Observado	No Victima	Victima	Porcentaje correcto
Entrenamiento	No Victima	364	145	71,5%
	Victima	150	359	70,5%
	Porcentaje global	50,5%	49,5%	71,0%
Prueba	No Victima	93	33	73,8%
	Victima	32	46	59,0%
	Porcentaje global	61,3%	38,7%	68,1%
Reserva	No Victima	421	200	67,8%
	Victima	60	135	69,2%
	Porcentaje global	58,9%	41,1%	68,1%

Variable dependiente: Victimización

El análisis de las curvas ROC nos permite analizar la sensibilidad de la red (la probabilidad de obtener un resultado positivo cuando el individuo es víctima) y la especificidad (la probabilidad de tener un resultado negativo cuando el individuo no ha sido victimizado). Los

valores del área debajo de la curva para ambos casos se muestran superiores a los generalmente aceptados (0,7) por lo que se puede afirmar que la red entrenada muestra poder predictivo.

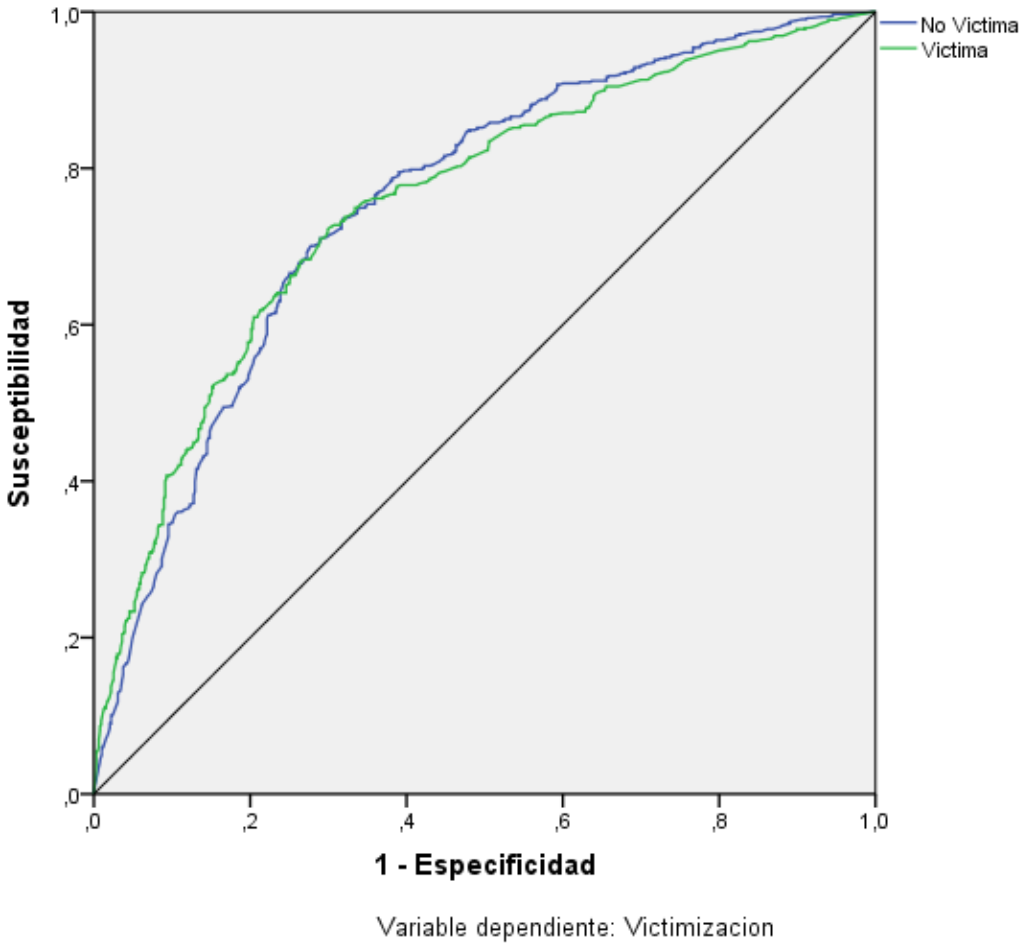


Ilustración 67. Curvas ROC

Tabla 77. Área debajo de la curva

		Área
Victimización	No Victima	,757
	Victima	,757

Del análisis de las variables incluidas en el modelo se extrae que todas las variables aportan información pero su importancia dentro del modelo varía del 3,5% al 100%. La variable con mayor importancia es el comportamiento desviado alcanzando un valor del 100%. En segundo lugar, aunque con gran diferencia con respecto a la primera, se encuentra el contacto con desconocidos, es decir, usar las TIC para conocer a personas nuevas. La tercera variable, es no agregar a las redes sociales a las personas que pueden ejercer un control, con un valor del 36%. La cuarta variable, es hacer uso de las TIC para cotillear a otras personas que alcanza un valor del 28,9%. La quinta, también es relativa a la interacción en el ciberespacio, concretamente, a hacer un mayor uso de las herramientas de comunicación disponibles en el ciberespacio (26,8%). En sexto lugar, queda el emplear mayor número de medios o herramientas para facilitar información personal real a otras personas (20,5%). En séptimo lugar, con una importancia normalizada del 17,9% se encuentra la falta de control ejercida por los padres y familiares sobre el uso de las TIC. El contacto con conocidos a través de las TIC se sitúa en octavo lugar con una importancia normalizada del 15%. En noveno lugar, se encuentra la variable guardar, es decir, almacenar archivos personales (fotos, vídeos, etc.) en los dispositivos con los que navegan por Internet. Las dos variables que

tienen menor importancia con valoras inferiores al 10% son facilitar datos personales reales a través de la red y usar las TIC para ligar.

Haciendo un análisis global de las variables, se observa como la interacción, es decir, realizar acciones en el ciberespacio que hacen más visible a una persona, son las que mayor influencia tiene en la victimización de los menores por ciberacoso continuado. Cuatro de las cinco primeras variables que tienen mayor peso en el modelo son formas de interacción en el ciberespacio (comportamiento desviado, contacto con desconocidos, cotillear y herramientas). Las otras dos variables incluidas en el modelo relativas a la interacción (contacto con conocidos y ligar) han quedado relegadas al octavo y al último lugar, respectivamente.

Pero no sólo la interacción tiene efecto en la victimización por ciberacoso continuado. El control que puedan ejercer los padres sobre el uso de las TIC así como ser admitido por sus hijos como amigos en las redes sociales, puede evitar que los menores puedan ser víctimas de esta forma de victimización.

Finalmente, también tiene efecto el introducir bienes en el ciberespacio. Aunque en menor medida que las otras dos variables, el hecho es que guardar datos personales reales en los dispositivos con los que se conecta Internet así como facilitar datos personales reales a otras personas a través de Internet, y sobre todo, si se emplean diferentes medios para hacerlo, supone un riesgo para los menores.

Tabla 78. Importancia de las variables independientes

	Importancia	Importancia normalizada
GUARDAR	,038	11,5%
DAR	,020	6,1%
MEDIO_DAR	,067	20,5%
COMPOTAMIENTO_DESV	,329	100,0%
HERRAMIENTAS	,088	26,8%
CONOCIDOS	,049	15,0%
COTILLEAR	,095	28,9%
LIGAR	,012	3,5%
DESCONOCIDOS	,125	37,9%
AGREGAR	,118	36,0%
NO_CONTROL	,059	17,9%

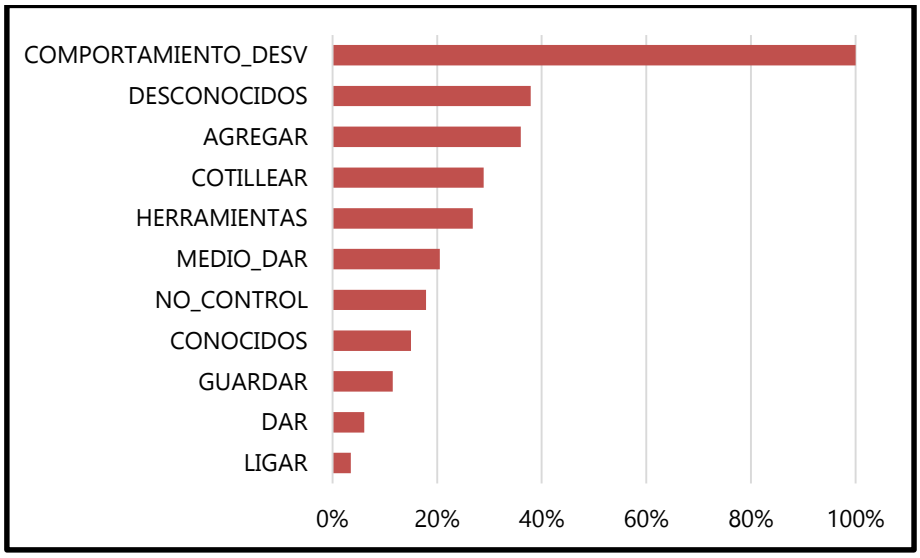


Ilustración 68. Importancia normalizada de las variables independientes

Tabla 79. Estimación de los parámetros

		Pronosticado										
		Capa oculta 1									Capa de salida	
Predictor		H(1:1)	H(1:2)	H(1:3)	H(1:4)	H(1:5)	H(1:6)	H(1:7)	H(1:8)	H(1:9)	[V=0]	[V=1]
Capa de entrada	(Sesgo)	,476	,452	,226	,299	-,026	,086	,227	,246	-,018		
	[GUARDAR=0]	,505	,435	-,364	,415	-,076	,634	-,545	-,276	-,507		
	[GUARDAR=1]	,274	,035	-,250	-,035	-,146	,586	-,225	,160	,606		
	[DAR=0]	,184	,011	,047	,398	-,367	-,131	,238	-,296	-,269		
	[DAR=1]	-,163	-,349	,524	-,265	,156	-,296	,422	,141	-,250		
	[MEDIO_DAR=0]	,080	,420	-,222	,406	-,249	,054	-,456	-,391	-,344		
	[MEDIO_DAR=1]	-,119	-,418	,217	,316	-,114	-,511	,188	-,020	,299		
	[AGREGAR=0]	,065	-,286	,312	,113	,297	,670	,231	,155	-,153		
	[AGREGAR=1]	,723	-,421	,578	,293	,035	-,473	,112	,008	-,036		
	[NO_CONTROL=0]	-,366	,055	-,115	-,232	,313	-,370	,403	-,374	-,049		
	[NO_CONTROL=1]	,426	-,547	-,436	,151	-,104	-,171	-,231	-,323	-,250		
	[COMPORTAMIENTO_DESV=0]	-,996	-,012	-,688	,649	,434	,804	-,541	,047	-,353		
	[COMPORTAMIENTO_DESV=1]	,984	-,061	,019	-,667	-,701	-,263	,505	,416	,494		
	[HERRAMIENTAS=0]	-,193	,369	,119	,359	,288	,139	,237	-,136	-,552		
	[HERRAMIENTAS=1]	,613	-,217	,248	,356	,090	,265	,006	,337	-,166		
	[CONOCIDOS=0]	,550	,123	-,049	-,345	,186	-,392	-,430	,008	-,024		
	[CONOCIDOS=1]	,088	-,256	-,236	-,493	-,744	-,444	,135	-,217	,137		
	[COTILLEAR=0]	-,298	,824	-,308	-,345	,203	-,302	-,611	,280	-,268		
	[COTILLEAR=1]	,302	,118	-,300	,397	-,092	,174	,603	,073	,666		
	[LIGAR=0]	,090	,415	-,134	,165	-,341	-,135	,377	,069	-,124		
	[LIGAR=1]	,469	-,232	-,425	,067	,277	,035	,016	-,223	,601		
	[DESCONOCIDOS=0]	-,637	,571	,449	-,102	-,096	-,038	,433	-,197	,192		
	[DESCONOCIDOS=1]	,291	-,316	,298	,099	-,364	-,565	-,132	,347	,544		
Capa oculta 1	(Sesgo)										,476	-,174
	H(1:1)										-,956	1,274
	H(1:2)										,383	-,276
	H(1:3)										-,171	,148
	H(1:4)										,614	,110
	H(1:5)										,594	-,554
	H(1:6)										,802	-,084
	H(1:7)										-,284	,360
	H(1:8)										,227	,406
	H(1:9)										-,103	,149

Capítulo II. Discusión, conclusiones y prospectiva

"La verdadera ciencia enseña, sobre todo, a dudar y a ser ignorante".

Miguel de Unamuno

Tras llevar a cabo el análisis de los resultados obtenidos, a continuación se realizará la discusión de los mismos, relacionándolos con las hipótesis de partida y las teorías criminológicas. Finalmente, se expondrán las conclusiones más relevantes, así como las críticas, las limitaciones encontradas y algunas reflexiones sobre lo que pueden ser futuras investigaciones en este campo.

1. Discusión

1.1. Prevalencia de la cibervictimización

Los resultados muestran que el ciberacoso continuado es un fenómeno presente entre los menores de la Provincia de Alicante y que un porcentaje significativo de ellos han sido víctimas de algún tipo de acto de ciberacoso continuado. Así, los porcentajes de victimización

obtenidos varían de un 4,8%, obtenido para la conducta de ser marginado de forma continuada a través de las TIC, un 14,4% cuando la conducta analizada es el contacto repetido no deseado habiendo solicitado previamente al agresor que cese tal acción, hasta el 23% de los jóvenes de la provincia de Alicante que han sido víctimas de insultos o ridiculización continuada. Hasta un 38,8% de la muestra de más de 2000 estudiantes de 12 a 18 años habría sufrido, al menos, alguna de las cuatro formas de victimización medidas. Siendo así, y comparando este resultado con el único estudio realizado hasta la fecha con una muestra representativa de la población española estudiante de secundaria en España, observamos que el porcentaje es significativamente superior en nuestro estudio. Y es que en 2007, el Defensor del Pueblo determinó que el porcentaje víctimas de ciberacoso en España era del 5,5% y aunque la diferencia puede parecer significativa, es razonable intuir que la misma se debe esencialmente a los diferentes objetos de medición en los distintos estudios, pero también a otras razones que se explicarán a continuación para reflexionar sobre la tasa de prevalencia que ofrece nuestro estudio.

En primer lugar, lo que pretendía medir el estudio del Defensor del Pueblo era el ciberacoso continuado causante de concretos efectos en los menores y no la victimización por actos o conductas específicas de ciberacoso como las aquí se han medido. Como también apunta Calmaestra (2011), el mencionado estudio no se centraba específicamente en el análisis de la cibervictimización por acoso o en la medición de conductas potenciales de ciberacoso, sino que más bien su objetivo principal era el de conocer mejor el fenómeno del maltrato entre iguales en la Enseñanza Secundaria Obligatoria en España, siendo

tangencial el análisis del ciberacoso mediante la inclusión de una única variable, que servía para medir en qué medida el maltrato entre compañeros también se realizaba a través de las TIC. Lo cierto es que cuando el objeto de estudio sí es el análisis de esta modalidad de victimización en particular y no el fenómeno del acoso escolar o del *bullying* en general, los porcentajes de prevalencia son claramente superiores. Así lo muestran otros estudios, aunque limitados a zonas geográficas concretas en España, como el de Ortega et al. (2008) realizado en 2007 y el realizado en el mismo año por Sureda et al. (2008). El primero de ellos, cifró que el porcentaje de escolares victimizados de forma continuada se situaba en un 1,5% y se elevaba a 9,3% cuando era de forma ocasional, tasa de prevalencia que hace referencia a una modalidad de victimización que sería más similar a la de "actos de ciberacoso continuado" que medimos en nuestro estudio. Por su parte, el estudio de Sureda et al. (2008) mostró porcentajes superiores, aunque tampoco tan altos como los encontrados en este estudio, concretamente entre el 8,8% y el 13,4% atendiendo al tipo de ciberacoso de que se tratase.

Es significativo observar, sin embargo, cómo las tasas de prevalencia de victimización por ciberacoso de otros estudios se van asemejando más a las que hemos presentado en este trabajo conforme las investigaciones se acercan en el tiempo. Así, Avilés cifró en 2009 el porcentaje de víctimas en Castilla y León y en Galicia en el 16,6% (Avilés, 2009b); en 2010, Buelga et al. en la Comunidad Valencia situaron el porcentaje de cibervictimización entre el 24,6% y el 29% (Buelga et al., 2010); y ese mismo año Estévez et al. (2010) encontraron que un 30,1% de los estudiantes habían experimentado alguna forma de ciberagresión.

Para explicar este significativo incremento de la victimización en el periodo que iría de 2006 (año en el que se realizan las mediciones del estudio del Defensor del Pueblo) a 2013, sí podría ser muy adecuada la teoría de las actividades cotidianas aunque, esta vez, en su formulación a nivel "macro". Si los cambios sociales pueden explicar incrementos en las tasas de criminalidad en general por el hecho de que los mismos hayan incidido en cambios en las actividades cotidianas de las personas que supongan un mayor acercamiento entre víctimas y agresores potenciales en ausencia de vigilantes capaces (Cohen y Felson (1979), y más recientemente, Aebi y Linde (2010), mostrando la validez de la teoría a nivel "macro" para las tendencias de la delincuencia en Europa), también puede, tanto el incremento significativo de los menores que han pasado a tener acceso a las TIC por la popularización de los *smartphones*, como por el aumento de horas que éstos pasan relacionándose con otros en el ciberespacio, la normalización de las redes sociales y los sistemas de mensajería instantánea como modo de interrelación social, explicar un significativo incremento de la victimización por conductas que antes sólo se podían dar a determinadas horas y en determinados momentos y ahora pueden producirse casi en cualquier momento. Para que un sujeto insultase o ridiculizase a otro delante de los demás, era necesario hace 10 años que todos los implicados estuvieran presentes (en el mismo espacio físico). Ahora ya no lo es, pues gran parte de los estudiantes están en las redes sociales, tienen perfiles y pueden ser objeto de burla y mofa sin que haya una cercanía espacio-temporal entre ellos. Y esta realidad apenas lo era en 2006, o por lo menos en comparación con lo que es en 2013. Así, como anteriormente hemos indicado, y apoyándonos en los datos del INE, desde el 2006 hasta el 2013 (fecha

en la que se obtienen los datos del presente estudio), el porcentaje del uso de las TIC por parte de los menores ha aumentado de manera significativa (INE, 2013). Concretamente, en 2006 el porcentaje de menores de entre 10 y 15 años que usaban Internet se situaba en el 72% mientras que en 2013 las cifras se elevaron el 92%, alcanzando el 99,6% cuando se amplía el margen de edad hasta los 26 años.

La idea de que el incremento de la prevalencia del ciberacoso sea debido principalmente al incremento de oportunidad de contacto entre agresores y víctimas potenciales también se refuerza si comparamos los porcentajes de victimización en el estudio nacional de victimización realizado sobre una muestra de adultos (Miró, 2013c), con los porcentajes de uso de las TIC entre los adultos en esa muestra y en la de los menores. Así, el porcentaje de victimización social en la muestra de adultos se sitúa en un 21%, pero al analizar sus actividades cotidianas se observa que sólo el 66% usaba la redes sociales, un 9,6% el chat y un 59,2% la mensajería instantánea (Miró, 2013a). Por el contrario, el porcentaje de victimización en la muestra de menores es superior (38,8%), pero es mayor el uso que hacen de las TIC: el 92% usa las redes sociales, 84% chatea y el 88,2% usa la mensajería instantánea. Es decir, que lo que incrementa el riesgo de victimización por ciberacoso no es el hecho de ser menor, sino el uso que se hace de las TIC y, concretamente, como se discutirá más adelante, de las concretas actividades que se realicen a través de ellas.

Si el significativo incremento en el uso del ciberespacio 2.0 como herramienta de comunicación social en los últimos cinco años puede explicar en parte la diferencia de la tasa de prevalencia en nuestro estudio frente a otros más antiguos, también es especialmente

relevante, a la hora de comparar tal tasa con otras investigaciones, tomar en consideración los sujetos objeto de investigación. Los estudios anteriormente citados, el llevado a cabo por el Defensor del Pueblo y otros estudios posteriores, tienen por objeto el ciberacoso escolar y, por tanto, el ciberacoso realizado sobre la víctima por parte de otros compañeros de colegio. Frente a ello, nuestro estudio tiene por objeto conductas de ciberacoso continuado pero no únicamente escolar, y es lógico que, si se acota el acoso, la victimización sea menos frecuente. De hecho, y si se analizan detenidamente los datos de prevalencia de estudios recientes, como el realizado por la Diputación Provincial de Alicante y el Centro Crímina (Miró, 2014a), donde se muestra claramente que no tiene su origen exclusivamente en el ámbito escolar, creemos que es importante empezar a adoptar una perspectiva más amplia del ciberacoso y no limitarla al *cyberbullying*, un fenómeno entre iguales y en las paredes (físicas o virtuales) del colegio. Hoy en día, pueden existir tanto acoso sistemático y continuado por parte de los compañeros del colegio como de otro tipo de organización o incluso de compañeros del ciberespacio, no teniendo por qué variar los efectos dañinos del mismo dependiendo del distinto ámbito de donde provengan este tipo de agresores, siempre que se realicen a través de las TIC. Como muestra el citado estudio, en la medida en que la comunicación de los menores a través de las TIC se amplía a otros ámbitos de su vida distintos al escolar, también se amplía la procedencia de las agresiones. Así, la cibercriminalidad social puede ser ejercida por los compañeros del colegio, pero también por compañeros de actividades extraescolares, conocidos de otros ámbitos del espacio físico como del lugar de vacaciones, conocidos a través de Internet, etc.; y además, este autor

de la agresión varía dependiendo del tipo de agresión y de la edad de las víctimas. Entre el 15% y el 38% de las agresiones que consisten en insultar y ridiculizar repetidamente, son realizadas por compañeros del colegio, mientras que entre un 20% y un 30% son realizas por conocidos ajenos al colegio, y entre un 14,7% y un 37% por desconocidos. En cambio, el contacto repetido no deseado a través de Internet, entre el 34% y 39% de las ocasiones, es ejercido por conocidos ajenos al colegio, entre el 25% y 34% por personas desconocidas por la víctimas, y entre el 2% y 5% por compañeros del colegio. Por último, la conducta de marginar suele realizarse entre compañeros del colegio hasta en un 52% de los casos dependiendo de la edad de la víctima, pero también hay un porcentaje importante de víctimas que lo son por parte de otros agresores distintos a los compañeros de colegio.

En definitiva, el ciberacoso continuado va más allá del *cyberbullying*, y aunque este fenómeno puede y debe seguir siendo estudiado, consideramos que, como se ha hecho en otros estudios, también es necesario investigar el fenómeno más amplio del ciberacoso. Y coherentemente con ello, es lógico pensar que las tasas de prevalencia sean más altas en el caso de que la victimización sea por conductas de ciberacoso continuado que por conductas de *cyberbullying*.

