PREVENCIÓ DE DELICTES A MENORS A INTERNET: L'EXPERIMENT D'OSTRAVA BASAT EN FACEBOOK[1]

FRANCESC REALES ARNÓ

Sotsinspector de la Policia de la Generalitat-Mossos d'Esquadra, llicenciat en filologia anglesa i criminologia, màster en criminologia i diplomat en estudis avançats del doctorat Sistema de Justícia Penal

L'article presenta el desenvolupament i els resultats de l'estudi que es va realitzar a la ciutat txeca d'Ostrava al març de 2011, que tenia com a objectiu analitzar la vulnerabilitat de les dades personals i de la intimitat dels usuaris de les xarxes socials. Es volia mostrar la facilitat amb què es poden aconseguir dades personals dels usuaris i les poques precaucions d'aquests a l'hora de protegir-les. Igualment es presenten diverses iniciatives i estudis per analitzar els fenòmens que afecten menors a la xarxa, com el *sexting*.[2] També es presenta la tasca del cos de Mossos d'Esquadra en el foment d'un ús correcte d'Internet entre el jovent. Els resultats mostren que és molt senzill obtenir dades personals de programes utilitzats en xarxes socials i que una part dels usuaris no pren les prevencions adequades a l'hora de publicitar les seves dades personals.

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 Catalan Police-Mossos d'Esquadra 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. INTRODUCCIÓ

La irrupció del fenomen d'Internet, les tecnologies de la informació i especialment la ràpida implantació de les anomenades xarxes socials ha facilitat que els contactes amb finalitats sexuals amb menors siguin més fàcils d'ocultar gràcies a

1. http://www.facebook.com

2. Anglicisme emprat per anomenar aquest fenomen emergent a la nostra societat, també conegut com a *sexteo*. Consisteix en l'enviament, a través del telèfon mòbil, de material eròtic o sexual d'alta o baixa intensitat (fotos o vídeos), i que tenen com a protagonistes les mateixes persones que l'envien (definició extreta de la pàgina "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/), on es pot ampliar informació mitjançant els enllaços complementaris [consulta: 12 novembre 2012]) [nota de l'ed.].

l'anonimat de la xarxa. Aquestes conductes –encaminades a guanyar-se la confiança dels menors amb la finalitat de concertar trobades per obtenir satisfacció sexual– han rebut recentment la consideració de delicte castigat penalment amb la reforma del Codi penal espanyol,[3] per la qual s'introdueix un nou article (183 bis) en què es tipifiquen les noves conductes de l'anomena't *grooming*[4] i es preveuen, a més, penes agreujades quan l'acostament al menor s'obtingui mitjançant coacció, intimidació o engany.[5]

D'una banda ens trobem amb situacions o comportaments delictius que utilitzen la xarxa com a mitjà propiciatori de l'activitat criminal i, d'altra banda, observem en l'actualitat altres fenòmens que utilitzen les noves tecnologies com a eina per dur a terme comportaments que poden interpretar-se o donar lloc a reprovacions penals, com ara el fenomen del *sexting*. Entre les possibles definicions d'aquest fenomen, utilitzaré la que en fa McLaughlin (2010, 11:4),[6] segons el qual:

> […] engloba les conductes o pràctiques entre adolescents consistents en la producció, per qualsevol mitjà, d'imatges digitals en les quals apareguin menors, de forma nua o seminua, i en la seva transmissió a altres menors, ja sigui a través de telefonia mòbil o correu electrònic, o mitjançant la seva posada a disposició de tercers a través d'Internet.

Agustina (2010) també fa una exhaustiva aproximació a aquest fenomen, del qual presenta la doble vessant de l'infractor com a víctima i com a autor del fet, i també quina hauria de ser la resposta penal al fenomen.

Si parlem de pornografia infantil, la irrupció de les noves tecnologies ha propiciat un canvi en el comportament dels individus consumidors d'aquest tipus de material. Aquests han passat d'una furtiva i costosa compra de revistes i vídeos, a la capacitat de descarregar-se una gran varietat i quantitat de fotos, sense haver de fer una despesa econòmica i en la privadesa del seu domicili. Aquesta facilitat representa en primer lloc un mínim risc per a aquests individus a l'hora d'aconseguir el seu material; en segon lloc, fa que n'aconsegueixin una gran quantitat i, en tercer lloc, genera una constant demanda de material nou i recent. Aquesta demanda constant significa que més i més menors esdevinguin víctimes de la producció de pornografia infantil (Taylor i Quayle, 2003).

