PREVENCIÓN DE DELITOS A MENORES EN INTERNET: EL EXPERIMENTO DE OSTRAVA BASADO EN FACEBOOK[1]

FRANCESC REALES ARNÓ

Subinspector de la Policía de la Generalitat-Mossos d'Esquadra, licenciado en filología inglesa y criminología, master en criminología y diplomado en estudios avanzados del doctorado Sistema de Justicia Penal

El artículo presenta el desarrollo y los resultados del estudio que se realizó en la ciudad checa de Ostrava en marzo de 2011, que tenía como objetivo analizar la vulnerabilidad de los datos personales y de la intimidad de los usuarios de las redes sociales. Se quería mostrar la facilidad con qué se pueden conseguir datos personales de los usuarios y las pocas precauciones de éstos a la hora de protegerlas. Igualmente se presentan diversas iniciativas y estudios para analizar los fenómenos que afectan a menores en la red, como el *sexting*.[2] También se presenta la tarea del cuerpo de Mossos d'Esquadra en el fomento de un uso correcto de Internet entre la juventud. Los resultados muestran que es muy sencillo obtener datos personales de programas utilizados en redes sociales y que una parte de los usuarios no toma las prevenciones adecuadas a la hora de publicitar sus datos personales

This article introduces the development and results of a research project that was carried out in the Czech Republic city of Ostrava in March, 2011. The objective of this experiment was to analyze the vulnerability of personal data, the intimacy of social network users and to review the few preventative actions taken at the moment to protect them. Several initiatives and research projects that study phenomena that affect youngsters on the net are also presented, including what is known as sexting. There is also a summary of the work carried out by Catalonia's Mossos d'Esquadra Police Force related with promoting the safe use of the Internet among young people. The results obtained show that it is very easy to obtain personal data from the programs used by social networks and that some users do not take appropriate precautions when they post information on the Internet.

1. INTRODUCCIÓN

La irrupción del fenómeno de Internet, las tecnologías de la información y especialmente la rápida implantación de las denominadas redes sociales ha facilitado que los contactos con finalidades sexuales con menores sean más fáciles de

1. http://www.facebook.com

2. Anglicismo empleado para denominar este fenómeno emergente en a nuestra sociedad, también conocido como *sexteo.* Consiste en el envío, a través del teléfono móvil, de material erótico o sexual de alta o baja intensidad (fotos o vídeos), y que tienen como protagonistas a las mismas personas que lo envían (definición extraída de la página «Sexting, quan la diversió o la broma esdevé malson» del web Jove.cat > Espai Xarxa > Entre tu i jo de la Generalitat de Catalunya (www.jove.cat/), donde se puede ampliar información mediante los enlaces complementarios [consulta: 12 noviembre 2012]) [nota del ed.].

ocultar gracias al anonimato de la red. Estas conductas –encaminadas a ganarse la confianza de los menores con la finalidad de concertar encuentros para obtener satisfacción sexual– han recibido recientemente la consideración de delito castigado penalmente con la reforma del Código penal español,[3] por la cual se introduce un nuevo artículo (183 bis) en el que se tipifican las nuevas conductas del denominado *grooming*[4] y se prevén, además, penas agravadas cuando el acercamiento al menor se obtenga mediante coacción, intimidación o engaño.[5]

Por un lado nos encontramos con situaciones o comportamientos delictivos que utilizan la red como medio propiciatorio de la actividad criminal y, por otro lado, observamos en la actualidad otros fenómenos que utilizan las nuevas tecnologías como herramienta para llevar a cabo comportamientos que pueden interpretarse o dar lugar a reprobaciones penales, como el fenómeno del *sexting*. Entre las posibles definiciones de este fenómeno, utilizaré la que hace McLaughlin (2010, 11:4),[6] según el cual:

> […] engloba las conductas o prácticas entre adolescentes consistentes en la producción, por cualquier medio, de imágenes digitales en las cuales aparezcan menores, de manera desnuda o semidesnuda, y en su transmisión a otros menores, ya sea a través de telefonía móvil o correo electrónico, mediante su puesta a disposición de terceros a través de Internet.

Agustina (2010) también hace una exhaustiva aproximación a este fenómeno, del cual presenta la doble vertiente del infractor como víctima y como autor del hecho, y también cuál tendría que ser la respuesta penal al fenómeno.

Si hablamos de pornografía infantil, la irrupción de las nuevas tecnologías ha propiciado un cambio en el comportamiento de los individuos consumidores de este tipo de material. Estos han pasado de una furtiva y costosa compra de revistas y vídeos, a la capacidad de descargarse una gran variedad y cantidad de fotos, sin tener que hacer un gasto económico y en la privacidad de su domicilio. Esta facilidad representa en primer lugar un mínimo riesgo para estos individuos a la hora de conseguir su material; en segundo lugar, hace que consigan una gran cantidad y, en tercer lugar, genera una constante demanda de material nuevo y

3. Ley orgánica 5/2010, de 22 de junio, y su entrada en vigor el 23 de diciembre.

4. El *grooming* o, en español, ciberacoso a menores, es la conducta pedofílica desarrollada normalmente a través de Internet, con la cual un individuo, valiéndose de una identidad falsa, busca establecer una relación afectiva con un menor para obtener imágenes de contenido sexual o bien abusar sexualmente (fuente: TERMCAT Centre de Terminologia, en línea http://www.termcat.cat/ [consulta: 12 noviembre 2012]) [nota del ed.].