Para finalizar con la comparación de los resultados de prevalencia con otros estudios anteriores, merece la pena destacar que si tal comparativa se realiza con las investigaciones realizadas a nivel internacional, las tasas de prevalencia son más similares que si se compara con los estudios a nivel nacional, aunque la horquilla de victimización varía desde el 6% al 40%, dependiendo también de la

conducta medida (Patchin y Hinduja, 2012; Tokunaga, 2010). En todo caso, podemos observar, si se analizan todos los estudios de victimización por ciberacoso que ofrecen resultados de prevalencia, que hay un amplísimo margen de diferencia entre unos y otros. Este amplio margen se debe a los diferentes métodos empleados para determinar la prevalencia de victimización, desde la definición hasta el instrumento utilizado, pasando por la delimitación de la muestra y el procedimiento, entre otros aspectos (Sabella, Patchin y Hinduja, 2013; Tokunaga, 2010). Sin embargo, es evidente que hay una clara necesidad de establecer criterios comunes para la medición y para el análisis de este fenómeno que, en eso todos coincidimos, afecta a un gran porcentaje de menores, pero que también debe ser analizado, en cuanto a las consideraciones sobre su gravedad, con la "frialdad necesaria". Al fin y al cabo, y como más adelante se razonará, pese a que la tasa de victimización total obtenida es del 38,8%, resulta necesario recordar que dentro de esta tasa habrá conductas de muy diferente gravedad entre sí (en términos de afectación a los intereses personales psicológicos y de dignidad de la víctima) y, por lo tanto, no es recomendable, sin disponer de la información necesaria, generalizar la victimización como algo menor o como algo excesivamente problemático. Es evidente, en todo caso, que el ciberacoso a menores es una realidad que debe preocuparnos y obligarnos a establecer las mejores medidas preventivas para evitarlo.

Entrando ya en el análisis de las concretas formas de victimización, los resultados de nuestro estudio coinciden con los del de Juvonen y Gross (2008) en cuanto a que la conducta de acoso que más sufren los menores a través de las TIC, de las medidas en ambos estudios, son los insultos. Sin embargo, comparando los porcentajes

obtenidos, se muestra una amplia diferencia: 63% frente a 23% encontrado en nuestro trabajo. Esto probablemente se deba a que los autores no delimitan la cantidad de victimización, por lo que los datos resultan extraños si tenemos en cuenta que el 63% hace referencia a que en alguna ocasión algún menor ha sido insultado a través de las TIC, mientras que el 23% hace referencia a haber sufrido insultos de manera continuada en el tiempo. Como ya se señaló anteriormente, se ha preferido tomar en consideración sólo conductas que tengan una gravedad mínima, y ser objeto de algún insulto de forma esporádica y no continuadamente por parte del agresor, no la tiene. Probablemente, si la victimización medida hubiera sido recibir insultos sin establecer como criterio la continuidad, el porcentaje obtenido habría sido mucho mayor.

La segunda conducta que con mayor frecuencia sufren los menores es la difamación por medio de rumores o mentiras falsas a través de Internet que les afecten gravemente. El porcentaje encontrado de esta conducta alcanza el 23%, siendo mayor la victimización en chicas que en chicos. Las características espacio-temporales de Internet que permiten que los mensajes comunicativos se fijen de forma permanente en el ciberespacio produciendo efectos continuados, facilitan que se lleve a cabo esta conducta, pues ya no es necesario que los receptores del mensaje compartan espacio y tiempo con el emisor, sino que éste puede dejarse en un blog, en un perfil, o en un foro, y producir sus efectos comunicativos en cada momento que un usuario se convierta en receptor del mismo al leerlo. Y todo ello convierte a esta conducta en especialmente dañina, dado que el rumor o la mentira pueden dispersarse en el ciberespacio llegando a muchas más personas de las que podrían haberse enterado de ellas en el

espacio físico, así como perpetuarse en el tiempo, dañando a una misma persona de forma continuada en distintos momentos, tantos como aquéllos en los que los receptores lean el mensaje. Estas reflexiones podrían abarcar también, la forma de victimización anteriormente comentada, la de los insultos, y dada la prevalencia nos obligan a replantear los deberes de los proveedores de servicios en relación con el denominado "Derecho al olvido" que recientemente ha sido reconocido por el Tribunal de Justicia de la Unión Europea en el Caso Google Spain S.L. contra la Agencia Española de Protección de Datos (AEPD)[34], en su Sentencia de 13 de mayo de 2014. Aunque sobre ello se volverá más adelante, dada la prevalencia de estas conductas, y pese a saber que muchas de las formas de victimización podrán ser de escasísima gravedad únicamente reconocida como significativa en la esfera subjetiva de la propia víctima, es indudable que deben crearse mecanismos que permitan a los menores víctimas de estas conductas borrar los mensajes que afecten gravemente al honor, a la intimidad o a la dignidad de las personas.

Por otra parte, al comparar el porcentaje obtenido para esta conducta concreta de victimización con otros estudios como el de Xiao y Wong (2013), observamos que es superior: 23% en este trabajo frente a un 14,2% en el estudio de estos autores. El motivo de esta diferencia puede deberse, de nuevo, a que en este estudio no se limita la procedencia de la agresión al ámbito escolar, por lo que no es de extrañar que la prevalencia obtenida sea mayor. Y pese a que es sabido por otros estudios que esta conducta es importante en la dinámica del

[34] STJUE, 13 de mayo de 2014, asunto C-131/12.

acoso continuado a nivel escolar, también puede proceder la misma de otros ámbitos, como demuestra el estudio de la Diputación Provincial de Alicante y el Centro Crímina (Miró, 2014a).

En lo que se refiere a la conducta de contacto repetido no deseado como forma de hostigamiento a un menor, el porcentaje de quienes lo han sufrido es de un 14,4%. Este porcentaje es inferior al encontrado por Reyns (2010), que cifra la prevalencia en un 23,3%, pero algo superior al del 10% encontrado por Miró (2013c). En ambos estudios la muestra está compuesta por adultos, aunque la horquilla de edad es muy diferente entre los dos. La muestra obtenida por Reyns (2010) tiene una edad entre 18 a 26 años, mientras que la de Miró (2013c) varía de los 18 a los 65 años. A primera vista, esta divergencia puede parecer sólo coherente con las hipótesis planteadas en el estudio de Miró (2013c), que mostraría una menor victimización en adultos (de 18 a 65 años) que en los jóvenes de nuestra muestra (de 12 a 18 años), y extrañarían los resultados de Reyns de incremento de los porcentajes de victimización hasta el 23,3%. Sin embargo, de acuerdo a la teoría de las actividades cotidianas en el ciberespacio, esta forma de victimización se hace menos probable conforme se entra en la edad adulta, dado que es en la adolescencia y en la primera adultez cuando se usan más las TIC como vehículo de comunicación social, y esto va disminuyendo a partir de la incorporación al trabajo y otros factores relacionados con la cotidianeidad de los adultos. Si reparamos, en cambio, en la edad de la muestra del estudio de Reyns (2010) y observamos con detenimiento los datos de victimización por rangos de edad del estudio realizado por la Diputación Provincial de Alicante y el Centro Crímina (Miró, 2014a), veremos que las hipótesis se ven confirmadas. En el caso del estudio de Reyns (2010) el intervalo de edad

está fijado en un marco en el que es más probable esta forma de victimización (entre 18 a 24 años), de forma que se podría decir que el uso de las TIC como instrumento de comunicación personal continúa o incluso se incrementa en los primeros años de adultez, por ejemplo, en el periodo de estudios universitarios. Esto, como hemos señalado, sería coherente con el hecho de que en el estudio sobre victimización de jóvenes en la Provincia de Alicante (Miró, 2014a) se observa como la probabilidad de ser víctima de esta conducta se incrementa conforme se va creciendo en edad. Así, la prevalencia de victimización para los menores entre 12 y 13 años se sitúa en un 10%, incrementándose a 12,2% cuando la edad de los sujetos es de 14 y 15 años, y llegando al 20,1% cuando los sujetos tienen entre 16 y 18 años. Siguiendo como pauta la edad de la muestra, se podría unir a continuación el 23,3% que obtiene Reyns (2010) para el grupo formado por los que tienen entre 18 y 26 años. De acuerdo con los datos y la teoría, la curva de victimización comenzaría a los 12-13 años, y seguiría aumentando hasta llegar un punto que empieza a decrecer, que coincide con el momento en que se entra completamente en la vida de adulto y dejan de usarse las TIC con la misma intensidad.

Finalmente, la cuarta forma de victimización medida es la exclusión o marginación a través de las TIC. Esta es la forma de victimización que más se relaciona con el *cyberbullying* propiamente dicho y la que los menores afirman sufrir en menor medida. El porcentaje obtenido, del 4,8%, es muy inferior al encontrado en otros estudios que sitúan la prevalencia en torno al 30% (Xiao y Wong, 2013). Pero de nuevo, el bajo nivel encontrado puede deberse a una cuestión de medición, dado que en nuestro estudio hemos preferido limitarnos a la marginación sufrida de forma continuada, dejando fuera actos de

bagatela como haber sido excluido o marginado por alguien puntualmente.

1.2. Características demográficas de las víctimas de ciberacoso continuado

Respecto al análisis del género de las víctimas de ciberacoso continuado, los resultados encontrados muestran que son las chicas quienes lo sufren en mayor medida. Los datos son aparentemente claros en este sentido, ya que en todos las conductas medidas, los porcentajes obtenidos por las chicas son superiores al de los chicos. Sin embargo, es en la victimización por contacto repetido no deseado y en la victimización por marginación o exclusión de forma continuada donde se encuentran las mayores diferencias entre ambos sexos (63% chicas frente a 37% chicos). Esta amplia diferencia entre ambos sexos se reduce, aunque sigue siendo estadísticamente significativa, cuando se atiende a la conducta por insultos continuados, encontrando que en el 57,6% de los casos, las víctimas son chicas, frente al 42,4%, que son chicos. Y se reduce aún más, dejando de ser así una diferencia estadísticamente significativa, en la victimización por difamación de rumores, aunque el porcentaje de chicas es ligeramente superior, 52,5% frente a 47,5%.

Los resultados encontrados son acordes a la mayoría de los estudios publicados hasta la fecha. Pese a que hay algunos que defienden que son los chicos quienes más sufren el ciberacoso (Avilés, 2009b; Li, 2007a) y otros que, simplemente, no encuentran diferencias de género en la cibervictimización (Calvete et al., 2010; Finn, 2004; Holt

y Bossler, 2009; Jackson y Cohen, 2012; Juvonen y Gross, 2008; Olenik-Shemesh, 2012; Vandebosch y Van Cleemput, 2010; Wigderson y Lynch, 2013; Williams y Guerra, 2007), la mayoría afirman que son las chicas las que más lo sufren (Brighi et al., 2012; Calmaestra, 2011; Hoff y Mitchell, 2009; Kowalski y Limber, 2007; Li, 2007b; Ortega et al., 2008a; Smith et al., 2006; Wang et al., 2009; Ybarra et al., 2006; Ybarra et al., 2007).

La explicación en la que parecen coincidir la mayoría de los autores, es que la violencia verbal siempre ha sido una práctica más habitual entre las chicas que entre los chicos. Todos los estudios realizados sobre *bullying* tradicional, así como en otras formas de delincuencia, concluyen que son los chicos quienes en mayor medida protagonizan las agresiones físicas directas e indirectas y las chicas tienden a participar en formas de violencia psicológica y emocional (Hinduja y Patchin, 2008). Por tanto, no es de extrañar que los resultados indiquen que son las chicas las que más lo sufren puesto que las formas de cibervictimización medidas en el presente estudio se caracterizan por ser de tipo verbal y de exclusión.

En lo relativo al contacto repetido no deseado a través de las TIC, los resultados también son acorde a los encontrados por Reyns (2010). Las chicas lo sufren más que los chicos y esto puede ser debido, como han argumentado Bossler y Holt (2009), a que pueden ser entendidas como un blanco potencial (*suitable target*). En cambio, como ha explicado Miró (2012), el contacto repetido es también una forma de ciberacoso propia de la violencia entre la pareja a través de las nuevas TIC, y del mismo que en el espacio físico, también la sufren más las chicas (Miró, 2014a).

No obstante, hay que ser cautos a la hora de hacer afirmaciones respecto al género de las víctimas, pues como se muestra al principio de este trabajo, en muchas ocasiones las diferencias porcentuales encontradas son leves, no superiores a 5 puntos (Brighi et al., 2012; Ybarra et al., 2006; Ybarra et al., 2007). Estas diferencias pueden ser estadísticamente significativas, no por una diferencia real, sino por la influencia de las grandes muestras empleadas en los estudios, que en muchas ocasiones son superiores a los 1000 sujetos. Por todo ello, el género no es determinante en la probabilidad de cibervictimización, sino las actividades que realizan los menores en Internet que pueden situarles en una posición de riesgo (Miró, 2012).

Respecto a la edad de las víctimas, la única forma de victimización que presenta diferencias significativas entre los diferentes grupos de edad es el contacto repetido no deseado, de forma que a mayor edad, mayor número de víctimas se concentran. En el resto de formas de victimización por ciberacoso continuado no se encuentran diferencias entre los grupos, y aunque los resultados son concordantes con la mayoría de los estudios publicados hasta el momento, en los que se afirma que la edad no es un factor relevante para la victimización (Beran y Li, 2007; Didden et al., 2009; Juvoven y Gross, 2008; Katzer et al., 2009; Patchin y Hinduja, 2006; Smith et al., 2008; Varjas, Henrich, y Meyers, 2009; Wolak et al., 2007; Ybarra, 2004), es cierto que hay otros autores que sí las han encontrado, determinando que la edad es relevante (Dehue et al., 2008; Hinduja y Patchin, 2008; Kowalski y Limber, 2007; Slonje y Smith, 2008; Ybarra y Mitchell, 2008; Ybarra et al., 2007). Probablemente, estos resultados aparentemente incoherentes se deben a los diversos rangos de edad empleados en los estudios (Tokunaga, 2010). Y es que generalmente, se suelen emplear

dos tipos de muestras, las compuestas por adolescentes cuyas edades oscilan entre los 10 y los 18 años, y las compuestas por adultos jóvenes, generalmente estudiantes universitarios, con edades comprendidas entre los 18 y 24. La falta de estudios con muestras con un rango amplio de edad nos imposibilita hacer un análisis real sobre la influencia de edad, aunque todo apunta a que se trata de un factor relevante en tanto en cuanto afecta a las actividades que desarrollan los usuarios Internet y, por consiguiente, su probabilidad de estar en riesgo.

1.3. Conductas de riesgo de los menores en Internet

Desde que se creara Internet, su uso ha ido creciendo paulatinamente experimentando un gran salto en la última década, especialmente entre los jóvenes, quienes lo han convertido en el medio para desarrollar su vida personal y social. Al hacerlo, realizan actividades cotidianas que les sitúan en una posición de riesgo, entre las que se encuentra la introducción voluntaria o involuntaria de bienes en el ciberespacio, cuyo acto supone el primer paso para que puedan ser atacados. En este sentido, se ha podido comprobar como los menores ceden información personal sobre ellos mismos a otras personas a través de las TIC y guardan en los dispositivos con los que navegan por Internet todo tipo de información personal, dando lugar a que éstos estén accesibles a otros usuarios. Asimismo, la cesión de datos personales reales a través de Internet correlaciona positivamente con el mayor número de medios empleados para tal fin y con guardar mayor información personal en los dispositivos electrónicos, lo que

indica que los que almacenan mayor información, son a su vez los que más información facilitan, empleando más medios para hacerlo.

En todo caso, por muchos bienes que se introduzcan en el ciberespacio, éste, como ámbito de intercomunicación personal, exige una interacción entre los usuarios. Quienes han tratado de aplicar la Teoría de las Actividades Cotidianas al ámbito de la cibercriminalidad han intentado relacionar la victimización con el uso de horas de Internet. En realidad lo importante para ser visible en el ciberespacio no es pasar horas en él, sino pasarlas interaccionando, relacionándose con otros, haciéndose presente para los demás. En este sentido, son múltiples las herramientas de comunicación que emplean para comunicarse con otras personas, como el correo electrónico, los foros, salas de chat, blogs, etc. Pero sin duda, son la mensajería instantánea y las redes sociales, las dos herramientas más utilizadas por los jóvenes. Su uso suele estar destinado a establecer contacto con personas conocidas en el medio físico, pero también para realizar otras conductas, que son consideradas por algunos autores como factores de riesgo. Entre ellas encontramos usar las herramientas de comunicación para ligar, cotillear a otras personas, conocer a personas nuevas, pero también para ejercer la violencia contra otras personas. Todos estos factores determinan la mayor visibilidad de los usuarios en el ciberespacio: si ligas, eres visible para potenciales agresores; si contactas con personas, eres visible y, desde luego, si realizas conductas desviadas, eres claramente visible para quien, como respuesta, puede decidir atacarte.

Sumada a las prácticas de interacción e introducción de datos en el ciberespacio, se observa que el control que ejercen los padres

sobre lo que hacen sus hijos en el ciberespacio es muy bajo y, en ocasiones, nulo. Y tampoco es usual por parte de los menores, realizar prácticas que faciliten la vigilancia por parte de familiares como por ejemplo, agregar a los padres a las redes sociales. Son muy pocos los menores que lo hacen, y aunque más de la mitad sí que comparten el ordenador con otros miembros de la familia, menos del 25% ve controlada su actividad con las TIC.

Se ha podido comprobar que estas prácticas de riesgo las realizan más los que tienen entre 16 y 18 años, pues en todas las conductas medidas, salvo en la de agregar a los familiares a las redes sociales, la tendencia es la misma: conforme aumenta la edad, aumentan las actividades en el ciberespacio. Sin embargo, las diferencias no son muy amplias, pues en la mayoría de los casos, las diferencias encontradas entre los que tienen 14-15 años y los que tienen 16-18 años, no son estadísticamente significativas.

Situación parecida se encuentra cuando se comparan las conductas de las chicas y de los chicos. Las chicas facilitan más información personal real a través de Internet y emplean más las TIC para contactar con conocidos y cotillear. En cambio, los chicos emplean más herramientas de comunicación y las usan más para ligar, contactar con desconocidos y para llevar a cabo conductas desviadas. Aunque de nuevo, las diferencias en el uso tampoco son tan claras.

Que la edad y el sexo de los menores no sean determinantes en la victimización pone de manifiesto que lo realmente importante es aquello que hagan los menores en el ciberespacio. Estudios previos apuntan esto mismo, que las actividades cotidianas de los usuarios en Internet determinan el riesgo de victimización (Bossler y Holt, 2009;

Choi, 2008; Holt y Bossler, 2009; Hutchings y Hayes, 2008; Marcum, 2008; Marcum et al., 2010; Miró, 2013c; Ngo y Paternoster, 2011; Pratt et al., 2010; Reyns, 2010) y además, algunas actividades tienen mayor efecto que otras dependiendo del tipo de ataque al que estemos haciendo referencia (Miró, 2014c; Ngo y Paternoster, 2011). Los resultados obtenidos en este estudio al comparar las actividades cotidianas del grupo de víctimas con el grupo de no víctimas son claros en este sentido: las víctimas realizan un mayor número de actividades en el ciberespacio que las no víctimas.

Las víctimas de insultos continuados a través de Internet obtienen puntuaciones mayores en todas conductas medidas, salvo el control paterno, siendo especialmente relevante la diferencia en el comportamiento desviado, es decir, en realizar ataques de cibercriminalidad social sobre otras personas, y mantener contacto con desconocidos. Similares resultados se han encontrado para el resto de formas de victimización. Cuando se han analizado las diferencias para la victimización consistente en difusión de rumores o mentiras de manera continuada, se repetían las variables de comportamiento desviado y contacto repetido, pero añadiendo además como variable relevante el uso de las TIC para establecer relaciones sentimentales con otras personas. Respecto a las víctimas de contacto repetido no deseado, guardan más información en los sistemas con los que se conectan a Internet, facilitan más información personal real a otras personas a través de Internet, realizan más comportamientos desviados, usan más las TIC para cotillear a otras personas y para contactar con desconocidos, que las no víctimas. En cambio, cuando se compara al grupo de los sujetos que han sido marginados de manera continuada con los que no lo han sido, son tres las variables en las que

se encuentran diferencias estadísticamente significativas, siendo éstas además las que de manera sistemática se repiten en las otras formas de victimización: comportamiento desviado, uso de las herramientas de comunicación y contacto con desconocidos.

Los resultados del modelo ponen el acento en el comportamiento desviado como la conducta que con mayor diferencia predice la cibervictimización. Esto es perfectamente coherente con la teoría de las actividades cotidianas y con la teoría criminológica de Marcus Felson que en repetidas ocasiones ha puesto de manifiesto la alta tasa de victimización de los agresores (Felson, 1998). Lo cierto es que, tanto realizar *sexting* como agredir a otras personas a través de Internet va a determinar la probabilidad de ser víctima de ciberacoso continuado. Y como han mostrado otros estudios, no sólo está relacionado con la cibercriminalidad social (Calmaestra, 2011; Holt y Bossler, 2009; Ngo y Paternoster, 2011; Reyns, 2010), también es un predictor para otras formas de victimización (Bossler y Holt, 2009; Choi, 2008; Ngo y Paternoster, 2011). Bossler y Holt (2010) relacionan el comportamiento desviado con el contacto con agresores motivados. Reyns (2010), por su parte, entiende que realizar este tipo de actividades expone a los usuarios a los potenciales agresores que también participan en las mismas actividades y que, por lo tanto, la proximidad entre ellos, aumenta la posibilidad de que se agredan entre ellos mismos (p.124). Puede hipotetizarse que, la razón de que esta forma de interacción sea un significativo factor de riesgo, se deba a que la victimización sufrida por un usuario sea generalmente consecuencia o respuesta a un ataque previo por su parte. De acuerdo con Vandebosch y Van Cleemput (2008), los motivos que llevan a un joven a agredir a otro a través del ciberespacio son muchos. Puede ser

como acto de venganza, como respuesta al acoso recibido anteriormente ya sea a través de Internet o en el espacio físico, como respuesta a una discusión previa, por desprecio o, incluso, por diversión o mostrar a otros sus habilidades con las TIC. Sea por eso o no, y siguiendo la argumentación que nosotros hemos defendido, parece bastante claro que hacer *sexting* y agredir verbalmente a otros a través de Internet sea de las conductas que más haga visibles a quienes las realizan y, por ello, potencialmente adecuados para los agresores. El que insulta se hace visible para otros, así como el que de otros modos acosa a sus víctimas. El sujeto se hace visible también al compartir las imágenes con quien en ese momento es su pareja, pero posteriormente se puede aprovechar ese material íntimo para ridiculizarla. Sea como fuere, lo que es cierto es que el ciberagresor con su actuar cotidiano se hace visible y así incrementa el riesgo de convertirse en víctima.