3. Llei orgànica 5/2010, de 22 de juny, i la seva entrada en vigor el 23 de desembre.

4. El *grooming* o, en català, ciberassetjament a menors, és la conducta pedofílica desenvolupada normalment a través d'Internet, amb la qual un individu, valent-se d'una identitat falsa, busca establir una relació afectiva amb un menor per a obtenir imatges de contingut sexual o bé abusar-ne sexualment (font: TERMCAT Centre de Terminologia, en línia http://www.termcat.cat/ [consulta: 12 novembre 2012]) [nota de l'ed.].

5. «El qui a través d'Internet, del telèfon o de qualsevol altra tecnologia de la informació i la comunicació contacti amb un menor de tretze anys i proposi concertar-hi una trobada a fi de cometre qualsevol dels delictes descrits en els articles 178 a 183 i 189, sempre que aquesta proposta s'acompanyi d'actes materials encaminats a l'acostament, serà castigat amb la pena d'un a tres anys de presó o multa de dotze a vint-i-quatre mesos, sense perjudici si escau de les penes corresponents als delictes comesos. Les penes s'imposaran en la seva meitat superior quan l'acostament s'obtingui mitjançant coacció, intimidació o engany».

6. Citat a Agustina, José R. (2010). Vegeu-ne la referència al final d'aquest article.

En aquesta facilitat a l'hora de produir material relacionat amb la pornografia infantil, hi té molt a veure la massiva irrupció de càmeres fotogràfiques i de vídeo digitals, fet que ha propiciat que la gent interessada en la visualització n'hagi pogut esdevenir productora.

Així, doncs, cal destacar la força que està prenent la xarxa com a vehicle, no només per albergar o facilitar la comissió de fets delictius o conductes desviades, sinó com a eina per difondre o arribar a una immensa quantitat de persones, en un espai de temps molt reduït, que fa que qualsevol activitat desenvolupada a la xarxa o informació, del tipus que sigui i en el format que sigui, esdevingui pública de manera immediata o gairebé immediata, des del moment que hom decideix incorporar-la a la xarxa o *World Wide Web*.

D'altra banda, hi ha altres conductes que poden considerar-se delictives i que utilitzen la web com a mitjà de perpetració dels fets; en aquest cas es pot parlar del ciberassetjament (Jaishankar i Sankary 2005). L'anomenat ciberassetjador no presenta una amenaça física per a la víctima però en segueix la seva activitat a Internet per recopilar-ne informació i fer-li amenaces o assetjar-la. L'anonimat de la interacció en línia redueix la possibilitat d'identificar-ne l'autor i fa que l'assetjament mitjançant la xarxa sigui molt més comú que l'assetjament físic. Segons Bocij (2003), el ciberassetjament consisteix en:

> Un grup de comportaments en els quals un individu, un grup d'individus o una organització usa les tecnologies de la informació i de les comunicacions per assetjar un altre individu, grup d'individus o organització. Aquests comportaments poden incloure, però no es limiten a, la transmissió d'amenaces i falses acusacions, danys a dades o equips, el robatori d'identitat, el robatori de dades, l'accés a l'ordinador, el contacte amb menors per a propòsits sexuals i qualsevol forma d'agressió. La fustigació és definida com un curs d'acció en què una persona raonable, en la possessió de la mateixa informació, pensaria que causa una altra persona raonable patir un trastorn emocional.

2. LA POLICIA DE LA GENERALITAT-MOSSOS D'ESQUADRA I LA PROTECCIÓ DE MENORS DAVANT DELS DELICTES A LA XARXA

L'any 2008 la Policia de la Generalitat-Mossos d'Esquadra[7] va impulsar, dins el seu àmbit de prevenció, el Pla d'Acció Internet Segura[8] amb l'objectiu de protegir els menors i prevenir la possible victimització de menors i adolescents per delictes a través de la xarxa. Aquest Pla es va presentar, doncs, per donar informació, consells i pautes per millorar la seguretat en l'ús de la xarxa, com per exemple

7. Agraeixo des d'aquí les dades aportades per l'Àrea d'Oficina Tècnica de la Comissaria General de Planificació i Organització de la Direcció General de la Policia del Departament d'Interior.