5. «El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que esta propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio si procede de las penas correspondientes a los delitos cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño».

6. Citado en Agustina, José R. (2010). Ver la referencia al final de este artículo.

reciente. Esta demanda constante significa que más y más menores sean víctimas de la producción de pornografía infantil (Taylor y Quayle, 2003).

En esta facilidad a la hora de producir material relacionado con la pornografía infantil, tiene mucho que ver la masiva irrupción de cámaras fotográficas y de vídeo digitales, lo que ha propiciado que la gente interesada en la visualización se haya podido convertir en productora.

Así, pues, hay que destacar la fuerza que está tomando la red como vehículo, no sólo para albergar o facilitar la comisión de hechos delictivos o conductas desviadas, sino como herramienta para difundir o llegar a una inmensa cantidad de personas, en un espacio de tiempo muy reducido, que hace que cualquier actividad desarrollada en la red o información, del tipo que sea y en el formato que sea, se convierta en pública de manera inmediata o casi inmediata, desde el momento que cualquiera decide incorporarla a la red o *World Wide Web*.

Por otro lado, hay otras conductas que pueden considerarse delictivas y que utilizan la web como medio de perpetración de los hechos; en este caso se puede hablar del ciberacoso (Jaishankar y Sankary 2005). El denominado ciberacosador no presenta una amenaza física para la víctima pero sigue su actividad en Internet para recopilar información y amenazarla o acosarla. El anonimato de la interacción en línea reduce la posibilidad de identificar al autor y hace que el acoso mediante la red sea mucho más común que el acoso físico. Según Bocij (2003), el ciberacoso consiste en:

> Un grupo de comportamientos en los cuales un individuo, un grupo de individuos o una organización usa las tecnologías de la información y de las comunicaciones para acosar a otro individuo, grupo de individuos u organización. Estos comportamientos pueden incluir, pero no se limitan a, la transmisión de amenazas y falsas acusaciones, daños a datos o equipos, el robo de identidad, el robo de datos, el acceso al ordenador, el contacto con menores para propósitos sexuales y cualquier forma de agresión. La fustigación es definida como un curso de acción en que una persona razonable, en la posesión de la misma información, pensaría que causa a otra persona razonable sufrir un trastorno emocional.

2. LA POLICÍA DE LA GENERALITAT-MOSSOS D'ESQUADRA Y LA PROTECCIÓN DE MENORES ANTE LOS DELITOS EN LA RED

En el año 2008 la Policía de la Generalitat-Mossos d'Esquadra[7] impulsó, dentro de su ámbito de prevención, el Plan de Acción Internet Segura[8] con el objetivo de proteger a los menores y prevenir la posible victimización de menores y adolescentes por delitos a través de la red. Este Plan se presentó, pues, para dar información,

7. Agradezco desde aquí los datos aportados por el Área de Oficina Técnica de la Comisaría General de Planificación y Organización de la Dirección General de la Policía del Departamento de Interior de la Generalitat.

8. Véase información completa y actualizada en la página web de los Mossos d'Esquadra <http://www20.gencat.cat/portal/site/mossos> dentro del apartado de Prevención > Internet segura.

consejos y pautas para mejorar la seguridad en el uso de la red, como por ejemplo mediante el fomento de la práctica segura de la actividad en las redes sociales como Messenger,[9] Tuenti,[10] o Facebook.

Este Plan no se ha circunscrito únicamente a los centres escolares –donde ha tenido una gran acogida por parte de la comunidad educativa– sino que también se ha introducido en otros puntos con acceso a Internet utilizados por la juventud, como locales juveniles o centros de recreo.