Si la interacción es la forma de hacerse visible en Internet y la visibilidad es condición básica para ser objeto de victimización, fácilmente puede comprenderse que otra conducta que, conforme a los resultados de nuestro estudio, aparezca altamente relacionada con la probabilidad de ser víctima de ciberacoso sea el contacto con desconocidos. De acuerdo con los resultados del modelo, estaríamos ante la segunda variable que con mayor fuerza incide en el proceso de victimización. Reyns (2010) entiende que contactar con extraños a través de Internet acerca a los usuarios a los agresores motivados, es decir, les aproxima a ellos. Distinto a lo entendido por Marcum (2008) quien considera que el contacto con desconocidos es una cualidad de la víctima, es decir, una característica del usuario de Internet que le convierte en un blanco adecuado ("targuet suitable"). En la línea de lo

que argumenta Miró (2013c), ya hemos señalado que el contacto con desconocidos lo que conlleva es un aumento de visibilidad de la víctima potencial para el agresor motivado. Dado que en el ciberespacio las distancias desaparecen (Miró 2011; Yar, 2005), todos los usuarios, tanto agresores como víctimas, se encuentra a la misma distancia, es decir, existe proximidad entre todos ellos. Lo que determina la victimización, que el agresor se decante por unos o por otros, depende de la visibilidad de estos. Pues como argumenta Cohen et al. (1981) la exposición al delincuente motivado viene determinada por la accesibilidad y la visibilidad y sucede cuando el delincuente sabe de la existencia del blanco potencial. En Internet todos los usuarios, hasta que se han conocido, podrían considerarse desconocidos entre sí, por lo que no puede pretenderse que por el hecho de contactar con otros a través de Internet ello suponga algo de por sí "peligroso". Pero es indudable que el mayor contacto incremente la posibilidad de hacerlo con aquellos que puedan realizar una conducta criminal.

Esta altísima importancia de la visibilidad de los objetivos adecuados para que lo sean de agresores potenciales que se especifica en el ciberespacio en el macro-constructo "interacción", se constata en que además del comportamiento desviado y el contacto con desconocidos, haya otras dos variables de tal categoría que, de acuerdo al modelo, estarían entre las cinco variables que con mayor fuerza predicen la victimización. Éstas son hacer un mayor uso de las TIC para cotillear a otras personas y hacer un mayor uso en general de las herramientas de comunicación. Ésta última variable ha sido barajada por muchos autores como un predictor fuerte. Concretamente, el uso de las salas de chat (Marcum et al., 2010), el correo electrónico (Marcum et al., 2010), la mensajería instantánea (Marcum et al., 2010;

Ngo y Paternoster, 2011; Reyns, 2010;) o las redes sociales (Reyns, 2010). Sin embargo, los resultados de este estudio muestran como todo los jóvenes hacen uso de éstas herramientas, sean víctimas o no. La diferencia entre un grupo y otro reside en la cantidad, de forma que las víctimas las usan más que las no víctimas, y ya no tanto en el número horas sino en la cantidad de herramientas que se emplean. El mayor número de herramientas empleadas aumenta la visibilidad de los sujetos en el ciberespacio y la probabilidad de victimización. Esto es un cambio importante respecto a trabajos anteriores: el riesgo no deviene de usar las TIC, sino de cómo se usan las TIC y, más concretamente, de que el sujeto se haga visible por el hecho de usar las TIC. Si alguien, por ejemplo, pasa cinco horas al día en Internet jugando a un juego *online*, se hace claramente visible para aquellos que juegan *online* y que pueden ser o no potenciales agresores. Si es la única actividad que él realiza en el ciberespacio, al igual que el que simplemente está cinco horas contestando emails o el que abre la red social "Facebook" durante ese tiempo, será visible pero sólo para ese entorno. Si, en cambio, una persona juega *online*, utiliza el correo electrónico, tiene perfiles en distintas redes sociales, usa la *webcam* para comunicarse con otros, etc., esto es, si interacciona más, se hará visible para muchas más personas y, por ello, también para los potenciales agresores.

Finalmente, y dentro del macro constructo interacción, también el contacto con conocidos y el empleo de las TIC para establecer relaciones sentimentales se muestran como factores de riesgo de la victimización por ciberacoso continuado. ¿Significa esto que es peligroso para la victimización por ciberacoso el uso de las TIC para realizar una actividad social tan importante como conocer personas y mantener relaciones sentimentales? En realidad lo peligroso es hacerlo

con mucha frecuencia. La mayoría de los menores emplean las TIC para contactar con conocidos y para establecer relaciones sentimentales, pero las víctimas lo hacen con mayor frecuencia que las no víctimas. La ventaja del modelo que hemos construido es que este factor, por sí mismo, no es de gran relevancia, pero unido a otro conjunto de variables puede conformar un actuar cotidiano que haga especialmente visible al que lo siga y, por tanto, que incremente su riesgo de victimización.

En definitiva, se acepta la hipótesis de que a mayor interacción, es decir, a mayor número de actividades que hacen visible a un menor en el ciberespacio, mayor será la probabilidad de que sufra ciberacoso continuado, así como queda demostrado que algunas de ellas, las conductas desviadas, el contactar con desconocidos o el usar una gran variedad de tecnologías de comunicación hacen especialmente visibles a los usuarios de Internet y les exponen a ser víctimas de ciberdelitos. Y esto nos lleva a dos reflexiones importantes: la primera, es que lo peligroso no es el día a día en el ciberespacio, sino lo que se hace durante ese día a día que incrementa la posibilidad de contactar con potenciales agresores. No hay que demonizar la tecnología, sino ayudar a los menores a comprender los riesgos que la misma conlleva y, en particular, los que vienen unidos a determinadas conductas ya analizadas en particular. La segunda reflexión es que se pueden crear estrategias preventivas, especialmente de tipo educativo, pero también otras, que nos ayuden a todos a actuar de forma más segura en el ciberespacio. En este sentido las propias redes sociales debieran establecer pautas de uso seguro que expliquen los riesgos del comportamiento desviado, del contacto con desconocidos y demás.

Y además de las diferentes conductas de interacción que hacen al sujeto visible en el ciberespacio, encontramos que la falta de supervisión sobre las actividades de los menores en Internet también incide en el proceso de victimización. El modelo muestra que el hecho de no agregar a los padres, hermanos u otros familiares a las redes sociales favorece la victimización. Del mismo modo que no compartir el ordenador con otras personas o no tener un control directo sobre el uso de los dispositivos con los que se conectan a Internet. Similares resultados a los encontrados por Marcum (2008), quien determinó que quienes tienen mayores privilegios por parte de los padres en el uso de Internet también son los que en mayor medida sufren la victimización. En este sentido, Apple et al. (2014) determinaron que los que tienen peor comunicación con los padres son los que sufren más agresiones en Internet y que, en cambio, aquellos los que si la poseen tienen experiencias positivas en el uso de Internet. Pero los estudios no son del todo concluyentes en este sentido (Sasson y Mesh, 2014) pues hay autores que han encontrado que el control paterno es ineficaz (Lee y Chae, 2007; Shin y Huh, 2011), lo cual podría deberse a que actualmente la mayoría de los dispositivos son móviles (en el sentido de portables) no quedando fijado su uso a un espacio concreto como sucedía con los antiguos ordenadores. Así, los menores pueden hacer uso de ellos las 24 horas del día, desde cualquier lugar, fuera del alcance de los padres, debiendo encontrar otras estrategias para compartir con los menores el mismo espacio-tiempo virtual. Y es que como advierten Sasson y Mesch (2014), no es lo mismo el control que la percepción de seguridad. Los menores que tienen más restricciones en el uso también son los que realizan más actividades de riesgo, pues los menores, muchas veces tienen más habilidades en el manejo de las

TIC que los padres y encuentran como saltar los controles impuestos. Sin embargo, cuando los jóvenes sienten la cercanía se sus padres, menor es la participación en actividades de riesgo (Sasson y Mesch, 2014).

Parece necesario por tanto, una mayor comunicación entre padres e hijos para lo que es fundamental que los padres tengan conocimientos sobre las nuevas tecnologías y puedan ejercer un control indirecto sobre la actividad de sus hijos. Y no sólo los padres, también aquellos familiares que puedan ejercer supervisión. Será importante también conseguir que los menores accedan a agregarlos a sus redes sociales, pues serán ellos quienes deban de aceptarlo en última instancia.

Finalmente, queda también comprobado que trasladar bienes personales del espacio físico al ciberespacio es un factor de riesgo, y creemos que este debe tenerse especialmente en cuenta en la prevención del ciberacoso continuado dado que el mismo se realiza muchas veces por los propios usuarios sin que sea necesario. En efecto, la gran mayoría de los menores traslada de forma voluntaria sus bienes personales, elementos de su intimidad, su dignidad, su honor, etc., al ciberespacio, bien cediéndolos directamente a otras personas o bien guardándolos en los dispositivos con los que se conectan a Internet. Estudios previos habían puesto de manifiesto los riesgo derivados de suministrar información personal a otra personas a través de Internet (Marcum, 2008; Miró, 2013c; Miró, 2014c) pero en el estudio que hemos llevado a cabo se observa, además, la importancia que desempeñan, en términos de riesgo, los medios empleados para realizar tal labor de introducción y para guardar información en los

dispositivos conectados a Internet. Así, tendrán más riesgo los que más tipos de información faciliten (bien a través de una cesión directa o bien guardándolo en los dispositivos), en el sentido de que ceder o guardar fotos personales entraña un riesgo, pero aún lo es más cuando además se facilite o se guarde otros tipos de informaciones personales (como nombre, apellidos, teléfono, ubicación, correo electrónico, etc.) y, además, este ejercicio se haga a través de varias herramientas. Los resultados así demuestran que quienes más información ceden, también emplean mayor número de herramientas para hacerlo. Este riesgo, por tanto, vendrá determinado por la cantidad de objetivos que se ponen a disposición de otros para que puedan ser atacados o, también, porque así se está dando la oportunidad a un agresor potencial de hacer un análisis previo del perfil de los usuarios, seleccionando así al más vulnerable o atacando a una víctima adecuada en el punto donde le pueda hacer más daño. Y de nuevo hay que hacer referencia a que introducir bienes en el ciberespacio es una práctica habitual ente todos los usuario de Internet, sin embargo, como se ha demostrado al comparar el grupo de las "victimas" con el de las "no víctimas", el primer grupo lo hace en niveles superiores. Dicho de otro modo, las víctimas introducen más información que las no víctimas, y por lo tanto, les sitúa en una posición de mayor riesgo.

El que quede probada por tanto, la hipótesis de que a mayor introducción de datos en el ciberespacio mayor es la probabilidad de ser víctima de ciberacoso continuado debería hacernos reflexionar significativamente sobre el papel de los prestadores de servicios de la sociedad de la información en estas conductas de riesgo y en la necesidad de establecer estrategias preventivas que les impliquen especialmente a ellos. Si bien hasta el momento hemos insistido en que

comprender los factores de riesgo de la victimización derivados de las conductas cotidianas de los menores puede ser esencial para prevenir estas conductas, focalizando así las estrategias de prevención básicamente en la mejora de la educación de los menores así como de los padres y los educadores, en relación a la introducción, debería ser complementada con establecer nuevas obligaciones a los proveedores de servicios con respecto a sus relaciones con los usuario.

En efecto, se ha demostrado que son conductas de riesgo dar datos personales reales para abrir cuentas en las redes sociales (Miró, 2013c), publicar todo información personal como el nombre completo, el estado civil, fotos de sí mismo, la dirección de correo, intereses, aficiones, etc. (Reyns, 2010), y las mismas, sin embargo, responden a dinámicas comunes en el ciberespacio derivadas de que son las propias páginas web las que demandan de los usuarios que publiquen estos contenidos privados para poder crear perfiles en redes sociales o para publicar fotos y demás. En muchas ocasiones tales demandas de introducción de datos personales no es realmente obligatoria, en el sentido de que el usuario efectivamente puede no poner tales datos y seguir utilizando los servicios web. Pero ni esto está bien explicitado en la mayoría de ellas ni es así en todos los casos. Además el hecho de que tales categorías estén, ya hace que muchos menores se sientan obligados a rellenarlas incluyendo sus datos personales. Si, como se ha demostrado, poner tal información incrementa el riesgo de diferentes ciberataques de tipo social, consideramos que sería necesario establecer pautas de seguridad a las redes sociales para evitar las mismas. Son muchas las obligaciones que los Estados imponen a las páginas web y a otros servicios de Internet por ejemplo en relación con

la privacidad, pero creemos que este tipo de medidas serían aun de mayor importancia.

La seguridad en el ciberespacio ya no puede concebirse exclusivamente en términos de integridad de los sistemas y las redes, sino que va más allá. Tampoco la única preocupación puede ser la privacidad. Es importante que todos, los propios usuarios sean adultos o menores, los padres, educadores y demás implicados, pero también las instituciones públicas y los diferentes proveedores de servicios en Internet, asumamos una concepción de la seguridad informática que tenga en cuenta también los nuevos riesgos que para bienes tan relevantes como la dignidad personal, el honor, la intimidad, la libre formación de la sexualidad y la propia libertad, existen en el ciberespacio. Precisamente por ello es importante comprender cómo sucede el crimen en el ciberespacio y, desde la perspectiva que nos ocupa, qué hace la víctima en su día a día que determina su propia victimización. Pero el objetivo no es sólo que lo sepa la víctima, sino también que lo comprendamos todos para ir configurando poco a poco un ciberespacio mejor, un ámbito en el que todos sepamos cómo comportarnos y en el que, en el día a día, se puedan prevenir muchas conductas que pueden afectar gravemente a las personas.

2. Recapitulación y conclusiones

1. La proliferación de la tecnología digital ha transformado la manera de relacionarnos, pues su constante desarrollo ha traído innumerables ventajas, aunque éstas también han sido aprovechadas para llevar a cabo todo tipo de actos negativos, del mismo modo que otras revoluciones tecnológicas fueron utilizadas por los delincuentes. Esto ha supuesto que formas tradicionales de criminalidad, como el fraude y el acoso, ahora también puedan realizarse a través de Internet, pero al mismo tiempo, ha provocado la creación de nuevas conductas criminales cuya existencia se debe a la creación del ciberespacio. Por ello, cuando se utiliza el término cibercrimen, se hace referencia a todos estos crímenes que se llevan a cabo en el ciberespacio.

2. El cibercrimen ha ido evolucionando y mutando de forma paralela a como lo han hecho las TIC y sus usuarios. Tanto es así, que en la actualidad asistimos a un tercera generación de cibercrímenes que están absolutamente determinados por el uso de Internet. En este sentido, la cibercriminalidad tiene una diversidad tan amplia como facetas desarrollan los usuarios en el ciberespacio y previsiblemente seguirá aumentando conforme progresen las TIC. Tal cantidad de tipologías han llevado a algunos autores a establecer sistemas de clasificación para entender mejor su funcionamiento. Estas distintas propuestas se pueden clasificar a su vez en tres grandes categorías: las que lo hacen desde una óptica legal, las que se basan en la incidencia de las TIC en la comisión delictiva y las que atienden a la intencionalidad del agresor. El hecho de seguir esta última

sistematización, permite distinguir los distintos cibercrímenes en tres categorías: en primer lugar, los cibercrímenes económicos, que son aquéllos en los que el cibercriminal lleva a cabo el ataque con intención de obtener un beneficio económico; en segundo lugar, los cibercrímenes políticos, aquéllos en los que al cibercriminal es motivado por cuestiones políticas o ideológicas; y por último, los cibercrímenes sociales, que son aquéllos que tienen intención de dañar a una persona.

3. Precisamente, dentro de los cibercrímenes sociales, el ciberacoso a menores es el ataque que en mayor medida preocupa a la sociedad, aunque también es cierto que los menores pueden sufrir otro tipo de ataques como los económicos. Sin embargo, en la medida en que los menores hacen mayor uso de Internet para desarrollar su vida personal y social, todas las facetas relacionadas con este ámbito pueden ser dañadas. En este sentido, son muchas las conductas que pueden sufrir los menores: humillación, amenazas, exclusión, suplantación de identidad, etc., y precisamente, el hecho de enfocar los estudios en esta forma de victimización, parte de las graves consecuencias que padecen los menores que la sufren.

4. Para entender el fenómeno criminal debemos necesariamente entender el lugar en que éste se lleva a cabo, y en este sentido, la configuración del ciberespacio no solamente ha permitido que se lleven a cabo estas formas tradicionales de acoso, sino que además se hagan con mayor facilidad. La idea básica parte de que estamos ante un fenómeno eminentemente verbal, es decir, alejado de la tradicional violencia física, y que ha encontrado un medio idóneo en el ciberespacio en la media en que éste fue concebido para la

comunicación entre las personas sin necesidad de proximidad física. Esta primera diferencia con el espacio físico (que no sea necesaria la proximidad) ha permitido que el contacto entre los menores se expanda, en cuanto al número de personas que pueden interactuar y el número de comunicaciones, y todo ello sin limitación de tiempo. En otras palabras, la agresión entre menores ya no está limitada a los compañeros de clase y del colegio, ni a las horas de clase, pudiéndose realizar desde cualquier espacio físico y en cualquier momento del día.

5. El ciberespacio permite compartir a tiempo real con los amigos (aunque no es tan fácil limitar este alcance) situaciones, sentimientos, instantáneas, etc., con facilidad y bajos costes. Estas cualidades, sumadas a las mencionadas en el párrafo anterior, hacen que los menores se expongan a numerosos riesgos, como han demostrado los estudios al señalar la existencia de casos de *cyberbullying, cyberharassment* y otras formas de acoso no sexual a través de Internet.

6. Dentro de las diferentes formas de cibercriminalidad social destaca el ciberacoso u hostigamiento al menor realizado a través las TIC. La manifestación más destacada por los estudios de este tipo de cibercriminalidad es el *cyberbullying*, entendido como el ciberacoso continuado entre menores centrado en el ámbito escolar. Sin embargo, en el presente estudio se ha optado por centrar el objeto de análisis en cuatro conductas concretas de ciberacoso continuado: recibir insultos de manera continuada, ser objeto de difamación de rumores o mentiras de forma continuada, haber sido contactado de manera repetida por otra persona tras haberle pedido previamente que no lo hiciera y haber sido marginado de manera repetida. La elección de

estas conductas de ciberacoso continuado responde a dos motivos: el primero de ellos, por tratarse de las conductas que con mayor frecuencia sufren los menores en Internet, siempre que se tenga en cuenta la característica de la continuidad; el segundo de ellos, por no limitar la procedencia del acoso al ámbito escolar, pues los menores ya no sólo se relacionan en el ciberespacio con los compañeros del colegio, ahora también lo hacen con amigos de otros ámbitos, e incluso con "amigos de Internet". Por lo tanto, al abrir el ámbito de las relaciones de los menores, las conductas de ciberacoso continuado podrán tener un origen distinto al escolar y no por ello ser menos dañinas para los menores.

7. La constatación de la existencia de este fenómeno de la cibercriminalidad social, ha llevado a la comunidad científica a identificar los factores de riesgo asociados a la victimización. Muchos autores se han centrado en analizar la relevancia de las variables demográficas, psicológicas y sociales, conforme a lo que tradicionalmente se ha venido haciendo con la modalidad *offline* de estas agresiones. Sin embargo, ha surgido en los últimos años una corriente de autores que han centrado la búsqueda de factores a partir de los hábitos de los menores en Internet, es decir, analizando cuántas horas al día se conectan las víctimas, de entre todas las herramientas de comunicación cuáles usan más, para qué las usan, qué es lo que hacen con ellas, etc. En resumen, cuáles son las actividades cotidianas de los menores víctimas en Internet y cómo inciden éstas en la victimización.

8. Partiendo de las formulaciones que realizaron Cohen y Felson, hace algo más de una década comenzaron a surgir estudios en

los que se analizaba de qué forma el cambio tecnológico y social había cambiado la cotidianeidad de las personas y modificado las oportunidades delictivas. Peter Grabosky (2001) fue uno de los primero autores en afirmar que en el ciberespacio habían incrementado las oportunidades de que confluyesen los tres elementos (delincuente motivado, objetivo adecuado y ausencia de un guardián capaz), y tras su trabajo comenzaron a publicarse otros como el de Yar (2005) o Miró (2011) que han tratado de analizar la aplicabilidad de la TAC. Ambos autores, aunque con argumentos distintos, llegan a la misma conclusión: para que se produzca un cibercrimen, sigue siendo necesario que converjan un agresor potencial y un objetivo adecuado en ausencia de un guardián capaz. Sin embargo, dada la configuración del nuevo lugar, la manera de relacionarse entre ellos cambia, y al hacerlo, también cambian las características que convierten a un objetivo en adecuado.

9. También son muchos los estudios que han tratado de aplicar la TAC, tanto para el análisis de la cibercriminalidad económica como para la social. La mayoría de ellos ha tratado de encontrar, a partir de encuestas de victimización, variables derivadas de todos los elementos de la TAC, como la exposición al delincuente motivado, proximidad al delincuente motivado, el objetivo adecuado o el guardián capaz. Sin embargo, en prácticamente la mayoría de los casos, lo que se está haciendo es identificar únicamente características del elemento "objetivo adecuado" en tanto que se está preguntando por aquello que hace el sujeto en el ciberespacio y especialmente, acerca de sus acciones de comunicación. En este sentido, cuando los autores hablan de "exposición o proximidad al delincuente motivado" están haciendo referencia a las principales actividades de comunicación que realizan

en el ciberespacio como el número de horas pasadas en Internet, el uso de herramientas de comunicación (correo electrónico, chat, etc.), número de "amigos" agregados a las redes sociales, etc.; y señalan como "guardián capaz", no a la vigilancia que puedan ejercer terceros, sino lo que hace la propia víctima para autoprotegerse, generalmente usando *software* de seguridad.

10. Al utilizar encuestas de victimización y tratar de relacionar el haber sido víctima de un cibercrimen con el actuar cotidiano de la víctima al cuestionarle sobre su día a día en el ciberespacio, resulta lógico tratar de centrarse en el constructo objetivo adecuado. Esto no significa que no se pueda obtener información sobre otros constructos como el guardián capaz, pero siempre que se le pregunte a la víctima sobre lo que ella hace y, en relación con eso, se obtengan datos sobre, por ejemplo, la vigilancia que otros tienen la posibilidad de ejercer sobre ella.

11. Felson (1998) explicó, a partir del acrónimo VIVA, que las características que hacen a un objetivo adecuado son el valor, la inercia, la visibilidad y la accesibilidad. En la adaptación de las mismas al ciberespacio, Yar (2005) señaló que sólo el elemento valor es el único que puede ser trasladado al ciberespacio. Esto es así, dado que el valor depende, al igual que en el espacio físico, del cálculo realizado por el agresor sobre el fin pretendido con la comisión del delito, mientras que el resto de elementos, al depender en mayor medida del espacio en el que tienen lugar y ser distinto el ciberespacio al espacio físico, no pueden ser adoptados para el cibercrimen. Por su parte Miró (2011) modifica el significado de algunos caracteres y crea el acrónimo IVI, manteniendo así el valor del objetivo como elemento de adecuación,

pero incluyendo como nuevos la introducción de los bienes al ciberespacio y la interacción como la forma de hacerlos visibles.