8. En trobareu informació completa i actualitzada a la pàgina web dels mossos d'esquadra <http://www20.gencat.cat/portal/site/mossos> dins l'apartat de Prevenció > Internet segura.

mitjançant el foment de la pràctica segura de l'activitat a les xarxes socials com Messenger,[9] Tuenti,[10] o Facebook.

Aquest Pla no s'ha circumscrit únicament als centres escolars –on ha tingut una gran acollida per part de la comunitat educativa– sinó que també s'ha introduït a altres punts amb accés a Internet utilitzats pel jovent, com casals de joves o esplais.

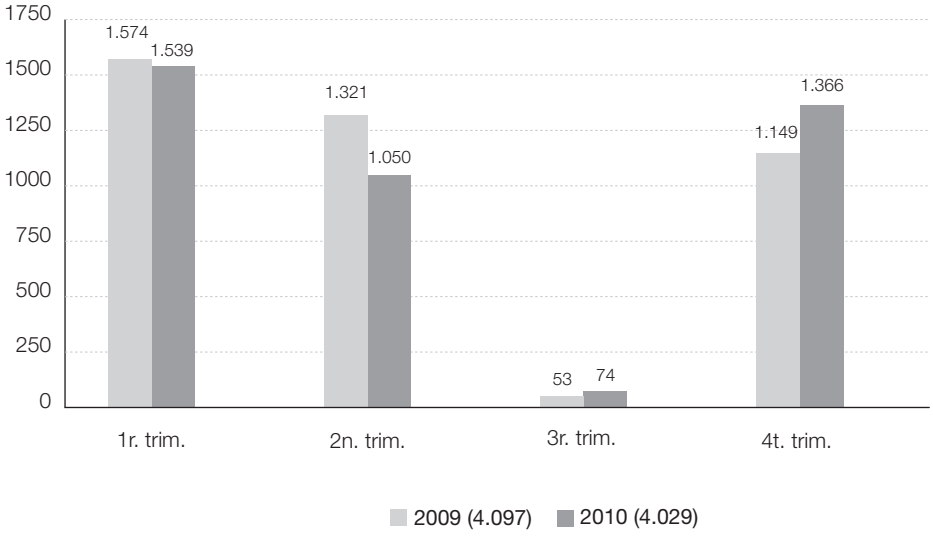
2.1 LES PRESENTACIONS DEL PLA D'ACCIÓ INTERNET SEGURA

El primer any d'implantació del Pla, el 2008, es van realitzar un total de 1.228 presentacions.

Seguidament es presenta més desenvolupada la tasca duta a terme pel cos de Mossos d'Esquadra durant el 2009 i el 2010, anys en què el Pla ja està consolidat.

Durant el primer trimestre escolar dels anys 2009 i 2010, la distribució de presentacions és molt similar; s'observa una lleugera disminució en el segon trimestre de l'any 2010 i una activitat mínima en el trimestre que comprèn els mesos d'estiu.

Figura 1. Presentacions del Pla d'Acció Internet Segura, anys 2009 i 2010, distribuïdes per trimestres