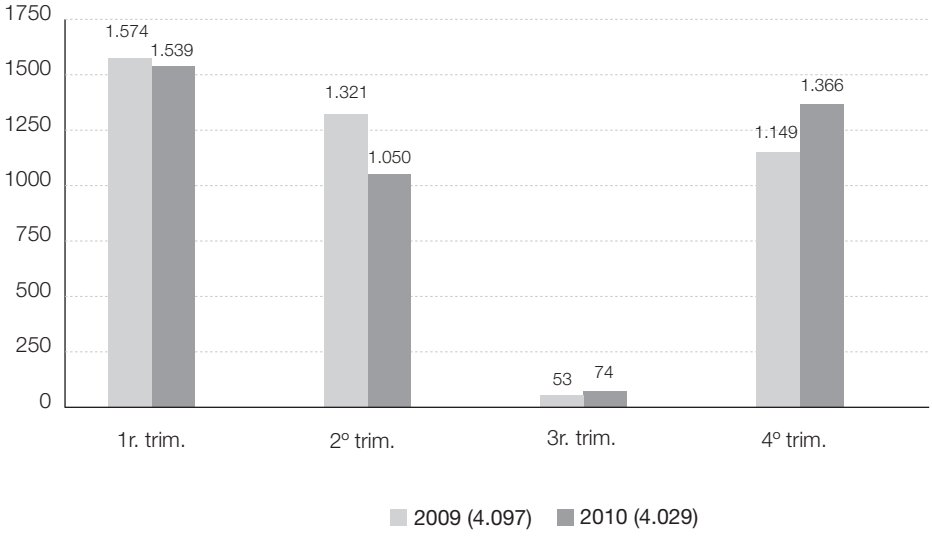
2.1 LAS PRESENTACIONES DEL PLAN DE ACCIÓN INTERNET SEGURA

En el primer año de implantación del Plan, el 2008, se realizaron un total de 1.228 presentaciones.

Seguidamente se presenta más desarrollada la labor llevada a cabo por el cuerpo de Mossos d'Esquadra durante el 2009 y el 2010, años en que el Plan ya está consolidado.

Durante el primer trimestre escolar de los años 2009 y 2010, la distribución de presentaciones es muy similar; se observa una ligera disminución en el segundo trimestre del año 2010 y una actividad mínima en el trimestre que comprende los meses de verano.

Figura 1. Presentaciones del Plan de Acción Internet Segura, años 2009 y 2010, distribuidas por trimestres



Fuente: Dirección General de la Policía de la Generalitat

9. http://windowslive.es.msn.com/messenger/

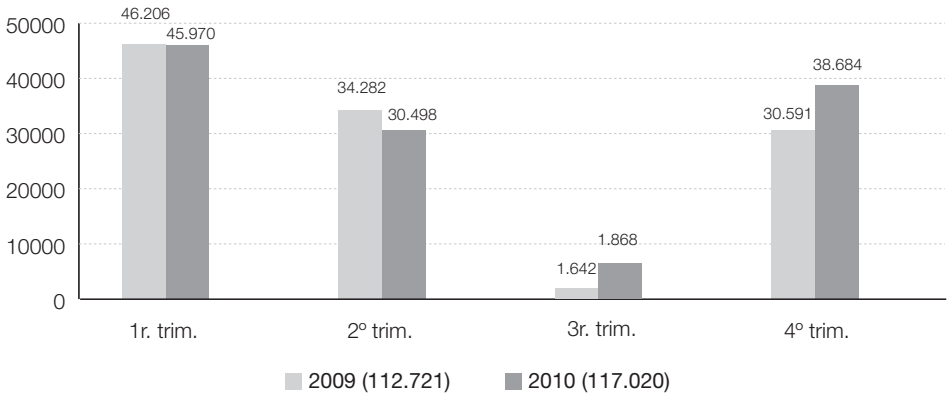
10. http://www.tuenti.com

Tabla 1. Número de presentaciones realizadas en el período 2008-2010

Año 2008	1.228
Año 2009	4.097
Año 2010	4.029
Total	**9.354**

La gráfica siguiente muestra el incremento en el número de asistentes en el total del año 2010 en comparación con el año 2009 y aún más si lo comparamos con los 34.138 asistentes del año 2008, del cual únicamente se puede contabilizar una parte ya que no coincidió la implantación del Plan con el año escolar.

Figura 2. Número de asistentes a las presentaciones del Plan de Acción Internet Segura, años 2009 y 2010, distribuidos por trimestres



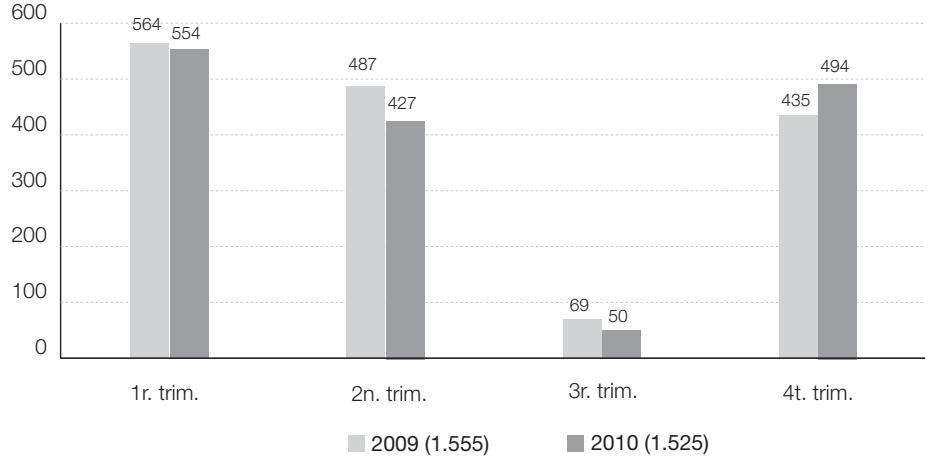
Fuente: Dirección General de la Policía de la Generalitat