12. A nuestro parecer, el valor del objetivo no puede ser medido en un estudio de estas características (que se centra en preguntarle a las víctimas por su actividad cotidiana al ciberespacio) porque depende de la intención del agresor. En cuanto a la inercia, tampoco se considera como elemento de adecuación porque en el ciberespacio los bienes a penas se diferencian entre sí por las propiedades físicas. En cambio, las características de accesibilidad y visibilidad sí pueden ser utilizadas, aunque cambian su significado. Así, la accesibilidad es la cualidad del objetivo que indica que no está suficientemente protegido por la propia víctima; mientras que la visibilidad en Internet, como ha señalado Miró (2012), depende de la interacción del usuario con otros, pues en la inmensidad del ciberespacio donde todos los bienes son públicos y por tanto visibles, destacará sobre el resto, es decir, se hará más visible, aquél que se mueva más mediante la interacción comunicativa. A estas dos características de accesibilidad y visibilidad, hay que sumarle la introducción, definida por Miró (2011) como los bienes que una persona traslada de forma voluntaria o involuntaria del mundo físico al ciberespacio.

13. Conforme a esto, un objetivo es más o menos adecuado dependiendo de que sea introducido en el ciberespacio, interaccione haciéndose así visible y esté accesible en la medida en que no adopte sistemas de autoprotección. Sin embargo, para la cibercriminalidad social, la autoprotección apenas funciona, porque el objetivo es la propia persona y está accesible en el momento en que accede en el ciberespacio. Y es que lo que Miró (2011) entiende por autoprotección

se relaciona más con la forma de protección económica. Esto es así porque hace referencia a los distintos *software* de seguridad, que en realidad están diseñados para proteger los sistemas informáticos que suelen ser, salvo contadas excepciones, el objetivo de los ataques económicos. Por todo ello, consideramos que esa variable, a los efectos de este trabajo, debe ser descartada como constitutiva del elemento "objetivo adecuado".

14. Junto al objetivo adecuado también es posible, por medio de encuestas de victimización, medir la vigilancia familiar en la medida en que se pregunte al sujeto sobre la supervisión que pueda estar ejerciendo un tercero sobre él. Es decir, a diferencia de lo que hacen otros estudios en los que se confunde al objetivo adecuado con las acciones que lleva a cabo la propia víctima para protegerse, se trata de preguntar a la persona sobre su actuar cotidiano en relación con otros familiares, como por ejemplo, preguntándole si comparte los sistemas informáticos con sus hermanos o si agrega a los familiares a sus perfiles de redes sociales.

15. A partir de estas premisas, se ha elaborado el presente trabajo con el objetivo de aportar mayor conocimiento acerca de la violencia que sufren los menores a través de Internet y cuáles son sus hábitos en el uso de las TIC que les coloca en una situación de riesgo.

16. Se ha podido constatar que el 38% de los participantes en el estudio han sufrido durante un periodo de su vida, algún acto de acoso continuado de carácter no sexual a través de las TIC. El tipo de ciberataque social que con mayor frecuencia sufren son los insultos (23%), seguido muy de cerca por la difusión de rumores o mentiras (21,5%). También han sufrido en menor medida, aunque son

porcentajes que no se pueden despreciar, el contacto repetido no deseado cuando previamente se ha solicitado que deje de realizar el contacto (14,4%) y marginar (4,8%).

17. Aunque los valores de prevalencia son algo superiores, son coherentes con el hecho, por un lado, de que los datos son más recientes que los estudios con los que se compara, por lo que pueden estar reflejando cómo la expansión del uso de las TIC incide en el incremento de la cibercriminalidad; y por otro lado, de que los resultados de victimización no se limitan a los ataques ejercidos por los compañeros del colegio, como así hacen en la mayoría de los estudios.

18. Respecto a las características demográficas de los menores víctimas de ciberacoso continuado, el estudio pone de manifiesto, como así han hecho estudios previos, que el ciberacoso, especialmente las cuatro formas de ataque medidas (insultos, rumores, contacto repetido y marginar), suelen ser sufridas en mayor medidas por las chicas que por los chicos. Se trata de formas de violencia indirecta, de tipo verbal y emocional, que tradicionalmente los estudios de criminología han identificado con las mujeres. Sin embargo, las mayores diferencias encontradas entre sexos se han dado en las conductas de contactar de manera repetida y marginar. En las otras dos conductas, las diferencias son mucho menores, incluso no siendo estadísticamente significativas en la difusión de rumores.

19. En cuanto a la edad de las víctimas, los datos todavía son más contundentes. Es cierto que los porcentajes aumentan conforme aumenta la edad, sin embargo, las pruebas estadísticas confirman que no hay diferencias significativas entre los grupos de edad. Esto viene a reforzar los planteamientos de que la edad y el sexo no son elementos

que determinen la probabilidad de ser víctima en el ciberespacio, sino que lo será la actividad que se desarrolle en él.

20. Los hábitos de los menores vienen determinados por la cantidad de aplicaciones que se han desarrollado hasta el momento para la comunicación (el correo electrónico, la mensajería instantánea, las salas de chat, las redes sociales, etc.) y por los múltiples usos que se le pueden otorgar. Sin embargo, todas las actividades que se desarrollan pueden agruparse principalmente en dos tipos: las relativas a la introducción de objetivos al ciberespacio y las que se identifican con la interacción del usuario.

21. La manera de introducir bienes en el ciberespacio puede ser, bien mediante la cesión voluntaria de información personal, o bien almacenándola en los dispositivos con los que se conecta a Internet. En ambos casos, la víctima con su actuar, consciente o inconscientemente, está dando la posibilidad de que otros puedan atacar sus bienes.

22. Una vez introducidos los objetivos en el ciberespacio, se hacen visibles a partir de la interacción, esto es, al comunicarse con otras personas; y lo hacen de múltiples maneras: usando el correo electrónico, la mensajería instantánea, las redes sociales, los foros, los blogs, las salas de chat, etc., para generalmente, mantener el contacto con personas conocidas en el espacio físico, pero también para ligar, cotillear, conocer personas nuevas e incluso para agredir a otras.

23. Las acciones realizadas de introducción e interacción por parte de los menores, les convierte en objetivos adecuados. Sin embargo, aunque converjan en un mismo espacio-tiempo con el delincuente potencial, el ataque sobre ellos podrá ser evitado con la

simple presencia de un guardián capaz. En el caso de la cibercriminalidad social realizada sobre menores, esta figura puede ser representada por los padres y otros familiares, compartiendo con ellos actividades cotidianas en el ciberespacio, así como usando los mismos dispositivos para navegar por la Red o frecuentando los mismos espacios virtuales como por ejemplo, las redes sociales.

24. Prácticamente todos los menores realizan actividades de interacción e introducción en el ciberespacio, pero el volumen de las actividades aumenta conforme avanza la edad de los sujetos. Sin embargo, este aumento es gradual conforme muestran los resultados al comparar la cantidad de actividades entre los diferentes grupos. Así, sólo se encuentra un salto significativo cuando se compara a los más pequeños (los que tienen entre 12 y 13 años) con los más mayores (los que tienen entre 16 y 18 años).

25. Tanto las chicas como los chicos realizan todas las conductas medidas en el estudio, sin embargo, las chicas facilitan más información personal real y usan las TIC para mantener el contacto con personas conocidas y para cotillear, mientras que los chicos emplean más herramientas de comunicación y usan las TIC para ligar, contactar con desconocidos y llevar a cabo conductas violentas. El resto de conductas incluidas en el estudio como actividades cotidianas, las hacen en la misma medida tanto los chicos como las chicas.

26. Independientemente de la edad y el sexo de los sujetos, todos los sujetos que han sido objeto de insultos, rumores, contacto repetido o marginación por otros a través de las TIC, realizan más actividades de riesgo y están menos protegidos que los que no han sido victimizados.

27. Todas las actividades cotidianas incluidas en el estudio, tanto las de introducción e interacción, como las de la vigilancia experimentada, tienen efecto sobre la victimización. Será la combinación de factores concretos la que determine en cada caso la probabilidad de victimización y la que indique que, como se muestra en la Red Neuronal Artificial, las conexiones pueden ser múltiples. Sin embargo, en general se ha podido comprobar cómo el aumento de la visibilidad de los menores en el ciberespacio, concretamente haciendo uso de las herramientas de comunicación para agredir a otras personas y para conocer a personas nuevas, está especialmente relacionado con la victimización; aunque también tienen un efecto destacable las otras conductas de interacción, así como las de introducir bienes en el ciberespacio y experimentar una menor vigilancia por parte de los padres u otros familiares.

28. Se confirma por tanto, que el menor juega un papel muy importante en su adecuación como víctima en el ciberespacio al introducir sus bienes y al hacerse visible para otros usuarios, a partir de sus actividades del día a día en la Red. Sin embargo, también será decisivo en la victimización del menor, el rol que puedan ejercer los padres y otros familiares como guardianes capaces en el ciberespacio. En este sentido, gran parte del esfuerzo de las políticas de prevención deberían ir encaminadas a modificar la adecuación de los menores como objetivos en el ciberespacio, como también a involucrar a los padres y otros familiares como potenciales guardianes de los menores. Todo ello, sin despreciar otro tipo de medidas enfocadas, por ejemplo, en los prestadores de servicios, en los creadores de las herramientas de comunicación, etc., que fomenten el uso seguro de las TIC por parte de los menores.

3. Limitaciones y prospectiva

Para finalizar este capítulo y con ello el trabajo, se hace mención en lo que sigue a lo que se consideran las principales limitaciones detectadas en el estudio y se exponen algunas propuestas que pueden mejorar el conocimiento científico relativo al acoso ejercido sobre menores a través de las TIC.

En primer lugar, aunque los resultados obtenidos en el estudio sirven para hacer una aproximación real de las dinámicas de los distintos ciberacosos a menores en general, en la medida en que la muestra está centralizada en una la provincia de Alicante, sería interesante ampliarla a otras regiones de España. Asimismo, convendría ampliar el rango de edad de la muestra incluyendo a menores de 12 años, pues en la medida que hacen uso de las TIC, pueden estar expuestos a situaciones de riesgo que se deben conocer y controlar.

En segundo lugar, el empleo de una herramienta creada *ad hoc*, a pesar de haber sido rigurosos con las exigencias psicométricas, no permite hacer comparaciones del todo fiables con otros estudios. En este sentido, a lo largo del trabajo se ha puesto de manifiesto en múltiples ocasiones la necesidad de crear una metodología común de investigación en cibervictimización, que permita la obtención de resultados con una mayor precisión y, a su vez, la comparación de éstos a nivel tanto nacional como internacional. Entre las cuestiones que se deben tener en especial consideración a la hora de elaborar los instrumentos, se ha detectado la necesidad de establecer pautas de control sobre la temporalización de las variables para garantizar un

mayor conocimiento del orden temporal de las relaciones entre ellas. Y a todo ello habría que sumar la evaluación de otros ataques sociales que sufren los menores en el ciberespacio, pero también en el ámbito de la ciberdelincuencia económica.

En tercer lugar, pese a que el modelo creado mejora significativamente los construidos hasta el momento, obteniendo resultados más que aceptados por las ciencias sociales, aportando información de cómo las actividades cotidianas en el ciberespacio influyen en el proceso de cibervictimización, lo cierto es que se ha alcanzado una tasa de acierto del 70% en las predicciones, lo que indica que se puede errar en tres de cada diez casos. Para mejorar la capacidad de pronóstico del modelo, podría ser interesante incluir otras variables que reflejaran más actividades cotidianas de los menores en el ciberespacio, así como otras destinadas, de acuerdo a la TAC, a completar la figura del guardián capaz y a avanzar en el análisis del agresor potencial. Ante la necesidad de obtener mejor información sobre estos dos elementos (delincuente potencial y guardián capaz), se propone emplear o desarrollar otros métodos de análisis que salven este inconveniente. En este sentido, podría ser interesante realizar investigaciones de corte cuasiexperimental donde se pudiesen controlar, en la medida de lo posible, todas las variables relativas a la TAC, así como también realizar investigaciones longitudinales que permitan tener una imagen más real del proceso de cibervictimización y cómo evoluciona, sobre todo si tenemos en cuenta que las TIC están en permanente cambio.

Bibliografía

Aebi, M. F., & Linde, A. (2010). Las encuestas de victimización en Europa: Evolución histórica y situación actual. *Revista de Derecho Penal Y Criminología*, *3*(3), 211–298.

Aebi, M. F., & Linde, A. (2012). Conviction Statistics as an Indicator of Crime Trends in Europe from 1990 to 2006. *European Journal on Criminal Policy and Research*, *18*(1), 103–144.

Aguirre Romero, J. M. (2004). Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. *Espéculo: Revista de Estudios Literaris*, *27*, 1–33.

Agustina, J. R. (2009). La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual. *International E-Journal of Criminal Sciences*, *4*(3), 1–31.

Agustina, J. R. (2010). ¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el Sexting. *Revista Electrónica de Ciencia Penal Y Criminología, 12*(11), 1–44.

Agustina, J. R. (2012). *La Pornografía. Sus efectos sociales y criminógenos. Una aproximación multidisciplinar*. Madrid: Edisofer, S.L.

Akers, R. L. (1997). *Criminological theories*. Los Ángeles: Roxbury.

Alcantara, J. (2011). *La neutralidad en La Red, y porqué es una mala idea acabar con ella*. Bilbao-Madrid-Montevideo: Biblioteca de Las Indias.

Appel, M., Stiglbauer, B., Batinic, B., & Holtz, P. (2014). Internet use and verbal aggression: The moderating role of parents and peers. *Computers in Human Behavior*, *33*, 235–241.

Aslanidou, S., & Menexes, G. (2008). Youth and the Internet: Uses and practices in the home. *Computers & Education*, *51*(3), 1375–1391.

Avilés, J. M. (2009). Cyberbullying: Diferencias entre el alumnado de secundaria. *Boletín de Psicología*, *96*, 79–96.

Avilés, J. M., Irurtia, M. J., García-Lopez, L. J., & Caballo, V. (2011). El maltrato entre iguales:"bullying." *Behavioral Psychology*, *19*(1), 57–90.

Baker, Ö. E., & Tanrıkulu, İ. (2010). Psychological consequences of cyber bullying experiences among Turkish secondary school children. *Procedia - Social and Behavioral Sciences*, *2*(2), 2771–2776.

Bandura, A. (1973). A. Social learning theory of aggression. En *The control of aggression: Implications from basic research*. Chicago: Aldine.

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

Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence*, *36*(2), 341–50.

Becker, H. S. (1963). *Outsiders. Studies in the Sociology of deviance*. New York y London: The Free Press y Collier-Macmillan.

Beckman, L., Hagquist, C., & Hellström, L. (2013). Discrepant gender patterns for cyberbullying and traditional bullying – An analysis of Swedish adolescent data. *Computers in Human Behavior*, *29*(5), 1896–1903.

Beirne, P. (1993). The Social Cartography of Crime : A . M . Guerry's Statistique Morale (1833). In *Inventing Criminology: Essays on the Rise of Homo Criminalis* (pp. 111–141). Albany: State University of Albany Press.

Belsey, B. (2005). Cyberbullying: An Emerging Threat to the "Always On" Generation. Canadá: Bullying.org.

Beran, T., & Li, Q. (2008). The relationship between cyberbullying and school bullying. *The Journal of Student Wellbeing*, *1*(2), 16–33.

Berne, S., Frisén, A., Schultze-Krumbholz, A., Scheithauer, H., Naruskov, K., Luik, P., Katzer, C., Erentaiter, R., & Zukauskiene, R. (2013). Cyberbullying assessment instruments: A systematic review. *Aggression and Violent Behavior*, *18*(2), 320–334.

Bertillon, A. (1909). *Anthropolige métrique*. Paris: Imprimerie national.

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

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

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

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227–236.

Brantingham, P. L., & Brantingham, P. J. (1981). *Environmental Criminology*. Beverly Hills, CA: Sage Publications.

Brantingham, P. L., & Brantringham, P. J. (1984). *Patterns in Crime*. New York, NY: Macmillan.

Bregant, J., & Bregant, R. (2014). Cybercrime and Computer Crime. (J. S. Albanese, Ed.) *The Encyclopedia of Criminology and Criminal Justice*. Oxford: Blackwell Publishing Ltd.

Brighi, A., Guarini, A., & Melotti, G. (2012). Predictors of victimisation across direct bullying, indirect bullying and cyberbullying. *Emotional and Behavioural Difficulties*, *17*(3-4), 375–388.

Brighi, A., Guarini, A., Melotti, G., & Genta, M. L. (2012). Emotional and Behavioural Difficulties Predictors of victimisation across direct bullying , indirect bullying and cyberbullying. *Emotional and Behavioural Difficulties*, *17*(3-4), 375–388.

Bringué, X., & Sádaba, C. C. (2011). Menores y redes sociales. Madrid: Foro Generaciones Interactivas.

Buelga, S., Cava, M. J., & Musitu, G. (2010). Cyberbullying: victimización entre adolescentes a través del teléfono móvil y de Internet. *Psicothema*, *22*(2006), 784–789.

Burke, S. C., Wallen, M., Vail-Smith, K., & Knox, D. (2011). Using technology to control intimate partners: An exploratory study of college undergraduates. *Computers in Human Behavior*, *27*(3), 1162–1167.

Cabero, J. (1996). El ciberespacio: el no lugar como lugar educativo. Extraído el 23 febrero de 2013 http://tecnologiaedu.us.es/cursos/29/html/bibliovir/pdf/104.pdf

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

Calvete, E., Orue, I., & Estévez, A. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior*, *26*(5), 1128–1135.

Campfield, D. C. (2008). *Cyber bullying and victimization: Psychosocial characteristics of bullies, victims, and bully/victims*. Tesis Doctoral. The University of Montana Missoula.

Çankaya, İ. H., & Tan, Ç. (2011). Effect of cyber bullying on the distrust levels of preservice teachers: considering internet addiction as a mediating Variable. *Procedia Computer Science*, *3*, 1353–1360.

Canter, D. (1983). The purposive Evaluation of places: a facet approach. *Environment and Behavior*, *15*(6), 659–698.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies*, *10*, 229–242.

Cappadocia, M. (2013). Cyberbullying Prevalence, Stability, and Risk Factors During Adolescence. *Canadian Journal of School Psychology*, *28*(2), 171–192.

Casabona, R., & Martín, J. A. (1988). *Poder informático y seguridad jurídica: la función tutelar del derecho penal ante las nuevas tecnologías de la información.* Madrid: Fundesco.

Casas, J. a., Del Rey, R., & Ortega-Ruiz, R. (2013). Bullying and cyberbullying: Convergent and divergent predictor variables. *Computers in Human Behavior*, *29*(3), 580–587.

Cavezza, C., & McEwan, T. E. (2014). Cyberstalking versus off-line stalking in a forensic simple. *Psychology, Crime & Law*, 1–16.

Chambliss, W. J. (1975). Towards a political economy of crime. *Theory and Society*, *2*, 149–170.

Chico, E. (1997). La invarianza en la estructura factorial del raven en grupos de delincuentes y no delincuentes. *Psicothema*, *9*(1), 47–55.

Chiu, D., Chung, T. T., & Wang, C. S. (2009). Attacking and Defending Perspective of E-Crime Behavior and Psychology: A Systemic Dynamic Simulation Approach. En *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on* (pp. 1035–1039). IEEE.

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

Choo, K. (2009). Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences. En *Research and Public Policy Series*. Australian Institute of Criminology.

Choo, K.-K. R. (2009). Responding to online child sexual grooming: an industry perspective. *Trends and Issues in Crime and Criminal Justice*, (379), 1–6.

Clarke, R. V. (1999). *Hot Products: Understanding, anticipating and reducing demand for stolen goods*. London: Home Office, Research Devolopment and Statics Directorate.

Clarke, R. V. (2004). Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research*, *10*(1), 55–63.

Clarke, R. V., & Felson, M. (1993). Introduction: Criminology, Routine Activity and Rational Choice. En R. V. Clarke & M. Felson (Eds.), *Advances in Criminological Theory* (pp. 1–13). New Jersey: Transaction Publishers.

Clarke, R. V., & Felson, M. (2009). The Origins of Situational Crime Prevention and the Routine Activity Approach. En F. T. Cullen, C. L. Jonson, A. J. Myer, & F. Adler (Eds.), *The Origins of American Criminology* (pp. 245–260). New Brunswick: Transaction Publishers.

Cleckley, H. (1941). *The Mask of Sanity: An Attempt to Clarify Some Issues About the So-Called Psychopathic Personality*. The C. V. Mosby Company.

Clodfelter, T. a., Turner, M. G., Hartman, J. L., & Kuhns, J. B. (2008). Sexual Harassment Victimization During Emerging Adulthood: A Test of Routine Activities Theory and a General Theory of Crime. *Crime & Delinquency*, *56*(3), 455–481.

Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, *37*(4), 671–680.

Cloward, R. A., & Ohlin, L. E. (1960). *Delinquency and oportunity, a Theory of delinquent gans*. New York: Free Press

Cohen, A. K. (1955). *Delinquent Boys: The culture of the gangs*. Glencoe: Free Press.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*, 588–608.

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

Colquhoun, L. D. (1800). *Treatise on the Commerce and Police of the River Thames*. (J. Mawman, Ed.). London: Joseph Mawman.

Corcoran, L., Connolly, I., & O´Moore, M. (2012). Cyberbullying in Irish schools: an investigation of personality and self-concept. *The Irish Journal of Psychology*, *33*(4), 153–165.

Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York, NY: Springer-Verlag.

Cornish, D., & Clarke, R. (1987). Understanding Crime Displacement: An Aplication of Rational Choice Theory. *Criminology*, *25*(4), 933–948.

Craven, S., Brown, S., & Gilchirst, E. (2006). Sexual grooming of children: review of literature and theoretical considerations. *Journal of Sexual Agression*, *12*(3), 287–299.

Dahrendorf, R. (1959). *Class and class conflict in industrial society*. Standford, California: Stanford University Press.

Damasio, A. (1994). *Descartes' Error: Emotion, Reason and the Human Brain*. New York, NY: Putnam.

Davidson, J., Grove-Hills, J., Bifulco, A., Gottschalck, P., Caretti, V., Pham, T., & Webster, S. (2011). Online Abuse: Literature Review and Policy Context. European Commission Safer Internet Plus Programme.

De la Cuesta, J. L. (2010). *Derecho penal informático*. Cizur Menor: Civitas.

Defensor del Pueblo. (2007). *Violencia escolar: el maltrato entre iguales en la Educación Secundaria Obligatoria 1999-2006*. Madrid: Publicaciones de la Oficina del Defensor del Pueblo.

Dehue, F., Bolman, C., & Vollink, T. (2008). Cyberbullying: Youngters' experiences and parental perception. *CyberPsychology & Behavior*, *11*(2), 217–223.

Del Rey, R., Elipe, P., & Ortega-Ruiz, R. (2012). Bullying and cyberbullying: Overlapping and predictive value of the co-occurrence. *Psicothema*, *24*(4), 608–613.