Font: Direcció General de la Policia

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

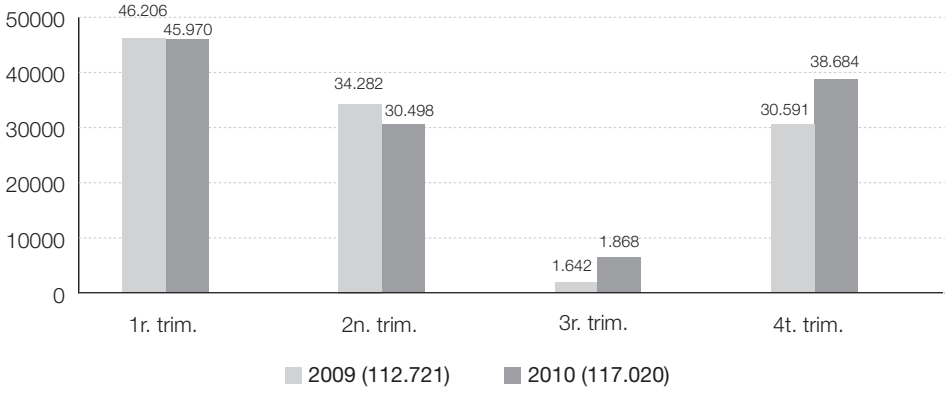
10. http://www.tuenti.com

Taula 1. Nombre de presentacions realitzades en el període 2008-2010

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

La gràfica següent mostra l'increment en el nombre d'assistents en el total de l'any 2010 en comparació amb l'any 2009 i encara més si el comparem amb els 34.138 assistents de l'any 2008, del qual únicament es pot comptabilitzar una part ja que no va coincidir la implantació del Pla amb l'any escolar.

Figura 2. Nombre d'assistents a les presentacions del Pla d'Acció Internet Segura, anys 2009 i 2010, distribuïts per trimestres



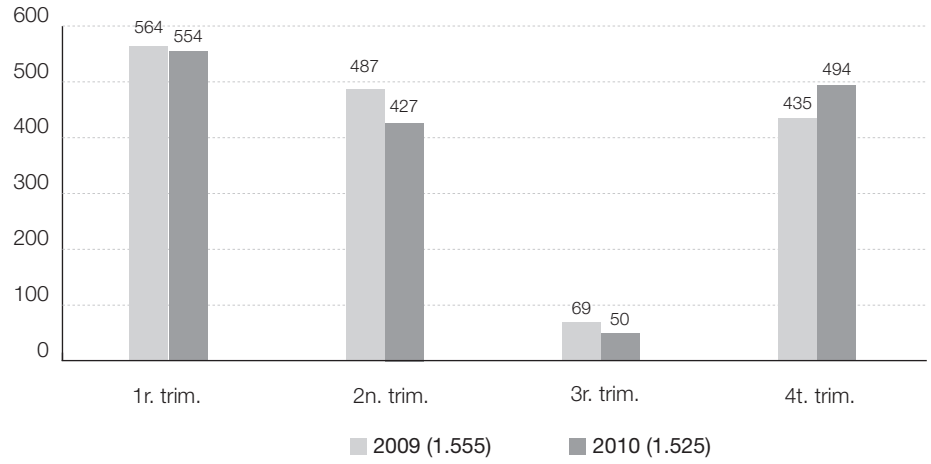
Font: Direcció General de la Policia

Taula 2. Nombre d'assistents a les presentacions realitzades en el període 2008-2010

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

Si analitzem els centres educatius col·laboradors amb el Pla d'Acció de la Policia de la Generalitat-Mossos d'Esquadra, trobem que el 2008 van participar-hi 405 centres. Ja durant els anys 2009 i 2010, la distribució per trimestres del nombre de centres educatius col·laboradors és la que es mostra a la figura següent:

Figura 3. Centres educatius col·laboradors, anys 2009 i 2010, distribuïts per trimestres



Font: Direcció General de la Policia

Com es pot observar, des del primer any de la posada en marxa del Pla, el nombre de centres va fer un salt quantitatiu i arribava a més de mil cinc-cents centres en els anys 2009 i 2010.

Taula 3. Nombre de centres educatius on s'han realitzat presentacions (període 2008-2010)