Tabla 2. Número de asistentes a las presentaciones realizadas en el período 2008-2010

Año 2008	34.138
Año 2009	112.721
Año 2010	117.020
Total	**263.879**

Si analizamos los centros educativos colaboradores con el Plan de Acción de la Policía de la Generalitat-Mossos d'Esquadra, vemos que el 2008 participaron 405 centros. Ya durante los años 2009 y 2010, la distribución por trimestres del número de centros educativos colaboradores es la que se muestra en la figura siguiente:

Figura 3. Centros educativos colaboradores, años 2009 y 2010, distribuidos por trimestres



Fuente: Dirección General de la Policía de la Generalitat

Como se puede observar, des del primer año de la puesta en marcha del Plan, el número de centros dio un salto cuantitativo y llegaba a más de mil quinientos centros en los años 2009 y 2010.

Tabla 3. Número de centros educativos donde se han realizado presentaciones (período 2008-2010)

Año 2008	405
Año 2009	1.555
Año 2010	1.525
Total	**3.485**

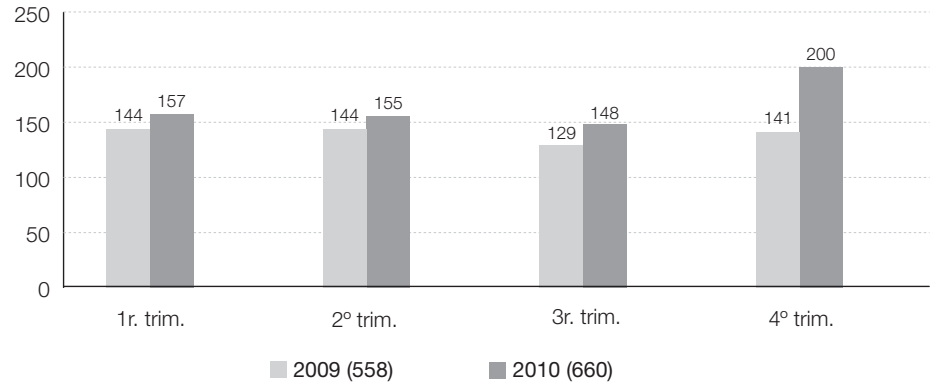
2.2 EL CORREO CORPORATIVO DEL PLAN DE ACCIÓN INTERNET SEGURA

El cuerpo de Mossos d'Esquadra configuró una dirección de correo electrónico[11] como un servicio de atención y consulta para las personas que crean que pueden ser víctimas de un delito o una falta relacionada con la navegación por Internet, en cualquiera de sus posibilidades, o para quien visualice alguna página de pornografía infantil.

11. La dirección electrónica es internetsegura@gencat.cat

La figura 4 recoge los datos sobre el número de correos gestionados por el cuerpo de Mossos d'Esquadra en relación a informaciones (pornografía infantil, estafas, consultas, etc.) facilitadas por la ciudadanía sobre Internet y nuevas tecnologías.

Figura 4. Gestión del correo internetsegura@gencat.cat, años 2009 y 2010 distribuidos por trimestres



Fuente: Dirección General de la Policía de la Generalitat (fecha de explotación: 20.01.2011)

En el gráfico se ve un aumento en el uso que hace la ciudadanía del correo para contactar con el Departamento de Interior de la Generalitat; este aumento es de un 18'27% respecto al año anterior.

3. EL EXPERIMENTO DE OSTRAVA BASADO EN FACEBOOK

Una de las redes sociales más populares utilizadas por los jóvenes es el Facebook y, por lo tanto, es una plataforma que puede atraer a personas que busquen víctimas potenciales de sus actividades delictivas.

Oficialmente el Facebook no permite inscribirse a menores de trece años pero, según la revista *Costumer Reports* en su edición de junio del 2011 en los Estados Unidos,[12] de los veinte millones de menores que activamente utilizaban Facebook en el último año, siete millones y medio –es decir, más de una tercera parte– eran menores de trece años. Este hecho vulnera las regulaciones de la Federal Children's Online Privacy Protection Act (Warmund 2000) del año 1998. Esta ley prohíbe a los sitios web mostrar conscientemente información personal identificable de menores o recoger datos personales de menores de trece años.

12. En línea en <http://www.consumerreports.org/cro/magazine-archive/2011/june/june-2011-toc.htm>.

Entre estos jóvenes usuarios, más de cinco millones tenían diez años o menos y sus cuentas eran mínimamente supervisadas por sus padres. Asimismo, el estudio mostraba que un millón de jóvenes fueron molestados, acosados o habían sido sometidos a otras formas de ciberacoso escolar[13] en la web, el año anterior.

En España, para acceder a Facebook, la empresa quería aplicar la legislación de los Estados Unidos, que permite el acceso a mayores de trece años, pero actualmente, a instancias de la Agencia de Protección de Datos, el acceso se permite a partir de los catorce años. Con edades inferiores, sólo pueden acceder con previo consentimiento paterno.