Di Tullio, B. (1980a). *La criminologie : bilan et perspectives.* Paris: A. Pedone.

Di Tullio, B. (1980b). *Naissance de la société internationale de criminologie*. Paris: A. Pédone.

Didden, R. M., Scholte, R. H., Korzilius, H., de Moor, J. M., Vermeulen, A., O´Reilly, M., Lang, R., & Lancioni, G. E. (2009). Cyberbullying among students with intellectual and developmental disability in special education stteing. *Developmental Neurorehabilitation*, *12*(3), 146–151.

Duncan, S. H. (2007). MySpace is also their space: Ideas for keeping children safe from sexual predators on social-networking sites. *Kentucky Law Journal*, *96*(4), 527–577.

Durkheim, E. (1894). *Les règles de la Méthode Sociologique*. Paris: Les Presses universitaires de France.

Eck, J. E. (1994). *Drug Markets and Drug Places: A Case-Control Study of the Spatial Structure of Illicit Drug Dealing*. Tesis Doctoral. University of Maryland.

Ekblom, P. (1995). Less crime, by design. *The Annals of the American Academy of Political and Social Science*, *539*(1), 114–129.

Eneman, M., Gillespie, A. A., & Bernd, C. S. (2010). Technology and sexual abuse: a critical review ofan internet grooming case. In *International Conference on Information Systems (ICIS)*.

Estévez, E., Villadrón, L., Calvete, E., Padilla, P., & Orue, I. (2010). Adolescentes víctimas de cyberbullying: prevalencia y características. *Psicología Conductual*, *18*(1), 73–89.

Exner, F. (1957). *Biología Criminal en sus rasgos fundamentales*. Barcelona: Bosch.

Eysenck, H. (1987). Personality theory and the problem of criminality. En *Appying Psychology to imprisonment: Theory and Practice* (pp. 29–58). London: HSMO.

Eysenck, H. J. (1977). *Crime and personality*. London: Routledge & K. Paul.

Eysenck, H. J. (1989). *The Causes and Cures of Criminality*. New York, NY: Plenun Press.

Farrington, D. P. (1993). Understanding and Preventing Bullying. *Crime and Justice*, *17*, 381–458.

Félix-Mateo, V., & Soriano-Ferrer, M. (2010). El ciberacoso en la enseñanza obligatoria. *Aula Abierta*, *38*(1), 47–58.

Felson, M. (1986). Linking criminal choices, routine activities, informal control, and criminal outcomes. En D. Cornish & R. V. Clarke (Eds.), *The reasoning criminal* (pp. 119–128). New York: Springer-Verlag.

Felson, M. (1995). Those who discourage crime. En J. E. Eck & D. Weisburd (Eds.), *Crime prevention studies: Vol 4. Crime and Place* (pp. 53–66). New York: Criminal Justice Press.

Felson, M. (1998). *Crime and Everyday Life* (2ª ed.). Thousand Oaks, California: Pine Forge Press.

Felson, M. (2006). *Crime and Nature*. Thousand Oaks: Sage Publications.

Felson, M. (2008). Routine activity approach. In R. Worley & L. Mazerolle (Eds.), *Environmental Criminology and Crime Analysis* (pp. 70–77). Collumpton, UK: William Publishing.

Felson, M., & Boba, R. (2010). *Crime and Everyday Life* (4ª ed.). Thousand Oaks, California: SAGE Publications.

Felson, M., & Clarke, R. V. (1998). *Opportunity Makes the Thief. Practical theory for crime prevention. Police Research Series, Paper 98*. London: Home Office, Policing and Reducing Crime Unit.

Felson, M., & Cohen, L. (1980). Human Ecology and Crime: A Routine Activity Approach. *Human Ecology*, *8*(4), 389–406.

Felson, M., & Poulsen, E. (2003). Simple indicators of crime by time of day. *International Journal of Forecasting*, *19*, 595–601.

Fenaughty, J., & Harré, N. (2013). Factors associated with young people's successful resolution of distressing electronic harassment. *Computers & Education*, *61*, 242–250.

Ferri, E. (1900). *Sociología Criminal*. Torino: Fratelli Bocca.

Finkelhor, D., Mitchell, K., & Wolak, J. (2000). Online victimization: A report on the nation's youth. Alexandria, VA: National Center for Missing and Exploited Children.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence*, *19*(4), 468–483.

Fishbein, D. H. (1992). Neuroendocrine responses to a glucose challenge in substance users with high and low levels of aggression, impulsivity and antisocial personality. *Neuropsychobiology*, *25*, 106–114.

Flores, J. (2009). *Menores y ciberdelitos, una realidad inevitable.* Extraído 3 de abril de 2013 http://controlparental. wordpress. com/2008/12/03/menores-y-ciberdelitos-unarealidad-evitable

Fonseca, V. (2003). Ciberespacio: reinventando la metáfora de lo humano. *Revista de La Escuela de Bibliotecología, Documentación E Información*, *21*(1-2), 5–17.

Fredtroms, B. K., Adms, R. E., & Gilman, R. (2011). Electronic and school-based victimization: Unique contexts for adjustment difficulties during adolescence. *Journal of Youth and Adolescence*, *40*(4), 405–415.

Furnell, S. (2003). Cybercrime: vandalizing the information society. *LNCS*, *2722*, 8–16.

Garaigordobil, M. (2011). Prevalencia y consecuencias del cyberbullying: una revisión. *International Journal of Psychology and Psychological Therapy*, *11*(2), 233–254.

Garcia, A., López-de-Ayala, M. C., & Catalina, B. (2013). Hábitos de uso de Internet y en las redes sociales de los adolescentes españoles. *Comunicar*, *41*(XXI), 195–204.

García, D. Á., & Pérez, J. N. (2011). Violencia a través de las tecnologías de la información y la comunicación en estudiantes de secundaria. *Anales de Psicología*, *27*(1), 221–230.

García-Pablos de Molina, A. (1999). *Tratado de criminologia*. Valencia: Tirant lo Blanch.

Gardner, H. (1995). *Siete Inteligencias. La teoría en la práctica*. Barcelona: Ediciones Páidos Ibérica S.A.

Garofalo, R. (1885). *Criminología: estudio sobre el delito, sobre sus causas y la teoría de la represión*. Turín.

Garrido, V., & Redondo, S. (2013). *Principios de Criminología* (4ª ed.). Valencia: Tirant lo Blanch.

Garrido, V., Redondo, S., & Stangeland, P. (2001). *Principios de Criminología* (1ª ed.). Valencia: Tirant lo Blanch.

Garrido, V., Stangeland, P., & Redondo, S. (2006). *Principios de Criminología* (3ª ed.). Valencia: Tirant lo Blanch.

Geer, D. E. (2007). The Physics of Digital Law: Searching for Counterintuitive Analogies. En J. M. Balking, J. Grimmelman, E. Katz, N. Kozlovski, S. Wagman, & T. Zarky (Eds.), *Cybercrime: Digital Cops in a Networked Enviroment.* (pp. 13–37). New York, NY: New York University Press.

Gibbs, C., Cassidy, M. B., & Rivers, L. (2013). A Routine Activities Analysis of White-Collar Crime in Carbon Markets. *Law & Policy*, *35*(4), 341–374.

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Giddens, A. (1993). *New rules of sociological method: a positive critique of interpretative sociologies*. Stanford, California: Stanford University Press.

Gillespie, A. (2004). Grooming definitions and the law. *The New Law Journal*, *154*, 586–587.

Glaser, D. (1978). The counterproductivity of conservative thinking about crime. *Criminology*, *16*(2), 209–224.

Gómez, A. (2005). Fronteras electronicas y nuevas dinamicas transnacionales en Internet. *Comunicación*, *3*, 39–49.

González, J. J. (1999). Protección penal de sistemas, elementos, datos, documentos y programas informáticos. *Revista Electrónica de Ciencia Penal Y Criminología*, 1–14.

Goring, C. B. (1913). *The english convict: A statistical Study*. Londres: HSMO.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Standford, California: Standford University Press.

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, *10*, 243–249.

Green, N. (2002). On the move: Technology, mobility and the mediation of social time and space. *The Information Society*, *18*(4), 281–292.

Hare, R. D. (1970). *Psychopathy: theory and research*. Wiley.

Hawley, A. (1950). *Human Ecology: A Theory of Community Structure*. New York: Ronald Press.

Hemphill, S. a, Kotevski, A., Tollit, M., Smith, R., Herrenkohl, T. I., Toumbourou, J. W., & Catalano, R. F. (2012). Longitudinal predictors of cyber and traditional bullying perpetration in Australian secondary school students. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *51*(1), 59–65.

Henggeler, S. W. (1989). *Delinquency in adolescence*. *Sage Publications,*. Thousand Oaks, CA: Sage Publications.

Henson, B. (2010). Cyberstalking. En *Encyclopedia of victimology and crime prevention*. Sage Publications.

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

Hernández, M. A., & Solano, I. M. (2007). Ciberbullying, un problema de acoso escolar. *Revista Iberoamericana de Educación a Distancia*, *10*(1), 17–36.

Hindelang, M. (1976). *Criminal Victimization in Eight American Cities: A Descriptive Analysis of Common Theft and Assault.* Cambridge, MA: Ballinger.

Hindelang, M., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: an empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger Publishing Co.

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

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, *14*(3), 206–221.

Hirschi, T. (1969). *Causas de la delincuencia. Berkeley y Los Angeles*. Los Ángeles: University of California Press.

Hoff, D. L., & Koops, B. J. (2011). Adolescents and Cybercrime: Natvigating between Freedom and Control. *Policy & Internet*, *3*(2), 1–28.

Hoff, D. L., & Mitchell, S. N. (2009). Cyberbullying: causes, effects, and remedies. *Journal of Educational Administration*, *47*(5), 652–665.

Hollis-Peel, M. E., Reynald, D. M., Van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: a critical review of the literature. *Crime, Law and Social Change*, *56*(1), 53–70.

Holt, T., & Bossler, A. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Hooton, E. A. (1931). *Up from the Ape*. New York: The Macmillan Company.

Jackson, C. L., & Cohen, R. (2012). Childhood victimization: Modeling the relation between classroom victimization, cyber victimization, and psychosocial functioning. *Psychology of Popular Media Culture*, *1*(4), 254–269.

Jacobs, J. (1961). *The Death and Life of Great American Cities*. New York, NY: Random House.

Jaishankar, K. (Ed). (2011). *Cyber Criminology*. Boca Ratón, FL: Taylor and Francis Group.

Jeffery, R. (1971). *Crime Prevention Through Environmental Design*. Beberly Hills, USA: SAGE Publications.

Jeffery, R. (1977). *Crime Prevention Through Environmental Design* (Rev. ed.). Beverly Hills: Sage Publications.

Jewkes, Y., & Yar, M. (2013). *Handbook of Internet crime*. New York: Routledge.

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012). Trends in youth internet victimization: findings from three youth internet safety surveys 2000-2010. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *50*(2), 179–86.

Jonsson, L. S., Priebe, G., Bladh, M., & Svedin, C. G. (2014). Voluntary sexual exposure online among Swedish youth – social background, Internet

behavior and psychosocial health. *Computers in Human Behavior*, *30*, 181–190.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? --Bullying experiences in cyberspace. *The Journal of School Health*, *78*(9), 496–505.

Kapatzia, A., & Sygkollitou, E. (2007). *Cyberbullying in middle and high schools: prevalence, gender and age differences*. Extraído el 3 marzo 2014 http://www.abs-center.si/gbccd/papers/p198.pdf

Katzer, C., Fetchenhauer, D., & Belschak, F. (2009). Cyberbullying: Who are the victims?: A comparison of victimization in internet chatrooms and victimization in school. *Journal of Media Psychology: Theories, Methods, and Applications*, *21*(1), 25.

Kelling, G., Pate, T., Dieckman, D., & Brown, C. (1974). *The Kansas City preventive patrol experiment: A summary report*. Washington: DC: Police Fundation.

Kowalski, R. M., & Fedina, C. (2011). Cyber bullying in ADHD and Asperger Syndrome populations. *Research in Autism Spectrum Disorders*, *5*(3), 1201–1208.

Kowalski, R. M., & Limber, S. P. (2007). Electronic Bullying Among Middle School Students. *Journal of Adolescent Health*, *41*, S22–S30.

Kowalski, R. M., & Limber, S. P. (2013). Psychological, physical, and academic correlates of cyberbullying and traditional bullying. *Journal of Adolescent Health*, *53*, S13–S20.

Kraepelin, E. (1915). *Psychiatrie: Ein Lehrbuchfür Studirende und Ärzte*. Leipzig: Barth.

Kraepelin, E. (2012). *La locura maniaco-depresiva*. Madrid: Ergon.

Kretschmer, E. (1961). *Constitución y carácter: investigaciones acerca del problema de la constitución y de la doctrina de los temperamentos* (3ª ed.). Barcelona: Labor.

Kshetri, N. (2011). Privacy and Security Aspects of Social Media : Institutional and Technological Environment. *Pacific Asia Journal of the Association for Information Systems*, *3*(4), 1–20.

Kuehl, D. T. (1957). From Cyberspace to Cyberpower: Defining the Problem. En F. D. Kraner, S. Starr, & L. K. Wentz (Eds.), *2009* (pp. 24–42). Virginia: Potomac Books Inc.

Kumazaki, A., Suzuki, K., Katsura, R., Sakamoto, A., & Kashibuchi, M. (2011). The Effects of Netiquette and ICT Skills on School-bullying and Cyber-bullying: The Two-wave Panel Study of Japanese Elementary, Secondary, and High School Students. *Procedia - Social and Behavioral Sciences*, *29*, 735–741.

Landry, J. M. (2008). Time and Space Compression in Criminology. *Professional Issues in Criminal Justice*, *3*(2), 87–96.

Law, D. M., Shapka, J. D., Hymel, S., Olson, B. F., & Waterhouse, T. (2012). The changing face of bullying: An empirical comparison between traditional and internet bullying and victimization. *Computers in Human Behavior*, *28*(1), 226–232.

Lee, S. J., & Chae, Y. G. (2007). Children´s Internet use in a family context: Influence on family relationships and parental mediation. *CyberPsychology & Behavior*, *10*, 640–644.

Lemert, E. M. (1951). *Social Pathology: A Systematic Approach to the Theory of Sociopathic Behavior*. New York: MacGraw-Hill.

Lemieux, A., & Felson, M. (2012). Risk of Violent Crime Victimization During Major Daily Activities. *Violence and Victims*, *27*(5), 635–655.

Lévy, P. (1998). *¿Qué es lo virtual?* Barcelona: Paidós.

Li, Q. (2006). Cyberbullying in Schools: A Research of Gender Differences. *School Psycology International*, *27*(2), 157–170.

Li, Q. (2007a). Bullying in the new playground: Research into cyberbullying and cyber victimisation. *Australasian Journal of Educational Technology*, *23*(4), 435.

Li, Q. (2007b). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, *23*(4), 1777–1791.

Li, Q. (2008). A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Research*, *50*(3), 223–234. doi:10.1080/00131880802309333

Li, Q. (2010). Cyberbullying in high schools: A study of students' behaviors and beliefs about this new phenomenon. *Journal of Aggression, Maltreatment & Trauma*, *19*(4), 372–392.

Lombroso, C. (1876). *L'uomo delinquente: stuiato in rapporto alla antropología, alla medicina legale ed alle discipline carcerarie*. Milano: Hoepli.

Lombroso, C. (1902). *El delito: sus causas y remedios*. Madrid: Librería General de Victoriano Suarez.

Luengo, J. A. (2014). Ciberbullying: Prevenir y Actuar. Colegio Oficial de Psicológos de Madrid.

Luque, M. E. (2006). Las encuentas de victimizacion. En E. En Baca, E. Echeburua, & J. M. Tamarit (Eds.), *Manual de victimología*. Valencia: Tirant lo Blanch.

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: an examination of adolescents' protection behavior against online harassment. *Journal of Adolescence*, *35*(1), 31–41.

MacDonald, C. D., & Roberts-Pittman, B. (2010). Cyberbullying among college students: prevalence and demographic differences. *Procedia Social and Behavioral Sciences*, *9*, 2003–2009.

Marañon, G. (1946). *Manual de diagnóstico etiológico*. Madrid: Espasa Calpe.

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

Marcum, C. D. (2008). Identifying Potential Factors of Adolescent Online Victimization for High School Seniors. *International Journal of Cyber Criminology*, *2*(2), 1–18.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing Sex Experiences of Online Victimization: An Examination of Adolescent Online Behaviors Using Routine Activity Theory. *Criminal Justice Review*, *35*(4), 412–437.

Maudsley, H. (1871). *Body and mind: an inquiri into their connection and mutual influence, specially in reference to mental disorders*. New York, NY: Appleton and Co.

Mayans, J. (2003). El ciberespacio, un nuevo espacio público para el desarrollo de la identidad local. En *Conferencia inaugural del III Encuentro de Telecentros y Redes de Telecentros*. Valladolid.

Mayhew, P., Clarke, R. V., Sturman, A., & Hough, J. M. (1976). Crime as Opportunity. In *Home Office Police Research Study. No. 4*. London: Home Office.

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.

Medina, J. E. (2013). *Prevención de la conducción influenciada por medio de los mapas del crimen. Un análisis desde la aplicación de las teorías criminológicas ambientales a la seguridad vial en Elche*. Tesis Doctoral. Universidad Miguel Hernández.

Medina, J. E. (2014). Felson, Marcus. En (M. Miller, Ed.) *The Encyclopedia of Theoretical Criminology*. John Wiley & Sons, Ltd.

Medina, J. J. (2011). *Políticas y estrategias de prevención del delito y seguridad ciudadana*. Madrid: Edisofer, S. L.

Merton, R. K. (1938). Social Structure and anomie. *American Sociological Review*, *3*(5), 672–682.

Messner, S. F., Lu, Z., Zhang, L., & Liu, J. (2007). Risks of Criminal Victimization in Contemporary Urban China: An Application of Lifestyle/Routine Activities Theory. *Justice Quarterly*, *24*(3), 496–522.

Miró, F. (2005). *Internet y delitos contra la propiedad intelectual*. Madrid: Iberautor Promociones Culturales.

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*(7), 1–55.

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

Miró, F. (2013a). Informe técnico sobre Encuesta Nacional de cibervictimización. Diputación de Alicante y Centro Crímina de la Universidad Miguel Hernández.

Miró, F. (2013b). Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio. *Revista de Internet, Derecho Y Política*, *16*, 61–75.

Miró, F. (2013c). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigacion Criminológica*, *11*, 1–35.

Miró, F. (2014a). Estudio sobre el alcance de la cibercriminalidad contra menores en la provincia de Alicante. Diputación de Alicante y Centro Crímina de la Universidad Miguel Hernández.

Miró, F. (2014b). Routine Activity Theory. En (M. Miller, Ed.) *The Encyclopedia of Theoretical Criminology*. John Willey & Sons.

Miró, F. (2014c). Rethinking Targuet Suitability in Cyberspace: Cybervictimization in Preparatory Economic Cybercrimes and Routine Activities in Cyberspace. *En Prensa*.

Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. *Children and Youth Services Review*, *34*(1), 63–70.

Mishna, F., Saini, M., & Solomon, S. (2009). Ongoing and online: Children and youth's perceptions of cyber bullying. *Children and Youth Services Review*, *31*(12), 1222–1228.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Online requests for sexual pictures from youth: risk factors and incident characteristics. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *41*(2), 196–203.

Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra, M. L., & Turner, H. (2011). Youth Internet victimization in a broader victimization context. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *48*(2), 128–34.

Mitchell, K. J., Jones, L. M., & Wells, M. (2013). Testing the Index of Problematic Online Experiences (I-POE) with a national sample of adolescents. *Journal of Adolescence*, *36*(6), 1153–63.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2007). Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the Internet. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *40*(2), 116–26.

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), 277–94.

Monahan, J. T., & Dennis, D. L. (1996). *Coercion and Aggressive Community Treatment; A New Frontier in Mental Health Law*. New York: Plenum Press.

Morales-Vallejo, P. (2012). *El tamaño del efecto (effect size): Análisis complementarios al contraste de medias Estadísticas aplicada a las Ciencias Sociales*. Madrid: Universidad Pontificia Comillas, Facultad de Ciencias Humanas y Sociales.

Morillas, D. L. (2005). *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*. Madrid: Dykinson.

Morillas, D. L., Patró, R. M., & Aguilar, M. (2011). *Victimología: un estudio sobre la víctima y los procesos de victimizacion.* (1ª ed.). Madrid: Dykinson.

Morillas, L. (2006). Nuevas Tendencias del Derecho Penal: ¿Hacia un Derecho Penal del Enemigo? Una Reflexión Dirigida a la Cibercriminalidad. *Estudios Jurídicos*, 1–16.

Morillas, L. (2008). Nuevas tendencias del Derecho penal. Una reflexión dirigida a la cibercriminalidad. *Cuadernos de Política Criminal*, *94*(1), 5–32.

Mura, G., Topcu, C., Erdur-Baker, O., & Diamantini, D. (2011). An international study of cyber bullying perception and diffusion among adolescents. *Procedia - Social and Behavioral Sciences*, *15*, 3805–3809.

Newuman, O. (1972). *Defensible Space: Crime Prevention Through Urban Design*. New York, NY: Macmillan.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Ciberbullying: Labels, Behaviours and Definition in Three European Countries. *Australian Journal of Guidance & Counselling*, *20*(2), 129–142.

Olenik-Shemesh, D., Heiman, T., & Eden, S. (2012). Cyberbullying victimisation in adolescence: Relationships with loneliness and depressive mood. *Emotional and Behavioural Difficulties*, *17*(3-4), 361–374.

Olmedo, M. (2009). Procedencia Aspectos generales y particulares de los delitos informáticos en el Código Penal vigente. En *Seguridad y nuevas tecnologías: XX Seminario "Duque de Ahumada"* (pp. 13–20). Madrid: Ministerio del Interior.

Olweus, D. (1993). *Conductas de acoso y amenaza entre escolares*. Madrid: Morata.

Olweus, D. (2005). Bullying en la escuela: datos e intervención. En *Violencia y escuela*. Valencia: Centro Reina Sofía para el estudio de la violencia.

ONTSI. (2011). Primer estudio sobre tendencias de las redes sociales en España. Ministerio de Industria, Energía y Turismo.

Ortega, R., Calmaestra, J., & Mora-Merchán, J. A. (2008). Cyberbullying. *International Journal of Psychology and Psychological Therapy*, *8*(2), 183–192.

Ortega, R., Del Rey, R., & Mora-Merchán, J. A. (2001). Violencia entre escolares: conceptos y etiquetas verbales que definen el fenómeno del maltrato entre iguales. *Revista Interuniversitaria de Formación Del Profesorado*, *41*, 95–113.

Ortega, R., Elipe, P., Mora-Merchán, J. A., Calmaestra, J., & Vega, E. (2009). The Emotional Impact on Victims of Traditional Bullying and Cyberbullying. *Journal of Psychology*, *217*(4), 197–204.