Como se ha comentado anteriormente, el uso de las redes sociales está a la orden del día y se ha convertido en uno de los medios de contacto entre los jóvenes alrededor del mundo, que no sólo se utiliza en momentos de ocio o con finalidad de intercambio de información sino que han sido utilizadas por movimientos con una intención política y de revolución social.

En un estudio reciente, Boshmaf *et al.* (2011) utilizan robots sociales[14] para captar amigos en Facebook. Estos investigadores crearon ciento dos robots sociales, cuarenta y nueve con un perfil masculino y cincuenta y tres con perfil femenino, los cuales enviaron veinticinco solicitudes de amistad por día a más de cinco mil usuarios reales de Facebook escogidos al azar. Los envíos de robots sociales de perfil masculino (dos mil trescientos noventa y uno) tuvieron una aceptación, en seis días, de un 15,9% (trescientos ochenta y uno) y los de perfil femenino (dos mil seiscientos sesenta y dos) tuvieron una aceptación de un 22,3% (quinientos noventa y cinco). Aproximadamente, el 86% de las aceptaciones de amistad fueron aceptadas en los primeros tres días. Únicamente fueron bloqueadas un 20% de solicitudes. El estudio duró ocho semanas y los investigadores consiguieron 250 Gb de datos personales de miles de usuarios.

Teniendo en cuenta esta posible vulnerabilidad en la red y, concretamente, la vulnerabilidad de los menores usuarios del programa Facebook, una organización informática checa y la ONG de protección de menores Nebud Obet, con la financiación del programa Life Long Learning de la Unión Europea, prepararon un experimento en la ciudad checa de Ostrava para analizar la vulnerabilidad de los jóvenes en la red y en Facebook.

4. EL TALLER INTERNET SAFETY

En este apartado resumiré el desarrollo y los resultados del trabajo de campo y el estudio empírico llevado a cabo durante el Taller Internet Safety que tuvo lugar

13. Concepto conocido en inglés como *cyberbullying,* Acoso escolar que se produce a través de Internet o utilizando otras tecnologías como el correo electrónico o los mensajes de texto de los teléfonos móviles (fuente: TERMCAT, en línea <http: www.termcat.cat/ [consulta: 12 noviembre 2012]) [nota del ed.].

14. Estos robots son programarios conocidos como *socialbots*.

en Ostrava (República Checa) entre los días 20 y 26 de marzo de 2011, en el marco del programa Life Long Learning de la Unión Europea.[15]

4.1 OBJETIVOS DEL TALLER

El objetivo principal del taller era comprobar la facilidad que hay para acceder a los datos de menores mediante la red. Se quería comprobar asimismo la vulnerabilidad de los datos que los menores «cuelgan» en la red y analizar los medios o estrategias que cualquiera puede utilizar para tener acceso a estos menores y a sus datos. Para llevar a cabo el estudio se utilizó el programa Facebook, que, como se ha dicho en el apartado anterior, es uno de los más utilizados entre los jóvenes para intercambiar información e interactuar entre ellos y sus familiares a través de la red, ya sea con el ordenador o con su teléfono móvil. Al mismo tiempo, se quería analizar la facilidad del acceso a los datos personales de menores mediante su perfil. Los datos a los cuales se quería tener acceso eran: teléfono, dirección, lugar de trabajo o estudio, fotos, vídeos... aparte de la dirección de correo electrónico.

Asimismo, el resultado del estudio tenía que servir para mostrar que fácil había sido conseguir los datos de un gran número de menores usuarios de esta red social y para concienciar a menores y familiares de la conveniencia de evitar la publicación de datos personales en la red. Este estudio, además, pretendía concienciar a los propios jóvenes participantes del proyecto de la necesidad de explicar los resultados a sus compañeros a través de la red.

Otro objetivo era atraer a un número de menores o jóvenes al hotel donde estábamos hospedados los participantes para comprobar si se había podido «engañar» a algún usuario con un perfil falso.

4.2 METODOLOGÍA

Para la realización de este trabajo empírico los organizadores invitaron a participar a quince investigadores de diversos países de la Unión Europea y que su campo de trabajo fuese la prevención de delitos en diferentes ámbitos. Por este motivo se seleccionaron profesionales del campo de la seguridad, ingenieros informáticos, psicólogos, educadores sociales, etc.

Al mismo tiempo, un grupo de treinta alumnos de un instituto de educación secundaria de la localidad de Ostrava realizaron el mismo trabajo de campo durante los mismos días que los investigadores europeos. A la mitad y al final del estudio se mantuvo contacto con los estudiantes.

Los medios empleados para hacer el estudio fueron ordenadores, programario (en concreto la red Facebook), proyectores y fichas de control.