Papakonstantinou, V. (2010). Cyberspace And Cybercrime. En H. Jahankhani, D. L. Watson, G. Me, & F. Leonhardt (Eds.), *Handbook of Electronic Security and Digital Forensics* (pp. 455–476). Singapure: World Scientific.

Pardo, J. (2010). Ciberacoso: cyberbullying, grooming, redes sociales y otros peligro. En J. García González (Ed.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet* (pp. 51–84). Valencia: Tirant lo Blanch.

Park, R. E., Burguess, E. W., & MacKenzie, R. D. (1925). *The city*. Chicago: University of Chicago Press.

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, *4*, 148–160.

Patchin, J. W., & Hinduja, S. (2010). Changes in adolescent online social networking behaviors from 2006 to 2009. *Computers in Human Behavior*, *26*(6), 1818–1821.

Patchin, J. W., & Hinduja, S. (2012). School-Based Efforts to Prevent Cyberbullying. *The Prevention Researcher*, *19*(3), 17–20.

Path, M., & Mullen, P. E. (1997). The impact of stalkers on their victims. *The British Journal of Psychiatry*, *170*(1), 12–17.

Pease, K. (1998). Repeat Victimization: Taking stock. Crime Detection and Prevention Series, Paper 90. London: Home Office.

Pease, K. (2001). Crime futures and foresight: Challenging criminal behaviour in the information age. En D. Wall (Ed.), *Crime and the Internet* (pp. 18–28). London: Routledege.

Pease, K., & Laycock, G. (1996). Revictimization: Reducing the Heat on Hot Victims. *Research in Action*.

Pereda, N. (2013). Aspectos metodológicos y Epidemiológicos. En N. Pereda & J. M. Tamarit (Eds.), *Victimología teórica y aplicada* (pp. 77–99). Barcelona: Huygens Editorial.

Pereda, N., Abad, J., & Guilera, G. (2012). Victimización de menores a través de Internet: descripción y características de las víctimas de online grooming. En L. M. Diaz Cortés & F. Pérez Alvarez (Eds.), *Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas ciencias penales: memorias II Congreso Internacional de Jóvenes Investigadores en Ciencias Penales 27, 28 y 29 de junio de 2011* (pp. 91–105). Salamanca: Ediciones Universidad de Salmanca.

Pereda, N., Guilera, G., & Abad, J. (2014). Victimization and polyvictimization of Spanish children and youth: Results from a community sample. *Child Abuse & Neglect*, *38*(4), 640–649.

Pérez, A., & Ortigosa, A. (2010). Una aproximación al ciberbullying. En J. García González (Ed.), *Ciberacoso: La tutela penal de la intimidad, la integridad y la libertad sexual en Internet* (pp. 15–28). Valencia: Tirant lo Blanch.

Pieschl, S., Porsch, T., Kahl, T., & Klockenbusch, R. (2013). Relevant dimensions of cyberbullying — Results from two experimental studies. *Journal of Applied Developmental Psychology*, *34*(5), 241–252.

Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2013). Analyzing the Influence of Micro-Level Factors on CCTV Camera Effect. *Journal of Quantitative Criminology*, *30*(2), 237–264.

Pollak, O. (1950). *The criminality of women*. Pennnsylvania: University of Pennsylvania Press.

Pratt, T. C., Holtfreter, K., & 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.

Price, M., & Dalgleish, J. (2010). Cyberbulling: Experiences, impacts and coping strategies as described by Australian young people. *Youth Studies Australia*, *29*(2), 51–64.

Puebla, J. G. (1998). Redes, espacio y tiempo. *Anales de Geografía de La Universidad Complutense*, *18*, 65–86.

Quetelet, A. (1833). *Research on the propensity for crime at different ages* (2º ed.). Cincinnati, OH: Anderson.

Quetelet, A. (2010). Of the Development of the Propensity to Crime (1842). En M. Andresen, P. Brantigham, & J. B. Kinney (Eds.), *Classics in Environmental Criminology* (pp. 29–75). Burnaby, Canadá: CRC Press.

Quinney, R. (1972). Who is the victim? *Criminology*, *10*(3), 314–323.

Raine, A. (1993). *The Psychopathology of Crime: criminal behavior as a clinical disorder*. San Diego: Gulf Professional Publishing.

Raine, A. (2013). *The Anatomy of Violence: The Biological Roots of Crime*. New York: Pantheon.

Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. *Developmental Psychology*, *43*(3), 564–575.

Rechea, C. (2008). *Estudios de criminología III*. Cuenca: Universidad de Castilla-La Mancha.

Reckless, W. C. (1970). American Criminology. *Criminology*, *8*(1), 4–22.

Redondo, S., & Martínez, A. (2011). Tratamiento y Cambio terapéutico en agresores sexuales. *Revista Española de Investigacion Criminológica*, *9*, 1–25.

Reiss, A. J. (1959). Are Educational Norms and Goals of Conforming, Truant, and Delinquent Adolescents Influence by Gropu Position in American Society? *Journal of Negro Educatión*, *37*, 252–267.

Reyns, B. W. (2010). *Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective*. Tesis Doctoral. University of Cincinnati.

Reyns, B. W., & Englebrecht, C. M. (2010). The stalking victim's decision to contact the police: A test of Gottfredson and Gottfredson's theory of criminal justice decision making. *Journal of Criminal Justice*, *38*(5), 998–1005.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Ribeiro, G. L. (2002). *El espacio-público-virtual*. Brasília: Departamento de Antropologia Instituto de Ciências Sociais Universidade de Brasília.

Romeo Casabona, C. M. (1988). *El poder informático y seguridad jurídica*. Madrid: Fundesco.

Romeo Casabona, C. M. (2006). De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal. En J. A. Choclán Montalvo (Ed.), *El cibercrimen Nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares.

Ruiz-Funes García, M. (1929). *Endocrinología y criminalidad*. Madrid: Javier Morata.

Rus, G. (1999). Protección penal de sistemas, elementos, datos, documentos y programas informáticos. *Revista Electrónica de Ciencia Penal Y Criminología*, *1*, 1–14.

Sabella, R. a., Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. *Computers in Human Behavior*, *29*(6), 2703–2711.

Şahín, M. (2012). The relationship between the cyberbullying/cybervictmization and loneliness among adolescents. *Children and Youth Services Review*, *34*(4), 834–837.

Salter, A. C. (2003). *Predators: Pedophiles, Rapists, and Other Sex Offenders: Who They Are, How They Operatem and How We Can Protect Our Children*. New York: Basic Books.

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: Au routine activity explanation of crime prevention success and failure. *Security Journal*, *23*, 37–51.

Sasson, H., & Mesch, G. (2014). Parental mediation, peer norms and risky online behavior among adolescents. *Computers in Human Behavior*, *33*, 32–38.

Schultze-Krumbholz, A., & Scheithauer, H. (2009). Social-Behavioral Correlates of Cyberbullying in a German Student Sample. *Journal of Psychology*, *217*(4), 224–226.

Sengupta, A., & Chaudhuri, A. (2011). Are social networking sites a source of online harassment for teens? Evidence from survey data. *Children and Youth Services Review*, *33*(2), 284–290.

Serrano Maillo, A. (2004). *Introuducción a la Criminología* (2ª ed.). Madrid: Dykinson.

Serrano Maillo, A. (2009). *Oportunidad y delito*. Madrid: Dykinson.

Serrano Maíllo, A. (2009). *Introducción a la Criminología* (6ª ed.). Madrid: Dykinson.

Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas*. Chicago: University of Chicago Press.

Sheldon, W. (1942). *The varieties of Temperament*. London: Macmillan Pub Co.

Sherman, L. W., Gartin, P. R., & Buerguer, M. E. (1989). Hot Spots Of Predatory Crime: Routine Activities And The Criminology Of Place. *Criminology*, *27*(1), 27–56.

Shin, W., & Huh, J. (2011). Parental mediation of teenagers´video game playing: Antecedents and consequences. *New Media & Society*, *13*, 945–962.

Sieber, U. (1980). *Computer Kriminalität und Strafrecht* (2ª ed.). Köln: Heymanns.

Sieber, U. (1998). Legal Aspects of Computer Related Crime in the Information Society. University of Würzburg. COMCRIME-Study Prepared for the European Commission.

Sinclair, K. O., Bauman, S., Poteat, V. P., Koenig, B., & Russell, S. T. (2012). Cyber and bias-based harassment: associations with academic, substance use,

and mental health problems. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *50*(5), 521–523.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, *49*, 147–154.

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, *29*(1), 26–32.

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

Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). *An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying*. *Research Brief*. Research Brief No RBX03-06 London.

Smith, P. K., & Sharp, S. (1994). The problem of school. En P. K. Smith & S. Sharp (Eds.), *School Bullying*. London: Routledge.

Snakenborg, J., Van Acker, R., & Gable, R. a. (2011). Cyberbullying: Prevention and Intervention to Protect Our Children and Youth. *Preventing School Failure: Alternative Education for Children and Youth*, *55*(2), 88–95.

Spano, R., & Freilich, J. (2009). An assessment of the empirical validity and conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005. *Journal of Criminal Justice*, *37*(3), 305–314.

Suárez, I. (2013). *El Gobierno de Internet*. iSuarez.

Sumter, S. R., Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2012). Developmental trajectories of peer victimization: Off-line and online experiences during adolescence. *Journal of Adolescent Health*, *50*(6), 607–613.

Sureda, J., Mut, B., Comas, R., Casero, A., Oliver, M., Salvà, F., & Morey, M. (2008). *Les TIC i els menors a les Illes Balears*. *Les TIC i els menors a les Illes Balears*. Palma, Illes Balears: Fundació IBIT.

Sutherland, E. H. (1939). *Principles of criminology*. Philadelphia: Lippincott.

Sutherland, E. H., & Cresswy, D. R. (1960). *Principles of criminology* (6ª ed.). Chicago: Lippincott.

Tamarit, J. M. (2006). La victimología: cuestiones conceptuales y metodológicas. In E. Beca, E. Echeburúa, & J. M. Tamarit (Eds.), *Manual de victimología* (pp. 17–50). Valencia: Tirant lo Blanch.

Tamarit, J. M. (2014). Las respuestas a la victimización: nuevas formas de intervención y reparación que garantice el rol subsidiario de la justicia penal. En J. M. Tamarit & N. Pereda (Eds.), *La respuesta de la victimología ante las nuevas formas de victimización* (pp. 303–336). Madrid: Edisofer, S.L.

Taylor, L., Walton, P., & Young, J. (1973). *The new criminology: for a theory of social deviance*. London: Routledge.

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). *Digital crime and digital terrorism*. Upper Saddle River, NJ: Pearson Prentice Hall.

Thrasher, F. . (1927). *The Gang: A Study of 1,313 Gangs in Chicago*. Chicago: Phoenix Books.

Tilley, N. (2009). *Crime Prevention*. Collumpton: William Publishing.

Tillyer, M. S., & Eck, J. E. (2009). Routine Activities. En J. M. Miller (Ed.), *21st Century Criminology: A Reference Handbook* (pp. 279–287). Thousand Oaks: SAGE.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, *26*(3), 277–287.

Turner, M. G., Exum, M. L., Brame, R., & Holt, T. J. (2013). Bullying victimization and adolescent mental health: General and typological effects across sex. *Journal of Criminal Justice*, *41*(1), 53–59.

Valkenburg, P. M., & Peter, J. (2011). Online communication among adolescents: an integrated model of its attraction, opportunities, and risks. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *48*(2), 121–7.

Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: a qualitative research into the perceptions of youngsters. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *11*(4), 499–503.

Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New Media & Society*, *11*(8), 1349–1371.

Varjas, K., Henrich, C. C., & Meyers, J. (2009). Urban middle school students' perceptions of bullying, cyberbullying, and school safety. *Journal of School Violence*, *8*(2), 159–176.

Vozmediano, L., & San Juan, C. (2010). *Criminología ambiental. Ecología del delito y de la seguridad*. Barcelona: Editorial UOC.

Wall, D. (2001). Cybercrimes and the Internet. En D. Wall (Ed.), *Crime and the Internet* (pp. 1–17). London: Routledge.

Wall, D. (2005). What are Cybercrimes? *Criminal Justice Matters*, *58*, 20.

Wall, D. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. *International Review of Law, Computers & Technology*, *22*(1-2), 45–63.

Walsh, A. (1995). *Biosociology: An Emerging Paradigm*. Westport: Praeger.

Wang, J., Iannotti, R., & Luk, J. (2012). Patterns of adolescent bullying behaviors: physical, verbal, exclusion, rumor, and cyber. *Journal of School Psychology*, *50*(4), 521–34.

Wang, J., Lannotti, R. J., & Nansel, T. R. (2009). School Bullying Among Adolescents in the United States: Physical, Verbal, Relational, and Cyber. *Journal of Adolescent Health*, *45*(4), 368–375.

Wang, J., Nansel, T., & Iannotti, R. (2011). Cyber and traditional bullying: differential association with depression. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *48*(4), 415–7.

Wentz, L. K. (2009). *Cyberpower and National Security*. Virginia: Potomac Books Inc.

Whittle, H. C., Hamilton-Giachristsis, C., Beech, A., & Collings, G. (2013). Areview of young people's vulnerabilities to online grooming. *Aggression and Violent Behavior*, *18*, 62–70.

Wigderson, S., & Lynch, M. (2013). Cyber-and traditional peer victimization: Unique relationships with adolescent well-being. *Psychology of Violence*, *3*(4), 297–309.

Willard, N. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Champaign, IL: Research Press.

Williams, K., & Guerra, N. (2007). Prevalence and predictors of internet bullying. *Journal of Adolescent Health*, *41*, S14–21.

Williams, M. (2007). Cyber-crime on the move. En S. Kleinman (Ed.), *Displacing Place: Mobile Communication in the Twenty-firts Century* (pp. 91–104). New York: Lang Publishing.

Wilsem, J. V. (2011). "Bought it, but Never Got it" Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, *29*(2), 168–178.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online "predators" and their victims: myths, realities, and implications for prevention and treatment. *The American Psychologist*, *63*(2), 111–28.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known

peers and online-only contacts. *Journal of Adolescent Health*, *41*, 51–58.

Wolfgang, M. E., & Ferracuti, F. (1967). *The subculture of violence*. *Sage Publications*. Londres: Tavistock.

Wong, D., Chan, H., & Cheng, C. (2014). Cyberbullying perpetration and victimization among adolescents in Hong Kong. *Children and Youth Services Review*, *36*, 133–140.

Xiao, B. S., & Wong, Y. M. (2013). Cyber-Bullying Among University Students: An Empirical Investigation from the Social Cognitive Perspective. *International Journal of Business and Information*, *8*(1), 34–69.

Yang, S. J., Stewart, R., Kim, J. M., Kim, S. W., Shin, I. S., Dewey, M. E., Maskey, S., & Yoon, J. S. (2013). Differences in predictors of traditional and cyber-bullying: a 2-year longitudinal study in Korean school children. *European Child & Adolescent Psychiatry*, *22*(5), 309–318.

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

Yar, M. (2006). *Cybercrime and society*. London: Sage.

Ybarra, M. L. (2004). Linkages between depressive symptomatology and Internet harassment among Young regular Internet users. *CyberPsychology & Behavior*, *7*, 247–257.

Ybarra, M. L., Diener-West, M., & Leaf, P. J. (2007). Examining the overlap in Internet harassment and school bullying: Implications for school intervention. *Journal of Adolescent Health*, *41*(6), 42–50.

Ybarra, M. L., Espelage, D. L., & Mitchell, K. J. (2007). The co-occurrence of Internet harassment and unwanted sexual solicitation victimization and perpetration: associations with psychosocial indicators. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *41*(6), 31–41.

Ybarra, M. L., & Mitchell, K. J. (2004a). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, *45*(7), 1308–1316.

Ybarra, M. L., & Mitchell, K. J. (2004b). Youth engaging in online harassment: associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, *27*(3), 319–36.

Ybarra, M. L., & Mitchell, K. J. (2007). Prevalence and Frequency of Internet Harassment Instigation: Implications for Adolescent Health. *Journal of Adolescent Health*, *41*(2), 189–195.

Ybarra, M. L., & Mitchell, K. J. (2008). How risk are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics*, *121*(2), 350–357.

Ybarra, M. L., Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Internet Prevention Messages: Targeting the Right Online Behaviors. *Archives of Pediatrics & Adolescent Medicine*, *161*, 138–145.

Ybarra, M., Mitchell, K., Wolak, J., & Finkelhor, D. (2006). Examining characteristics and associated distress related to Internet harassment: findings from the Second Youth Internet Safety Survey. *Pediatrics: Official Journal of the Academy of Pediatrics*, *118*(4), 1169–1177.

Young, K. (2005). Profiling online sex offenders, cyber-predators, and pedophiles. Journal of Behavioral Profiling. *Journal of Behavioral Profiling*, *5*(1), 1–18.

Yucedal, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories*. Tesis Doctoral. Kent State University.

Tabla de ilustraciones

ILUSTRACIÓN 1. EVOLUCIÓN DEL USO DE LAS TIC EN LA POBLACIÓN ESPAÑOLA 2003-2013. ELABORACIÓN PROPIA A PARTIR DE LOS DATOS OFRECIDOS POR EL INE 78
ILUSTRACIÓN 2. USO DE INTERNET Y DEL MÓVIL POR EDAD. ELABORACIÓN PROPIA A PARTIR DE LOS DATOS DEL INE (2013) 80
ILUSTRACIÓN 3. TRIÁNGULO DE LA CRIMINALIDAD 128
ILUSTRACIÓN 4. REPRESENTACIÓN DEL CONTACTO EN EL ESPACIO FÍSICO ENTRE UN AGRESOR MOTIVADO Y UNA VÍCTIMA. OBTENIDO DE MIRÓ (2011, P.27) 199
ILUSTRACIÓN 5. REPRESENTACIÓN DEL CONTACTO EN EL CIBERESPACIO ENTRE UN AGRESOR MOTIVADO Y UNA VÍCTIMA. OBTENIDO DE MIRÓ (2011; P. 28) 199
ILUSTRACIÓN 6. INTERACCIÓN EN EL CIBERESPACIO DE UN USUARIO. OBTENIDO DE MIRÓ (2011; P. 32) 201
ILUSTRACIÓN 7. SEXO DE LOS PARTICIPANTES 220
ILUSTRACIÓN 8. HISTOGRAMA EDAD 221
ILUSTRACIÓN 9. DISTRIBUCIÓN DE LOS PARTICIPANTES POR CURSO 221
ILUSTRACIÓN 10. PREVALENCIA DE CIBERVICTIMIZACIÓN POR INSULTOS CONTINUADOS .. 251
ILUSTRACIÓN 11. PREVALENCIA DE CIBERVICTIMIZACIÓN POR RUMORES O MENTIRAS CONTINUADAS 252
ILUSTRACIÓN 12. PREVALENCIA DE CIBERVICTIMIZACIÓN POR CONTACTO REPETIDO NO DESEADO 252
ILUSTRACIÓN 13. PREVALENCIA DE CIBERVICTIMIZACIÓN POR HABER SIDO MARGINADO DE MANERA REPETIDA 253
ILUSTRACIÓN 14. OFRECER DATOS PERSONALES REALES A TRAVÉS DE INTERNET 254
ILUSTRACIÓN 15. TIPO DE DATOS PERSONALES FACILITADOS POR INTERNET 255
ILUSTRACIÓN 16. MEDIO EMPLEADO PARA CEDER DATOS PERSONALES REALES EN INTERNET 256
ILUSTRACIÓN 17. GUARDAR INFORMACIÓN O ARCHIVOS EN EL ORDENADOR CON EL QUE SE CONECTAN A INTERNET 257
ILUSTRACIÓN 18. TIPO DE INFORMACIÓN CONTENIDA EN EL ORDENADOR CON EL QUE SE CONECTA A INTERNET 258
ILUSTRACIÓN 19. GUARDAR INFORMACIÓN O ARCHIVOS EN EL MÓVIL CON EL QUE SE CONECTAN A INTERNET 259

ILUSTRACIÓN 20. TIPO DE INFORMACIÓN CONTENIDA EN EL ORDENADOR CON EL QUE SE CONECTAN A INTERNET 260
ILUSTRACIÓN 21. USO OTORGADO AL MÓVIL 261
ILUSTRACIÓN 22. NÚMERO DE CORREOS RECIBIDOS AL DÍA 262
ILUSTRACIÓN 23. HORAS A LA SEMANA DEDICADAS A CHATEAR 263
ILUSTRACIÓN 24. HORAS AL DÍA DEDICADAS A LAS REDES SOCIALES 265
ILUSTRACIÓN 25. NÚMERO DE CUENTAS ABIERTAS DE REDES SOCIALES USANDO DATOS REALES 266
ILUSTRACIÓN 26. USO EMPLEADO A LAS REDES SOCIALES 268
ILUSTRACIÓN 27. PERSONAS QUE AGREGAN A LAS REDES SOCIALES 269
ILUSTRACIÓN 28. POSEER UN BLOG PROPIO 270
ILUSTRACIÓN 29. ESCRIBIR COMENTARIOS EN BLOGS O FOROS AJENOS 270
ILUSTRACIÓN 30. HORAS A LA SEMANA DEDICADAS A HACER VIDEOCONFERENCIAS O VIDEOLLAMADAS 271
ILUSTRACIÓN 31. HORAS A LA SEMANA DEDICADAS A JUGAR A VIDEOJUEGOS *ONLINE* CON EL ORDENADOR 273
ILUSTRACIÓN 32. HORAS A LA SEMANA DEDICADAS A JUGAR A VIDEOJUEGOS *ONLINE* CON EL MÓVIL 274
ILUSTRACIÓN 33. CHATEAR A TRAVÉS DE VIDEOJUEGOS *ONLINE* 276
ILUSTRACIÓN 34. CONTACTAR CON DESCONOCIDOS A TRAVÉS DE INTERNET 276
ILUSTRACIÓN 35. MEDIO USADO PARA CONTACTAR CON DESCONOCIDOS A TRAVÉS DE INTERNET 277
ILUSTRACIÓN 36. MOTIVO POR EL QUE CONTACTAN CON DESCONOCIDOS 278
ILUSTRACIÓN 37. SEXTING 279
ILUSTRACIÓN 38. COMPORTAMIENTO DESVIADO 280
ILUSTRACIÓN 39. COMPARTIR EL ORDENADOR 281
ILUSTRACIÓN 40. LIMITAR EL ACCESO A LAS REDES SOCIALES 282
ILUSTRACIÓN 41. COMUNICAR A LOS PADRES EL USO DE LAS REDES SOCIALES 283
ILUSTRACIÓN 42. CONTROL DE LOS PADRES SOBRE EL USO DEL ORDENADOR Y EL MÓVIL 284
ILUSTRACIÓN 43. SATURACIÓN EN COMPONENTES. GUARDAR 288
ILUSTRACIÓN 44. SATURACIÓN EN COMPONENTES. FACILITAR INFORMACIÓN PERSONAL REAL A TRAVÉS DE INTERNET 291
ILUSTRACIÓN 45. SATURACIÓN EN COMPONENTES. MEDIOS USADOS PARA FACILITAR INFORMACIÓN PERSONAL REAL 293