15. Quiero agradecer la invitación para participar en el taller Internet Safety, por las organizaciones Rizika Internetu a Komunikačních Technologií y Nebud Obět (Don't be a victim!), esta última dedicada a la prevención de delitos mediante la red y en especial a la prevención de abusos a menores a través de este medio.

Previamente al inicio del estudio los padres y madres de los alumnos, ya que estos eran menores, dieron su autorización para que sus hijos participasen. Los organizadores también informaron a las autoridades policiales de la ciudad sobre el desarrollo de este experimento.

Las diversas fases del estudio fueron registradas en vídeo y de este experimento se ha hecho un documental que ha sido puesto a disposición de los usuarios en la red y repartido a organizaciones y escuelas del país organizador.

4.3 DESARROLLO

Cada uno de los participantes europeos hizo una presentación de los proyectos que realizan en su país de origen referentes a la prevención de delitos a través de Internet. La Policía de la Generalitat-Mossos d'Esquadra mostró en su presentación la tarea que lleva a cabo en los centros educativos a partir de la implantación, en el año 2008, del Plan de Acción Internet Segura para la protección del menor.[16]

Durante esta sesión de presentación se planteó el proyecto, se presentaron los objetivos de la investigación y se explicó la preparación previa que se llevó a cabo con las autoridades locales, familiares, profesorado, etc.

Se planteó la creación de perfiles falsos de Facebook para contactar con menores y llevar a cabo la recogida de datos personales. Cada participante era libre de seguir su propia estrategia con tal de contactar con los menores y emplear la información que desease en su perfil (vídeos, fotos, etc.).

4.4 CONSIDERACIONES ÉTICAS

Hay que destacar que, ya en el planteamiento del estudio, aparecieron opiniones de algunos participantes que discrepaban del carácter ético de este tipo de estudio: manifestaban que era reprobable hacer un estudio científico empírico utilizando el engaño y que la participación de un grupo de treinta estudiantes de secundaria podía comportar problemas psicológicos tanto a los propios participantes como a las víctimas del estudio, en el caso de que fuesen menores.

La participante psicóloga fue la que planteó más objeciones a la coparticipación de jóvenes estudiantes en el estudio. Después de un debate entre los participantes, la opinión de la mayoría fue que, si con el resultado del estudio se podía evitar la comisión de algún delito o concienciar a un gran número de jóvenes y hacerles ver qué fácil es ser víctima de un engaño a través de la red, el estudio valía la pena de llevarse a cabo. Se creyó que experimentos realistas con un riesgo mínimo son la única manera de analizar con fiabilidad la viabilidad de un ataque de estas características en el mundo real.

16. Con la presentación del Power-Point *Safe Internet Access,* elaborado por el cuerpo de Mossos d'Esquadra.

Esta postura es al parecer la opinión de otros investigadores que comparten este punto de vista, como Bilge *et al.* (2009) y Jagatic *et al.* (2007).[17]

4.5 PUESTA EN MARCHA

Con tal de crear un perfil falso de Facebook, en primer lugar, cada participante creó una nueva cuenta de correo electrónico anónima, a la cual se vinculó el perfil falso. La mayoría de participantes hizo esta operación en menos de veinte minutos; por otra parte, el grupo de estudiantes de secundaria ya habían comenzado a crear sus perfiles la semana anterior. La mayoría de los participantes crearon una identidad nueva, ligada a este perfil de Facebook, en el que se hacían pasar por jóvenes de entre quince y dieciocho años; para esta nueva identidad, incorporaron fotos descargadas de la web, para darle más veracidad. La creación de perfiles no fue homogénea en el sentido de que algunos participantes masculinos se hicieron pasar por chicos o por chicas en la red.

El idioma empleado en los perfiles fue el inglés ya que la totalidad de los participantes era de procedencia extranjera, por lo cual también se hubieron de inventar motivos lógicos para la estancia en el país y no levantar sospechas. Los estudiantes participantes utilizaban su lengua, el checo. Algún participante utilizó el mundo de la música o de los deportes para atraer a los jóvenes a un encuentro en la ciudad el último día del estudio.

La mayor dificultad a la hora de dar veracidad al perfil de Facebook era el hecho que se trataba de perfiles nuevos, con pocas amistades añadidas y con un historial corto. Para minimizar esta circunstancia se añadieron como amistades los mismos miembros del grupo investigador, entre ellos y con su perfil falso.

Apareció otro problema con el mismo programa Facebook, ya que bloqueó a algunos de los investigadores al hacer estos envíos masivos de solicitud de amistad. Una de las estrategias para poder «acceder» a nuevas amistades fue solicitarla a equipos juveniles de fútbol locales, clubs de fans de grupos musicales, etc. Para poder acceder a jóvenes de la ciudad se hizo un filtrado a través de Facebook con el nombre de la ciudad y así se acotó a los posibles objetivos.

Uno de los primeros hechos que destacaron los investigadores fue la rapidez –inmediatez, en algunos casos– a la hora de aceptar las solicitudes de amistad de los perfiles falsos de los diversos investigadores o de los estudiantes de secundaria participantes en el estudio.

Otro hecho destacable era la cantidad de datos personales que muchos menores tenían en su perfil de Facebook: la dirección de su domicilio, su número de teléfono, su lugar de trabajo o la clase y el centro educativo donde cursaban sus estudios. Por otro lado, también se tenía acceso a una gran cantidad de fotografías y vídeos donde aparecían los menores y sus amigos también menores en la red.

El objetivo de la fase de estudio era conseguir atraer, al hotel donde se alojaban los investigadores, a posibles víctimas o posibles autores de acoso u otros delitos

17. Ver las referencias completas al final del artículo.

contra la inmunidad sexual y concienciar a estas víctimas potenciales del riesgo que comporta acudir a encuentros con personas que no conocen.

Con tal de hacer venir jóvenes al hotel, cada investigador creó un «acontecimiento» en Facebook relacionado con la temática y las características que cada investigador configuró en «su» perfil; así pues, hubo investigadores que crearon acontecimientos como que un cantante conocido asistiría a firmar autógrafos durante una campaña de promoción o que asistiría un determinado jugador de fútbol famoso para promocionar algún producto, etc. Se ha de destacar que la estrategia establecida por la mayoría de los estudiantes participantes se basó en la proposición directa de un contacto de amistad o de invitar a conocerse personalmente después de unos días de diálogo mediante el Facebook con un contenido de marcado componente sexual. El hecho que el hotel fuese de gama alta hizo pensar que podía ser un obstáculo para dar veracidad a algunas estrategias o ser un factor positivo para otros. También había el peligro que los jóvenes que tuviesen añadidos a unos cuantos investigadores sospechasen de diversos actos en el mismo hotel o que se lo comentasen entre ellos.

La cuestión del idioma fue también un obstáculo para los investigadores ya que, en las conversaciones a través de Facebook con algunos jóvenes, se tenían que utilizar servicios de traducción como el Google Traductor,[18] programa que los jóvenes utilizaban con facilidad. Este obstáculo idiomático no lo tenían, en cambio, los participantes del centro educativo de Ostrava ya que interactuaban con su perfil falso y otros jóvenes, en su idioma nativo.

En la finalización de la cuarta sesión los resultados eran los siguientes:

Tabla 4. Resultados de los perfiles de Facebook creados al efecto de este taller

Solicitudes de amistad enviadas	2.403
Solicitudes de amistad confirmadas	1.592
Amistades canceladas	52
Número de encuentros planeados	34

4.6 FINALIZACIÓN DEL TALLER

El último día de la estancia en la ciudad fue el que proporcionó los resultados prácticos del estudio, como se ha comentado anteriormente; en este punto se analizó a las personas que acudieron a las diversas convocatorias de los participantes en el estudio. La mayor parte de los asistentes eren jóvenes que habían acudido para contactar con los «falsos amigos» que habían conocido en Facebook.

18. http://translate.google.com/

Cabe destacar la presencia de dos adultos que habían contactado con una de las investigadoras del proyecto y que, sorprendidos por las características del estudio, participaron en el desarrollo final y explicaron su visión de Facebook.

Igualmente hay que destacar la presencia de un adulto por los alrededores del hotel que había contactado con una estudiante del instituto de secundaria y que podía relacionarse su perfil con un sospechoso de conductas pedófilas: en primer lugar fue requerido para dar explicaciones por su presencia en el lugar y manifestó que había sido un error; asimismo un medio de comunicación local entrevistó a este individuo y él no quiso explicar ninguna de sus motivaciones para encontrarse en el lugar mencionado.

Por otro lado, se ha de remarcar la cantidad indeterminada pero numerosa de individuos que se aproximaron al hotel pero que finalmente no accedieron y que fueron controlados por miembros del grupo organizador.

A los menores que habían concurrido a la convocatoria, ya en el lugar, se les presentó material relacionado con los peligros en Internet y se hizo una charla informativa sobre el estudio realizado.

Al final del taller, y una vez analizadas las diversas observaciones, se dio por finalizado el experimento de Ostrava. Sobre todas las fases del experimento y sobre los resultados obtenidos se realizó y registró un vídeo documental,[19] que ya ha sido utilizado por las diversas ONG del país y por la comunidad educativa para realizar sus planes de prevención de delitos en Internet.

5. CONCLUSIONES

Este estudio ha puesto de manifiesto la facilidad para acceder a los datos personales de otros usuarios del programa Facebook, y concretamente de los menores. Los datos personales que se pueden obtener con facilidad y siempre desde el anonimato que proporciona un perfil de usuario falso son, entre otros: dirección del domicilio, teléfono, dirección electrónica, sitio donde se cursan estudios, lugar de trabajo, fotos, vídeos, etc.

Hay que concienciar mucho más a los menores a la hora de crear sus perfiles y de introducir la información que proporcionan en la red. Hay que hacerles entender que esta información puede ser fácilmente accesible, que se puede hacer mal uso y ponerse ellos mismos en peligro. Realmente hay una falta de concienciación a la hora de analizar la privacidad de sus datos: muchas veces la juventud acepta como amistades a otras personas de manera automática sin hacer un mínimo análisis.