ILUSTRACIÓN 46. SATURACIÓN EN COMPONENTES. COMPORTAMIENTO DESVIADO EN EL CIBERESPACIO 295
ILUSTRACIÓN 47. SATURACIÓN EN COMPONENTES. USO DE HERRAMIENTAS DE COMUNICACIÓN 298
ILUSTRACIÓN 48. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA CONTACTAR CON CONOCIDOS 300
ILUSTRACIÓN 49. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA COTILLEAR 302
ILUSTRACIÓN 50. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA ESTABLECER RELACIONES SENTIMENTALES 304
ILUSTRACIÓN 51. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA CONTACTAR CON DESCONOCIDOS 307
ILUSTRACIÓN 52. SATURACIÓN EN COMPONENTES. NO AGREGAR A LOS FAMILIARES A LAS REDES SOCIALES 309
ILUSTRACIÓN 53. SATURACIÓN EN COMPONENTES. NO SUPERVISIÓN 311
ILUSTRACIÓN 54. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. COMPONENTE GUARDAR 314
ILUSTRACIÓN 55. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. FACILITAR INFORMACIÓN PERSONAL REAL A TRAVÉS DE INTERNET 315
ILUSTRACIÓN 56. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. MEDIOS USADOS PARA FACILITAR INFORMACIÓN PERSONAL REAL 315
ILUSTRACIÓN 57. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. COMPORTAMIENTO DESVIADO EN EL CIBERESPACIO 316
ILUSTRACIÓN 58. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. USO DE HERRAMIENTAS DE COMUNICACIÓN 316
ILUSTRACIÓN 59. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. USO DE LAS TIC PARA CONTACTAR CON CONOCIDOS 317
ILUSTRACIÓN 60. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. USO DE LAS TIC PARA COTILLEAR 317
ILUSTRACIÓN 61. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. USO DE LAS TIC PARA ESTABLECER RELACIONES SENTIMENTALES 318
ILUSTRACIÓN 62. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. USO DE LAS TIC PARA CONTACTAR CON DESCONOCIDOS 318
ILUSTRACIÓN 63. GRÁFICO Q-Q NORMAL DE PUNTUACIONES. NO AGREGAR A LOS FAMILIARES A LAS REDES SOCIALES 319
ILUSTRACIÓN 64. GRÁFICO Q-Q NORMAL DE PUNTUACIÓN. NO CONTROL 319
ILUSTRACIÓN 65. EJEMPLO PERCEPTRÓN 367

ILUSTRACIÓN 66. DIAGRAMA DE RED.....375
ILUSTRACIÓN 67. CURVAS ROC.....378
ILUSTRACIÓN 68. IMPORTANCIA NORMALIZADA DE LAS VARIABLES INDEPENDIENTES 382

Índice de tablas

TABLA 1. REVISIÓN SOBRE LA CONSTRUCCIÓN DE LAS VARIABLES DE LA TAC EN LOS ESTUDIOS DE VICTIMIZACIÓN ECONÓMICA 157
TABLA 2. REVISIÓN DE LOS FACTORES DE RIESGO RELACIONADOS CON LA CIBERVICTIMIZACIÓN ECONÓMICA 162
TABLA 3. FICHA TÉCNICA DEL ESTUDIO *IDENTIFYING POTENTIAL FACTORS OF ADOLESCENT ONLINE VICTIMIZATION FOR HIGH SCHOOL SENIORS* (MARCUM, 2008) 165
TABLA 4. FICHA TÉCNICA DEL ESTUDIO *EXAMINING THE APPLICABILITY OF LIFESTYLE-ROUTINE ACTIVITIES THEORY FOR CYBERCRIME VICTIMIZATION* (HOLT Y BOSSLER, 2009) 166
TABLA 5. FICHA TÉCNICA DEL ESTUDIO BEING A PURSUED ONLINE: EXTENT AND NATURE OF CYBERSTALKING VICTIMIZATION FROM A LIFESTYLE/ROUTINE ACTIVITIES PERSPECTIVE (REYNS, 2010) 167
TABLA 6. FICHA TÉCNICA DEL ESTUDIO *CYBERCRIME VICTIMIZATION: AN EXAMINATION OF INDIVIDUAL AND SITUACIONAL LEVEL FACTORS* (NGO Y PATERNOSTER, 2011) 169
TABLA 7. FICHA TÉCNICA DEL ESTUDIO LA VICTIMIZACIÓN POR CIBERCRIMINALIDAD SOCIAL. UN ESTUDIO A PARTIR DE LA TEORÍA DE LAS ACTIVIDADES COTIDIANAS EN EL CIBERESPACIO (MIRÓ, 2013C) 171
TABLA 8. REVISIÓN DE LOS FACTORES DE RIESGO RELACIONADOS CON LA CIBERVICTIMIZACIÓN SOCIAL 180
TABLA 9. ESTADÍSTICOS DE LA VARIABLE EDAD 220
TABLA 10. TABLA RESUMEN DE LAS VARIABLES INCLUIDAS EN EL ESTUDIO 242
TABLA 11. ESTADÍSTICOS DE LA VARIABLE NÚMERO DE CORREOS RECIBIDOS AL DÍA 262
TABLA 12. ESTADÍSTICOS DE LA VARIABLE HORAS A LA SEMANA DEDICADAS A CHATEAR.. 264
TABLA 13. ESTADÍSTICOS DE LA VARIABLE HORAS AL DÍA DEDICADAS A LAS REDES SOCIALES 265
TABLA 14. ESTADÍSTICOS DE LA VARIABLE NÚMERO DE CUENTAS DE REDES SOCIALES 267
TABLA 15. ESTADÍSTICOS DE LA VARIABLE REALIZAR VIDEOCONFERENCIAS O VIDEOLLAMADAS 272
TABLA 16. ESTADÍSTICOS DE LA VARIABLE HORAS DEDICADAS A JUGAR A VIDEOJUEGOS *ONLINE* CON EL ORDENADOR 273
TABLA 17. ESTADÍSTICOS DE LA VARIABLE HORAS DEDICADAS A JUGAR A VIDEOJUEGOS *ONLINE* CON EL MÓVIL 275
TABLA 18. VARIABLES TRANSFORMADAS PARA EL CATPCA 285

TABLA 19. RESUMEN DEL MODELO. GUARDAR....287
TABLA 20. SATURACIÓN EN COMPONENTES. COMPONENTE GUARDAR....288
TABLA 21. RESUMEN DEL MODELO. FACILITAR INFORMACIÓN PERSONAL REAL A TRAVÉS DE INTERNET....289
TABLA 22. SATURACIÓN EN COMPONENTES. FACILITAR INFORMACIÓN PERSONAL REAL A TRAVÉS DE INTERNET....290
TABLA 23. RESUMEN DEL MODELO. MEDIOS USADOS PARA FACILITAR INFORMACIÓN PERSONAL REAL....292
TABLA 24. SATURACIÓN EN COMPONENTES. MEDIOS USADOS PARA FACILITAR INFORMACIÓN PERSONAL REAL....292
TABLA 25. RESUMEN DEL MODELO. COMPORTAMIENTO DESVIADO EN EL CIBERESPACIO...294
TABLA 26. SATURACIÓN EN COMPONENTES. COMPORTAMIENTO DESVIADO EN EL CIBERESPACIO....295
TABLA 27. RESUMEN DEL MODELO. USO DE HERRAMIENTAS DE COMUNICACIÓN....296
TABLA 28. SATURACIÓN EN COMPONENTES. USO DE HERRAMIENTAS DE COMUNICACIÓN..297
TABLA 29. RESUMEN DEL MODELO. USO DE LAS TIC PARA CONTACTAR CON CONOCIDOS ..299
TABLA 30. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA CONTACTAR CON CONOCIDOS....300
TABLA 31. RESUMEN DEL MODELO. USO DE LAS TIC PARA COTILLEAR....301
TABLA 32. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA COTILLEAR....301
TABLA 33. RESUMEN DEL MODELO. USO DE LAS TIC PARA ESTABLECER RELACIONES SENTIMENTALES....303
TABLA 34. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA ESTABLECER RELACIONES SENTIMENTALES....303
TABLA 35. RESUMEN DEL MODELO. USO DE LAS TIC PARA CONTACTAR CON DESCONOCIDOS 305
TABLA 36. SATURACIÓN EN COMPONENTES. USO DE LAS TIC PARA CONTACTAR CON DESCONOCIDOS....306
TABLA 37. RESUMEN DEL MODELO. NO AGREGAR A LOS FAMILIARES A LAS REDES SOCIALES 308
TABLA 38. SATURACIÓN EN COMPONENTES. NO AGREGAR A LOS FAMILIARES A LAS REDES SOCIALES 308
TABLA 39. RESUMEN DEL MODELO. NO CONTROL....310
TABLA 40. SATURACIÓN EN COMPONENTES. NO SUPERVISIÓN 310
TABLA 41. DESCRIPTIVOS DE LAS COMPONENTES PRINCIPALES....313

TABLA 42. PRUEBA DE KOLMOGOROV-SMIRNOV PARA UNA MUESTRA 314
TABLA 43. ANÁLISIS FACTORIAL: VARIANZA TOTAL EXPLICADA 321
TABLA 44. ANÁLISIS FACTORIAL: MATRIZ DE FACTORES ROTADOS 323
TABLA 45. TABLA DE CONTINGENCIA: VÍCTIMAS DE INSULTOS POR SEXO 325
TABLA 46. PRUEBAS DE CHI-CUADRADO: VÍCTIMAS DE INSULTO POR SEXO 326
TABLA 47. ESTIMACIÓN DE RIESGO: VÍCTIMAS DE INSULTO POR SEXO 326
TABLA 48. TABLA DE CONTINGENCIA: VÍCTIMAS DE RUMORES POR SEXO 327
TABLA 49. PRUEBAS DE CHI-CUADRADO: VÍCTIMAS DE RUMORES POR SEXO 328
TABLA 50. ESTIMACIÓN DE RIESGO: VÍCTIMAS DE RUMORES POR SEXO 328
TABLA 51. TABLA DE CONTINGENCIA: VÍCTIMAS DE CONTACTO REPETIDO POR SEXO 330
TABLA 52. PRUEBAS DE CHI-CUADRADO: VÍCTIMAS DE CONTACTO REPETIDO POR SEXO ... 331
TABLA 53. ESTIMACIÓN DE RIESGO: VÍCTIMAS DE CONTACTO REPETIDO POR SEXO 332
TABLA 54. TABLA DE CONTINGENCIA: VÍCTIMA DE MARGINACIÓN POR SEXO 333
TABLA 55. PRUEBAS DE CHI-CUADRADO: VÍCTIMAS DE MARGINACIÓN POR SEXO 334
TABLA 56. ESTIMACIÓN DE RIESGO: VÍCTIMAS DE MARGINACIÓN POR SEXO 335
TABLA 57. FRECUENCIA Y PORCENTAJE DE LA EDAD AGRUPADA 336
TABLA 58. VÍCTIMA DE INSULTOS POR EDAD 337
TABLA 59. ESTADÍSTICOS DE CONTRASTE. VÍCTIMA INSULTOS POR EDAD 338
TABLA 60. VÍCTIMA DE RUMORES POR EDAD 339
TABLA 61. ESTADÍSTICOS DE CONTRASTE. VÍCTIMA RUMORES POR EDAD 339
TABLA 62. VÍCTIMA DE CONTACTO REPETIDO POR EDAD 340
TABLA 63. ESTADÍSTICOS DE CONTRASTE. VÍCTIMA INSULTOS POR EDAD 341
TABLA 64. VÍCTIMA DE MARGINACIÓN POR EDAD 342
TABLA 65. ESTADÍSTICOS DE CONTRASTE. VÍCTIMA INSULTOS POR EDAD 343
TABLA 66. COMPARACIÓN ENTRE CIBERVICTIMIZACIÓN POR INSULTOS Y LAS VARIABLES INDEPENDIENTES 345
TABLA 67. COMPARACIÓN ENTRE CIBERVICTIMIZACIÓN POR RUMORES Y LAS VARIABLES INDEPENDIENTES 347
TABLA 68. COMPARACIÓN ENTRE CIBERVICTIMIZACIÓN POR CONTACTO REPETIDO NO DESEADO Y LAS VARIABLES INDEPENDIENTES 349
TABLA 69. COMPARACIÓN ENTRE CIBERVICTIMIZACIÓN POR MARGINAR Y LAS VARIABLES INDEPENDIENTES 350
TABLA 70. COMPARACIÓN DE LAS PUNTUACIONES DE LAS VARIABLES INDEPENDIENTES POR SEXO 352

TABLA 71. COMPARACIÓN DE LAS PUNTUACIONES DE LAS VARIABLES INDEPENDIENTES POR GRUPOS DE EDAD....357
TABLA 72. DISTRIBUCIÓN DEL USO DE LAS TIC POR SEXO Y EDAD....360
TABLA 73. CORRELACIONES ENTRE LAS COMPONENTE PRINCIPALES....364
TABLA 74. DIVISIÓN DE LA MUESTRA PARA LA CONSTRUCCIÓN DE LA RED....370
TABLA 75. RESUMEN DEL MODELO....376
TABLA 76. CLASIFICACIÓN....377
TABLA 77. ÁREA DEBAJO DE LA CURVA....379
TABLA 78. IMPORTANCIA DE LAS VARIABLES INDEPENDIENTES....381
TABLA 79. ESTIMACIÓN DE LOS PARÁMETROS....383

Anexo I. Encuesta

DIPUTACIÓN DE ALICANTE

CRÍMINA
Centro para el estudio y prevención de la delincuencia

UNIVERSITAS Miguel Hernández

1.INTRODUCCIÓN

1. Eres un:(*)

☐ Chico
☐ Chica

2. ¿Qué edad tienes?(*)

12	13	14	15	16	17	18	19	20	+20 años
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

3. ¿En qué instituto/colegio estudias?(*)

☐

4. ¿En qué cursos estás?(*)

☐ 1º E.S.O
☐ 2º E.S.O
☐ 3º E.S.O
☐ 4º E.S.O
☐ 1º BACH
☐ 2º BACH

5. Entre semana, ¿cuántas horas aproximadamente pasas al día solo (sin tus padres) en casa?(*)

0	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

6. Y los fines de semana, ¿cuántas horas aproximadamente pasa al día solo (sin tus padres) en casa?(*)

0	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

7. ¿Cuántos hermanos tienes que vivan en casa?(*)

0	1	2	3	4	5	Más de 5 hermanos
☐	☐	☐	☐	☐	☐	☐

8. ¿Qué tipo de ordenador con conexión a Internet tienes? (Debes responder a las 3 opciones)(*)

	SI	NO
Portátil	☐	☐
Ordenador de mesa	☐	☐
Tablet	☐	☐

9. ¿Tienes habitación propia (no compartida)?(*)

☐ SI
☐ NO

10. ¿Compartes el ordenador/Tablet con otras personas? (Puedes responder a más de una opción)(*)

☐ Con nadie
☐ Con mis padres
☐ Con mis hermanos
☐ Otros familiares
☐ Otras personas. ¿Quién?

11. ¿Tienes móvil con acceso a Internet?(*)

☐ SI
☐ NO

12. ¿Tienes tarifa de datos en tu móvil? (cuando te puedes conectar a internet con el móvil a todas horas, sin wifi)(*)

☐ SI
☐ NO

13. ¿Pagas tú los recibos del móvil?(*)

☐ SI
☐ NO

14. ¿Utilizas el móvil en horario de clase?(*)

☐ SI
☐ NO

15. ¿Para qué usas el móvil? (Puedes responder más de una opción)(*)

☐ Para conocer personas nuevas
☐ Para jugar por Internet
☐ Para cotillear
☐ Para organizar fiestas/actividades
☐ Para quedar con los amigos
☐ Para estar en contacto con mis amigos
☐ Para ligar
☐ Para entretenerme

16. ¿Desde dónde accedes a Internet con el ordenador/Tablet? (Puedes responder más de una opción)(*)

☐ Nunca me he conectado a Internet
☐ Desde mi casa
☐ Desde la escuela
☐ Desde cibercafés
☐ Desde casa de amigos
☐ En otro lugar. ¿Cuál?

17. ¿Cuántas horas a la semana pasas navegando con el ordenador/Tablet por Internet aproximadamente?(*)

☐ Menos de 1 hora
☐ De 1 a 3 horas
☐ De 4 a 6 horas
☐ De 7 a 9 horas
☐ 10 horas o más

18. ¿Cuántas horas al día pasas hablando por WhatsApp o Line?(*)

☐ Ninguna, no tengo ni WhatsApp ni Line
☐ Menos de 1 hora
☐ De 1 a 3 horas
☐ De 4 a 6 horas
☐ De 7 a 9 horas
☐ 10 horas o más

19. ¿Tienes grupos cerrados a los que no pueden acceder otras personas?(*)

SI	NO
☐	☐

20. ¿Cuántas horas al día pasas navegando por Internet aproximadamente desde el móvil?(*)

☐ Menos de 1 hora
☐ De 1 a 3 horas
☐ De 4 a 6 horas
☐ De 7 a 9 horas
☐ 10 horas o más

21. ¿Alguien controla cuántas horas usas el ordenador/móvil para acceder a Internet? (Debes responder a las 2 opciones)(*)

	SI	NO
Ordenador/tablet	☐	☐
Móvil	☐	☐

22. ¿Alguien controla lo que haces en Internet? (Debes responder a las 2 opciones)(*)

	SI	NO
Ordenador/Tablet	☐	☐
Móvil	☐	☐

23. ¿Sabes si en tu ordenador hay instalados sistemas de control parental?(*)

SI ☐ NO ☐

24. ¿En algún momento de tu vida alguien te ha insultado o ridiculizado repetidamente a través de Internet o del móvil?(*)

SI ☐ NO ☐

25. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

☐ No lo sé
☐ Uno o varios compañeros de clase
☐ Uno o varios compañeros de otras clases
☐ Conocidos ajenos al colegio
☐ Desconocidos
☐ Mi novio/a o exnovio/a

26. ¿En algún momento de tu vida alguien ha contado rumores o mentiras sobre ti de forma repetida para hacerte daño a través de Internet o del móvil?(*)

SI ☐ NO ☐

27. ¿Quién te lo hizo? (Puedes responder más de una opción)(*)

☐ No lo sé
☐ Uno o varios compañeros de clase
☐ Uno o varios compañeros de otras clases
☐ Conocidos ajenos al colegio
☐ Desconocidos
☐ Mi novio/a o exnovio/a

28. ¿Han publicado alguna vez fotos o vídeos tuyos de carácter íntimo o privado sin tu consentimiento a través de Internet o del móvil?(*)

SI ☐ NO ☐

29. ¿Cuántas veces te ha ocurrido?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ Más de 10 veces ☐

30. ¿Quién te lo hizo? (Puedes responder más de una opción)(*)

☐ No lo sé
☐ Uno o varios compañeros de clase
☐ Uno o varios compañeros de otras clases
☐ Conocidos ajenos al colegio
☐ Desconocidos
☐ Mi novio/a o exnovio/a

31. ¿Alguna vez han difundido información secreta o íntima sin tu consentimiento a través de Internet o del móvil?(*)

SI ☐ NO ☐

32. ¿Cuántas veces te ha ocurrido?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ Más de 10 veces ☐

33. ¿Quién te lo hizo? (Puedes responder más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a

34. ¿Alguien ha accedido sin tu consentimiento al contenido de tu correo electrónico, WhatsApp, redes sociales, etc.?(*)

SI ☐ NO ☐

35. ¿Cuántas veces te ha ocurrido?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ Más de 10 veces ☐

36. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a
- ☐ Mis padres
- ☐ Otro (por favor, especifique)

37. ¿En algún momento de tu vida alguien ha utilizado Internet o el móvil para marginarte o excluirte de manera continuada?(*)

SI ☐ NO ☐

38. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a

39. ¿Te han amenazado a través de Internet o el móvil?(*)

SI ☐ NO ☐

40. ¿Cuántas veces te ha ocurrido?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ Más de 10 veces ☐

41. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a

42. ¿Te han obligado con violencia o intimidación a hacer algo que no querías a través de Internet o el móvil?(*)

SI ☐ NO ☐

43. ¿Cuántas veces te ha ocurrido?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ Más de 10 veces ☐

44. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a

45. ¿Se han hecho pasar por ti para dañarte en Internet o el móvil?(*)

SI ☐ NO ☐

46. ¿Cuántas veces te ha ocurrido?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ Más de 10 veces ☐

47. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a

48. ¿En algún momento de tu vida alguien ha contactado contigo repetidamente a través de Internet o el móvil tras haberle pedido que no lo hiciera?(*)

SI ☐ NO ☐

49. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a

50. ¿Alguna vez has sido acosado repetidamente con mensajes de carácter sexual a través de Internet o el móvil?(*)

SI ☐ NO ☐

51. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

- ☐ No lo sé
- ☐ Uno o varios compañeros de clase
- ☐ Uno o varios compañeros de otras clases
- ☐ Conocidos ajenos al colegio
- ☐ Desconocidos
- ☐ Mi novio/a o exnovio/a

52. ¿Alguna vez te has sentido obligado a realizar comportamientos de tipo sexual a través de webcam o videollamada?(*)

SI ☐ NO ☐

53. ¿Cuántas veces te ha ocurrido?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ Más de 10 veces ☐

54. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

☐ No lo sé
☐ Uno o varios compañeros de clase
☐ Uno o varios compañeros de otras clases
☐ Conocidos ajenos al colegio
☐ Desconocidos
☐ Mi novio/a o exnovio/a

55. ¿Alguna vez te han obligado a enviar fotos tuyas con contenido sexual a través de Internet o el móvil?(*)

SI	NO
☐	☐

56. ¿Cuántas veces te ha ocurrido?(*)

1	2	3	4	5	6	7	8	9	10	Más de 10 veces
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

57. ¿Quién te lo hizo? (Puedes responder a más de una opción)(*)

☐ No lo sé
☐ Uno o varios compañeros de clase
☐ Uno o varios compañeros de otras clases
☐ Conocidos ajenos al colegio
☐ Desconocidos
☐ Mi novio/a o exnovio/a

58. ¿Tu novio/a o exnovio/a ha intentado controlarte pidiéndote que retiraras fotos o comentarios de tus redes sociales, WhatsApp, Line, etc.?(*)

SI	NO
☐	☐

59. ¿Cuántas veces te ha ocurrido?(*)

1	2	3	4	5	6	7	8	9	10	Más de 10 veces
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

60. ¿Tu novio/a o exnovio/a ha intentado controlarte pidiéndote que no agregaras o que eliminaras a personas de tus redes sociales, WhatsApp, Line, etc.?(*)

SI	NO
☐	☐

61. ¿Cuántas veces te ha ocurrido?(*)

1	2	3	4	5	6	7	8	9	10	Más de 10 veces
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

62. ¿Tu novio/a o exnovio/a ha intentado influir en la información, el estado, el tablón o las fotos que publicas en las redes sociales, WhatsApp, Line, etc.?(*)

SI	NO
☐	☐

63. ¿Cuántas veces te ha ocurrido?(*)

1	2	3	4	5	6	7	8	9	10	Más de 10 veces
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

64. ¿Usas correo electrónico?(*)

SI	NO
☐	☐

65. ¿Cuántas horas a la semana dedicas a leer el correo electrónico?(*)

- ☐ Menos de 1 hora
- ☐ De 1 a 3 horas
- ☐ De 4 a 7 horas
- ☐ De 8 a 15 horas
- ☐ Más de 15 horas

66. ¿Cuántos correos recibes aproximadamente al día?(*)

- ☐ Ninguno
- ☐ De 1 a 3 correos
- ☐ De 4 a 7 correos
- ☐ De 8 a 15 correos
- ☐ De 15 a 30 correos
- ☐ Más de 30 correos

67. ¿Cuántos correos enviados por desconocidos recibes aproximadamente a la semana?(*)

- ☐ Ninguno
- ☐ De 1 a 3 correos
- ☐ De 4 a 7 correos
- ☐ De 8 a 15 correos
- ☐ De 15 a 30 correos
- ☐ Más de 30 correos

68. ¿Has recibido alguna vez algún correo proponiéndote algún tipo de favor o negocio económico del que sospechabas que era falso?(*)

- ☐ NO
- ☐ SÍ

69. ¿Cuántos correos de este tipo dirías que recibes aproximadamente a la semana?(*)

- ☐ De 1 a 3 correos
- ☐ De 4 a 7 correos
- ☐ De 8 a 15 correos
- ☐ De 15 a 30 correos
- ☐ Más de 30 correos

70. ¿Has recibido alguna vez algún correo del que sospechabas que la identidad de quien lo enviaba era falsa?(*)

☐ NO
☐ SÍ

71. ¿Cuántos correos de este tipo dirías que recibes aproximadamente a la semana?(*)

☐ De 1 a 3 correos
☐ De 4 a 7 correos
☐ De 8 a 15 correos
☐ De 15 a 30 correos
☐ Más de 30 correos

72. ¿Alguna vez has comprado algo a través del móvil?(*)

SI	NO
☐	☐

73. ¿Qué has comprado por el móvil? (Puedes responder a más de una opción)(*)

☐ Aplicaciones de juegos
☐ Otras aplicaciones
☐ Música
☐ Entradas
☐ Billetes de avión/tren/autobús
☐ Otros: ¿cuál?