Es necesaria una supervisión del padre, la madre o tutor/a de la actividad desarrollada por los jóvenes en la red y de la información que estos aportan o «cuelgan», ya sean datos personales o archivos gráficos como fotos y vídeos.

Las medidas de control de las empresas creadoras del programario utilizado en las redes sociales no aplican medidas de seguridad suficientemente eficaces

19. Accesible, por ejemplo, en la web de la ONG Nebud Obet <http://www.nebudobet.cz/?lang=en> [Consulta: octubre 2012].

a la hora de prevenir un mal uso, impedir el registro a menores de trece años –catorce años en España– o medidas poco eficaces como el bloqueo de solicitudes masivas de amistad.

La prevención de delitos a través de Internet que tienen menores como víctimas es una cuestión de gran interés a escala mundial; por eso, se han puesto en marcha iniciativas para intentar mejorar la prevención, como el experimento que se ha presentado en este artículo.

La Policía de la Generalitat-Mossos d'Esquadra es uno de los cuerpos policiales pioneros en la prevención de delitos en la red con programas como el Plan de Acción Internet Segura, que se presenta en los centros educativos, entre otros sitios. Esta tarea en otros países es llevada a cabo por el mismo profesorado de los centros u otros especialistas.

La aplicación de técnicas conducentes a la reducción de oportunidades englobadas en la prevención situacional del delito, como:

– incrementar el esfuerzo que debe llevar a cabo el infractor para cometer el delito;

– incrementar el riesgo que el infractor debe afrontar para cometer el delito, o

– reducir los beneficios o recompensas que el delincuente aspira conseguir con la consecución del delito,

puede llevar a disminuir los hechos delictivos en la red y al mismo tiempo reducir la victimización de menores en ese entorno.

Ejemplos de la aplicación de estas técnicas de prevención situacional dirigidas a modificar una situación con el fin de reducir las oportunidades de cometer delitos en el ámbito de Internet podrían ser:

a) controlar el acceso y uso de las redes sociales por parte de menores y, al mismo tiempo, establecer un lugar en la vivienda donde colocar el ordenador para facilitar su supervisión. De este modo dificultamos el acceso ilícito al menor y evitamos conversacions con personas inadecuadas, así como que los jóvenes asuman el rol de víctimas propiciatorias;

b) informar a los menores de la necesidad de no introducir en la red datos personales, fotos, direcciones, teléfonos, costumbres, ya que pueden ser utilizados para actos preparatorios de delitos;

c) evitar, en la red social donde se interviene, la participación de personas cuya identidad no se conoce con seguridad o sencillamente se desconoce.

Estas técnicas relacionadas con la prevención situacional del delito van encaminadas, como se ha dicho anteriormente, a reducir la recompensa, incrementar el riesgo del posible infractor a ser detectado e incrementar su esfuerzo para conseguir su finalidad delictiva. En definitiva, a evitar que en un entorno virtual, igual que se ha defendido que hay que evitarlo en un espacio físico, se puedan encontrar a un delincuente motivado con una víctima potencial con la absencia de un guardián eficaz (Cohen y Felson, 1979).

Con la implementación de estas medidas se pretende, pues, evitar la oportunidad de cometer el delito y en consecuencia la victimización de menores en el ámbito de las redes sociales.

6. REFERENCIAS

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* [en línea], núm. 12-11, p. 11:1-11:44.

BILGE, L. *et al.* (2009) «Proceedings of the 18th International Conference on World Wide Web - WWW '09; all Your Contacts are Belong to Us»: 551.

BOCIJ, P. (2003) «Victims of Cyberstalking: An Exploratory Study of Harassment Perpetrated Via the Internet.» *First Monday,* 8(10), 2004.

BOSHMAF, Y.; MUSLUKHOV, I.; BEZNOSOV, K. (2011) «The Socialbot Network: When Bots Socialize for Fame and Money». ACSAC, 11. Dec. 5-9, 2011. Orlando, Florida (EUA).

COHEN, L. E.; FELSON, M. (1979). «Social Change and Crime Rate Trends: A Routine Activity Approach.» *American Sociological Review* 44 (4):588-608.

JAGATIC, T. N. *et al.* (2007) «Social Phishing.» *Commun. ACM,* 50(10), p. 94-100.

JAISHANKAR, K.; SANKARY, V. U. (2005) «Cyber Stalking: A Global Menace in the Information Super Highway». *ERCES Online Quarterly Review*, 2(3).

MCLAUGHLIN, J. H. (2010) «Crime and Punishment: Teen Sexting in Context.»

TAYLOR, M.; QUAYLE, E. (2003) *Child Pornography: An Internet Crime.* Routledge.

WARMUND, J. (2000). «Can COPPA Work-an Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act.» *Fordham Intell. Prop. Media & Ent.LJ* 11:189.