74. ¿Alguna vez has comprado algo por Internet?(*)

☐ SI
☐ NO

75. ¿Qué has comprado por Internet? (Puedes responder a más de una opción)(*)

☐ Ropa
☐ Billetes de avión/tren/autobús
☐ Música
☐ Libros
☐ Entradas
☐ Películas
☐ Juegos
☐ Otros: ¿cuál?

76. ¿Y alguna vez te han estafado en alguna compra?(*)

Nunca	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

77. ¿En los ordenadores que usas tienes instalados antivirus?(*)

SI ☐ NO ☐ No sé lo que es un antivirus ☐

78. ¿El antivirus te ha avisado alguna vez de que tenías algún virus?(*)

Nunca ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

79. ¿Has perdido información o sufrido daños a causa de un virus informático?(*)

Nunca ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

80. ¿Cuántas horas a la semana dedicas aproximadamente a chatear por el ordenador/Tablet?(*)

- ☐ Nunca chateo
- ☐ Menos de 1 hora
- ☐ De 1 a 3 horas
- ☐ De 4 a 7 horas
- ☐ De 8 a 15 horas
- ☐ Más de 15 horas

81. ¿Cuántas horas al día dedicas aproximadamente a las redes sociales como Tuenti, Instagram, Facebook, Twitter u otros? (*)

- ☐ Ninguna, no uso redes sociales
- ☐ Menos de 1 hora
- ☐ De 1 a 3 horas
- ☐ De 4 a 7 horas
- ☐ De 8 a 15 horas
- ☐ Más de 15 horas

82. ¿Cuántas cuentas has abierto usando datos personales reales?(*)

Ninguna ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

83. ¿Para qué usas las redes sociales? (Puedes responder a más de una opción)(*)

- ☐ Para conocer personas nuevas
- ☐ Para jugar por Internet
- ☐ Para cotillear
- ☐ Para organizar fiestas/actividades
- ☐ Para quedar con los amigos
- ☐ Para estar en contacto con mis amigos
- ☐ Para ligar
- ☐ Para entretenerme
- ☐ Para seguir a mis ídolos (cantantes, actores...)

84. ¿Qué tipo de personas agregas a tus redes sociales? (Puedes responder a más de una opción)(*)

- ☐ Compañeros de clase
- ☐ Compañeros de otras clases
- ☐ Compañeros actividades extraescolares
- ☐ Amigos de otros amigos
- ☐ Hermanos
- ☐ Padres
- ☐ Otros familiares
- ☐ Desconocidos

85. ¿Limitas el acceso a tus cuentas en redes sociales? (Sólo los contactos que tienes agregados pueden ver tu información)(*)

SI	NO
☐	☐

86. ¿Tus padres saben que tienes cuentas en redes sociales?(*)

SI	NO
☐	☐

87. Dinos en cuál de las siguientes redes sociales tienes cuenta: (Puedes responder a más de una opción)(*)

- ☐ WhatsApp
- ☐ Line
- ☐ Facebook
- ☐ Tuenti
- ☐ Twitter
- ☐ Google +
- ☐ Instagram
- ☐ Badoo
- ☐ Otra

88. Y, ¿cuál de todas ellas las usas de forma habitual (más de una vez a la semana)? (Puedes responder a más de una opción) (*)

- ☐ WhatsApp
- ☐ Line
- ☐ Facebook
- ☐ Tuenti
- ☐ Twitter
- ☐ Google +
- ☐ Instagram
- ☐ Badoo
- ☐ Otra

89. ¿Tienes un blog propio?(*)

SI	NO
☐	☐

90. ¿A qué dedicas tu blog? (Puedes responder a más de una opción)(*)

- ☐ Lo uso como diario
- ☐ Para dar mi opinión sobre temas sociales
- ☐ Para hablar de mis hobbies como música, cine, moda, deporte...
- ☐ Otros

91. ¿Cuántas horas a la semana dedicas a hablar en tu blog?(*)

- ☐ Menos de 1 hora
- ☐ De 1 a 3 horas
- ☐ De 4 a 7 horas
- ☐ De 8 a 15 horas
- ☐ Más de 15 horas

92. ¿Escribes comentarios en foros o blogs ajenos?(*)

- ☐ SI
- ☐ NO

93. ¿Para qué escribes en foros o blogs ajenos?(Puedes responder a más de una opción)(*)

- ☐ Para dar mi opinión sobre temas sociales o políticos
- ☐ Para dar mi opinión sobre mis hobbies (música, cine, deporte, moda, etc.)
- ☐ Para criticar las opiniones de los demás
- ☐ Para ligar
- ☐ Otros

94. Cuando participas en foros ajenos, ¿cómo publicas los comentarios? (Debes responder a las 4 opciones)(*)

	Nunca	Pocas veces	Muchas veces	Siempre
Anónimo	☐	☐	☐	☐
Con un Nick	☐	☐	☐	☐
Con tu nombre verdadero	☐	☐	☐	☐
Con un nombre falso	☐	☐	☐	☐

95. ¿Usas tus cuentas de correo propias para escribir en los foros o blogs ajenos?(*)

SI	NO
☐	☐

96. ¿Cuántas horas a la semana dedicas a hacer videoconferencias o videollamadas?(*)

- ☐ Ninguna
- ☐ Menos de 1 hora
- ☐ De 1 a 3 horas
- ☐ De 4 a 7 horas
- ☐ De 8 a 15 horas
- ☐ Más de 15 horas

97. ¿Para qué utilizas las videollamadas? (Puedes responder a más de una opción)(*)

- ☐ Para hablar con los amigos
- ☐ Para hablar con los compañeros del colegio
- ☐ Para hablar con mi novio/a
- ☐ Para hablar con gente que acabo de conocer
- ☐ Para hablar con desconocidos
- ☐ Para hablar con familiares
- ☐ Otros

98. ¿Cuántas horas a la semana dedicas a usar webs de contacto como Badoo o Meetic?(*)

- ☐ Ninguna
- ☐ Menos de 1 hora
- ☐ De 1 a 3 horas
- ☐ De 4 a 7 horas
- ☐ De 8 a 15 horas
- ☐ Más de 15 horas

99. ¿Cuántas cuentas en webs de contacto has abierto usando datos personales reales?(*)

Ninguna	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

100. ¿Cuántas horas a la semana pasas jugando a videojuegos online con el ordenador, el móvil o la consola? (Debes responder a las 3 opciones)(*)

	Ninguna hora	**Menos de 1 hora**	**De 1 a 3 horas**	**De 4 a 7 horas**	**De 8 a 15 horas**	**Más de 15 horas**
Ordenador	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐
Consola	☐	☐	☐	☐	☐	☐

101. ¿Utilizas los videojuegos para hablar (chatear) con otros jugadores?(*)

SI	NO
☐	☐

102. ¿Alguna vez has dado tus datos reales a alguien a través de Internet?(*)

- ☐ NO
- ☐ SI

103. ¿Cuáles? (Puedes responder más de una opción)(*)

- ☐ Nombre
- ☐ Apellidos
- ☐ Teléfono
- ☐ Fotos mías
- ☐ Correo electrónico
- ☐ Colegio
- ☐ Ubicación desde la que hablas
- ☐ Número de tarjeta
- ☐ Dirección
- ☐ Edad
- ☐ Estado civil

104. ¿A través de qué medio? (Puedes responder a más de una opción)(*)

- ☐ Correo electrónico
- ☐ Mensajería instantánea (WhatsApp, Line,...)
- ☐ Salas de chat
- ☐ Redes sociales (Instagra, Facebook,...)
- ☐ Foros
- ☐ Webs de contacto
- ☐ Páginas de videojuegos
- ☐ Contraseñas
- ☐ Otro

105. ¿Cuántas veces has contactado con desconocidos a través de Internet?(*)

Nunca	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

106. ¿Qué tipo de contacto? (puedes responder a más de una opción)(*)

- ☐ Para mantener una amistad
- ☐ Relación esporádica
- ☐ Relación sentimental
- ☐ Para jugar online
- ☐ Otros

107. ¿A través de qué medio? (Puedes responder a más de una opción)(*)

- ☐ Correo electrónico
- ☐ Mensajería instantánea
- ☐ Salas de chat
- ☐ Redes sociales
- ☐ Foros
- ☐ Webs de contacto
- ☐ Páginas de videojuegos
- ☐ Otro

108. ¿Alguna vez has abierto o descargado enlaces o archivos enviados por desconocidos?(*)

Nunca ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

109. ¿A través de qué medio te los envían? (Puedes responder a más de una opción)(*)

- ☐ Correo electrónico
- ☐ Mensajería instantánea
- ☐ Salas de chat
- ☐ Redes sociales
- ☐ Foros
- ☐ Webs de contacto
- ☐ Páginas de videojuegos
- ☐ Otro (por favor, especifique)

110. ¿Descargas archivos a través de Internet?(juegos, programas, documentos, música, fotos, películas, aplicaciones...)(*)

SI ☐ NO ☐

111. ¿Cuántos archivos dirías que te descargas a la semana?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

112. ¿A través de qué medio te descargas los archivos? (puedes responder a más de una opción)(*)

- ☐ Programas como el Jdownloader, Pandos, Emule, Torrent, Ares, etc
- ☐ Páginas web como mega, seriespepito, desdeunlugarmejor.com, rapidshare o file share
- ☐ Otro (por favor, especifique)

113. ¿Qué tipo de archivos te descargas? (Puedes responder a más de una opción)(*)

- ☐ Juegos
- ☐ Programas informáticos (software)
- ☐ Pornografía
- ☐ Música
- ☐ Películas/series de televisión
- ☐ Aplicaciones para el móvil o Tablet
- ☐ Otro (por favor, especifique)

114. ¿Alguna vez te has hecho una foto comprometida (íntima) y se la has enviado a alguien a través del móvil o Internet?(*)

Nunca ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

115. ¿A quién se la has enviado? (puedes responder a más de una opción)(*)

- ☐ A tu novio/a o exnovio/a
- ☐ A personas conocidas a través de Internet
- ☐ A amigos/as
- ☐ A desconocidos
- ☐ Otro (por favor, especifique)

116. ¿Alguna vez te has hecho un vídeo comprometido (íntimo) y se lo has enviado a alguien a través del móvil o Internet?(*)

Nunca	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

117. ¿A quién se lo has enviado? (puedes responder varias opciones)(*)

- ☐ A tu novio/a o exnovio/a
- ☐ A personas conocidas a través de Internet
- ☐ A amigos/as
- ☐ A desconocidos
- ☐ Otro (por favor, especifique)

118. ¿Has mantenido conversaciones eróticas de forma voluntaria a través de Internet o el móvil?(*)

Nunca	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

119. ¿Con quién has mantenido las conversaciones? (puedes responder más de una opción)(*)

- ☐ Con tu novio/a o exnovio/a
- ☐ Con personas conocidas a través de Internet
- ☐ Con amigos/as
- ☐ Con desconocidos
- ☐ Otro (por favor, especifique)

120. ¿En el ordenador/Tablet con el que te conectas a Internet guardas alguna de estas cosas? (en caso afirmativo puedes responder a más de una opción)(*)

- ☐ Ninguna
- ☐ Un archivo con contraseñas
- ☐ Fotos personales
- ☐ Fotos íntimas
- ☐ Vídeos personales
- ☐ Información personal/íntima

121. ¿Y en el teléfono móvil? (en caso afirmativo puedes responder a más de una opción)(*)

- ☐ Ninguna
- ☐ Un archivo con contraseñas
- ☐ Fotos personales
- ☐ Fotos íntimas
- ☐ Vídeos personales
- ☐ Información personal/íntima

122. ¿Usas software (programas) piratas?(*)

SI ☐ NO ☐

123. ¿Cuántos programas de los que usas son piratas?(*)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

124. ¿Usas la misma contraseña para todo?(*)

SI ☐ NO ☐

125. ¿Cuántas veces al año cambias tus contraseñas?(*)

Nunca ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

126. ¿Alguna vez has dado tu contraseña por Internet o el móvil?(*)

Nunca ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ +10 ☐

127. ¿Cuántas horas a la semana dedicas aproximadamente a realizar actividades extraescolares regladas? (entrenamiento deportivo, idiomas, clases de apoyo/refuerzo, música,...)(*)

- ☐ Ninguna
- ☐ Menos de 1 hora
- ☐ De 1 a 3 horas
- ☐ De 4 a 7 horas
- ☐ De 8 a 15 horas
- ☐ Más de 15 horas

24.CONDUCTAS

128. ¿Alguna vez has insultado o ridiculizado a alguien de forma repetida a través de Internet? (Si tu respuesta es sí, puedes responder a más de una opción)(*)

- ☐ No, a nadie
- ☐ Sí, a uno o varios compañeros de clase
- ☐ Sí, a uno o varios compañeros de otras clases
- ☐ Sí, a conocidos ajenos al colegio
- ☐ Sí, a desconocidos
- ☐ Sí, a mi novio/a o exnovio/a

129. ¿Y a través del teléfono móvil?
(si la respuesta es sí, puedes responder a más de una opción)
(*)

☐ No, a nadie
☐ Sí, a uno o varios compañeros de clase
☐ Sí, a uno o varios compañeros de otras clases
☐ Sí, a conocidos ajenos al colegio
☐ Sí, a desconocidos
☐ Sí, a mi novio/a o exnovio/a

130. ¿Alguna vez has contado rumores o mentiras sobre alguien de forma repetida para hacerle daño a través de Internet?
(si la respuesta es sí, puedes responder a más de una opción)
(*)

☐ No, sobre nadie
☐ Sí, sobre uno o varios compañeros de clase
☐ Sí, sobre uno o varios compañeros de otras clases
☐ Sí, sobre conocidos ajenos al colegio
☐ Sí, sobre desconocidos
☐ Sí, sobre mi novio/a o exnovio/a

131. ¿Y a través del teléfono móvil? (si la respuesta es sí, puedes responder a más de una opción)(*)

☐ No, de nadie
☐ Sí, de uno o varios compañeros de clase
☐ Sí, de uno o varios compañeros de otras clases
☐ Sí, de conocidos ajenos al colegio
☐ Sí, de desconocidos
☐ Sí, de mi novio/a o exnovio/a

132. ¿Has publicado alguna vez fotos o vídeos de carácter íntimo o privado de alguien sin su consentimiento a través de Internet o el móvil? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

133. ¿De quién es esa información que has publicado?
(puedes responder a más de una opción)
(*)

☐ De nadie
☐ De uno o varios compañeros de clase
☐ De uno o varios compañeros de otras clases
☐ De conocidos ajenos al colegio
☐ De desconocidos
☐ De mi novio/a o exnovio/a

134. ¿Alguna vez has difundido información secreta o íntima de alguien, sin su consentimiento a través de Internet o del móvil? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

135. ¿De quién es esa información que has difundido?
(puedes responder a más de una opción)
(*)

☐ De nadie
☐ De uno o varios compañeros de clase
☐ De uno o varios compañeros de otras clases
☐ De conocidos ajenos al colegio
☐ De desconocidos
☐ De mi novio/a o exnovio/a

136. ¿Has accedido alguna vez al contenido de correo electrónico, WhatsApp, redes sociales,..., de alguien sin su consentimiento? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

137. ¿De quién era el correo electrónico, WhatsApp, red social... al que has accedido sin permiso? (En caso afirmativo puedes señalar más de una opción)(*)

☐ No, nunca he accedido al de nadie
☐ Sí, al de uno o varios compañeros de clase
☐ Sí, al de uno o varios compañeros de otras clases
☐ Sí, al de conocidos ajenos al colegio
☐ Sí, al de desconocidos
☐ Sí, al de mi novio/a o exnovio/a

138. ¿Has utilizado Internet para marginar o excluir de manera continuada a alguien? (en caso afirmativo puedes responder a más de una opción)(*)

☐ No, nunca
☐ Sí, a uno o varios compañeros de clase
☐ Sí, a uno o varios compañeros de otras clases
☐ Sí, a conocidos ajenos al colegio
☐ Sí, a desconocidos
☐ Sí, a mi novio/a o exnovio/a

139. ¿Y a través del teléfono móvil? (en caso afirmativo puedes responder a más de una opción)(*)

- ☐ No, nunca
- ☐ Sí, a uno o varios compañeros de clase
- ☐ Sí, a uno o varios compañeros de otras clases
- ☐ Sí, a conocidos ajenos al colegio
- ☐ Sí, a desconocidos
- ☐ Sí, a mi novio/a o exnovio/a

140. ¿Has amenazado a través de Internet o el móvil a alguien? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

141. ¿A quién has amenazado? (en caso afirmativo puedes responder a más de una opción)(*)

- ☐ A nadie
- ☐ A uno o varios compañeros de clase
- ☐ A uno o varios compañeros de otras clases
- ☐ A conocidos ajenos al colegio
- ☐ A desconocidos
- ☐ A mi novio/a o exnovio/a

142. ¿Has obligado con violencia o intimidación a alguien a hacer algo que no quería a través de Internet o el móvil? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

143. ¿A quién has obligado? (en caso afirmativo puedes responder a más de una opción)(*)

- ☐ A nadie
- ☐ A uno o varios compañeros de clase
- ☐ A uno o varios compañeros de otras clases
- ☐ A conocidos ajenos al colegio
- ☐ A desconocidos
- ☐ A mi novio/a o exnovio/a

144. ¿Te has hecho pasar por alguien para dañarle por Internet o el móvil? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

145. ¿Por quién te has hecho pasar?
(en caso afirmativo puedes responder a más de una opción)
(*)

- ☐ Por nadie
- ☐ Por uno o varios compañeros de clase
- ☐ Por uno o varios compañeros de otras clases
- ☐ Por conocidos ajenos al colegio
- ☐ Por desconocidos
- ☐ Por mi novio/a o exnovio/a

146. ¿Has contactado con alguien de forma repetida a través de Internet tras haberte pedido que no lo hicieras?

- ☐ No, con nadie
- ☐ Sí, con uno o varios compañeros de clase
- ☐ Sí, con uno o varios compañeros de otras clases
- ☐ Sí, con conocidos ajenos al colegio
- ☐ Sí, con desconocidos
- ☐ Sí, con mi novio/a o exnovio/a

147. ¿Y a través del teléfono móvil?
(en caso afirmativo puedes responder a más de una opción)
(*)

- ☐ No, con nadie
- ☐ Sí, con uno o varios compañeros de clase
- ☐ Sí, con uno o varios compañeros de otras clases
- ☐ Sí, con conocidos ajenos al colegio
- ☐ Sí, con desconocidos
- ☐ Sí, con mi novio/a o exnovio/a

148. ¿Has acosado repetidamente a alguien con mensajes de carácter sexual a través de Internet o el móvil? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

149. ¿A quién has acosado? (en caso afirmativo puedes responder a más de una opción)(*)

- ☐ A nadie
- ☐ A uno o varios compañeros de clase
- ☐ A uno o varios compañeros de otras clases
- ☐ A conocidos ajenos al colegio
- ☐ A desconocidos
- ☐ A mi novio/a o exnovio/a

150. ¿Has obligado a alguien a realizar comportamientos de tipo sexual a través de webcam o videollamada? (debes responder a las 2 opciones)(*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

151. ¿A quién has obligado? (en caso afirmativo puedes responder a más de una opción)(*)

☐ A nadie
☐ A uno o varios compañeros de clase
☐ A uno o varios compañeros de otras clases
☐ A conocidos ajenos al colegio
☐ A desconocidos
☐ A mi novio/a o exnovio/a

152. ¿Has obligado a alguien a enviar fotos con contenido sexual a través de Internet o el móvil? (debes responder a las 2 opciones) (*)

	Nunca	1	2	3	4	5	6	7	8	9	10	+10
Internet	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Móvil	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

153. ¿A quién has obligado? (en caso afirmativo puedes responder a más de una opción)(*)

☐ A nadie
☐ A uno o varios compañeros de clase
☐ A uno o varios compañeros de otras clases
☐ A conocidos ajenos al colegio
☐ A desconocidos
☐ A mi novio/a o exnovio/a

154. ¿Has intentado alguna vez controlar a tu novio/a o exnovio/a pidiéndole que retirara fotos o comentarios de su redes sociales, WhatsApp, Line u otros?(*)

Nunca	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

155. ¿Has intentado controlar a tu novio/a o exnovio/a pidiéndole que no agregara a personas a sus redes sociales, WhatsApp, Line u otros?(*)

Nunca	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

156. ¿Has intentado controlar a tu novio/a o exnovio/a pidiéndole que eliminara a contactos de sus redes sociales, WhatsApp, Line u otros?(*)

Nunca	1	2	3	4	5	6	7	8	9	10	+10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