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

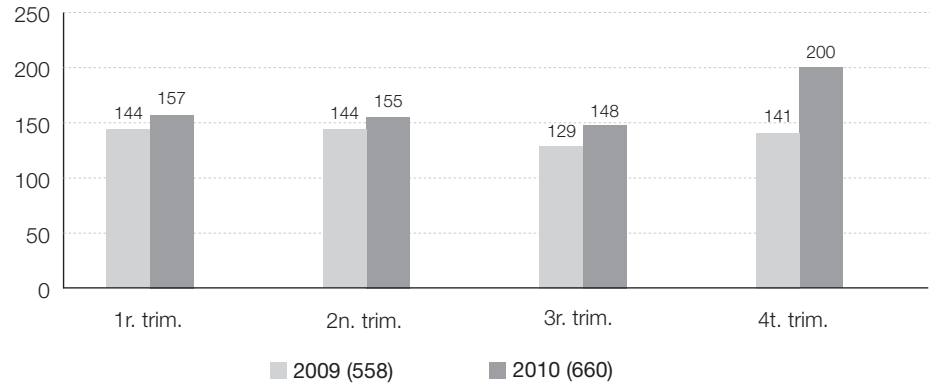
2.2 EL CORREU CORPORATIU DEL PLA D'ACCIÓ INTERNET SEGURA

El cos de Mossos d'Esquadra va configurar una adreça de correu electrònic[11] com un servei d'atenció i consulta per a les persones que creguin que poden ser víctimes d'un delicte o una falta relacionada amb la navegació per Internet, en qualsevol de les seves possibilitats, o per a qui visualitzi alguna pàgina de pornografia infantil.

11. L'adreça electrònica és internetsegura@gencat.cat.

La figura 4 recull les dades sobre el nombre de correus gestionats pel cos de Mossos d'Esquadra amb relació a informacions (pornografia infantil, estafes, consultes, etc.) facilitades per la ciutadania sobre Internet i noves tecnologies.

Figura 4. Gestió del correu internetsegura@gencat.cat, anys 2009 i 2010 distribuïts per trimestres



Font: Direcció General de la Policia (data d'explotació: 20.01.2011)

En el gràfic es veu un augment en l'ús que fa la ciutadania del correu per a contactar amb el Departament d'Interior; aquest augment és d'un 18'27% respecte de l'any anterior.

3. L'EXPERIMENT D'OSTRAVA BASAT EN FACEBOOK

Una de les xarxes socials més populars utilitzades pels joves és el Facebook i, per tant, és una plataforma que pot atraure persones que busquin víctimes potencials de les seves activitats delictives.

Oficialment el Facebook no permet inscriure-s'hi menors de tretze anys però, segons la revista *Costumer Reports* en la seva edició de juny del 2011 als Estats Units,[12] dels vint milions de menors que activament utilitzaven Facebook en el darrer any, set milions i mig –és a dir, més d'una tercera part– eren menors de tretze anys. Aquest fet vulnera les regulacions de la Federal Children's Online Privacy Protection Act (Warmund 2000) de l'any 1998. Aquesta llei prohibeix als llocs web mostrar conscientment informació personal identificable de menors o recollir dades personals de menors de tretze anys.

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

Entre aquests joves usuaris, més de cinc milions tenien deu anys o menys i els seus comptes eren mínimament supervisats pels seus pares. Així mateix, l'estudi mostrava que un milió de joves van ser molestats, assetjats o havien estat sotmesos a altres formes de ciberassetjament escolar[13] a la web, l'any anterior.

A l'Estat espanyol, per accedir a Facebook, l'empresa volia aplicar la legislació dels Estats Units, que en permetia l'accés a majors de tretze anys, però actualment, a instàncies de l'Agencia de Protecció de Dades, l'accés es permet a partir dels catorze anys. Amb edats inferiors, només hi poden accedir amb previ consentiment patern.

Com s'ha comentat anteriorment, l'ús de les xarxes socials està a l'ordre del dia i ha esdevingut un dels mitjans de contacte entre els joves arreu del món, que no només s'utilitza en moments d'oci o amb finalitat d'intercanvi d'informació sinó que han estat utilitzades per moviments amb una intenció política i de revolta social.

En un estudi recent, Boshmaf *et al.* (2011) utilitzen robots socials[14] per a captar amics a Facebook. Aquests investigadors van crear cent dos robots socials, quaranta-nou amb un perfil maculí i cinquanta-tres amb perfil femení, els quals van enviar vint-i-cinc sol·licituds d'amistat per dia a més de cinc mil usuaris reals de Facebook triats a l'atzar. Els enviaments de robots socials de perfil masculí (dos mil tres-cents noranta-un) varen tenir una acceptació, en sis dies, d'un 15,9% (tres-cents vuitanta-un) i els de perfil femení (dos mil sis-cents seixanta-dos) van tenir una acceptació d'un 22,3% (cinc-cents noranta-cinc). Aproximadament, el 86% de les acceptacions d'amistat van ser acceptades en els primers tres dies. Únicament van ser bloquejades un 20% de sol·licituds. L'estudi va durar vuit setmanes i els investigadors van aconseguir 250 Gb de dades personals de milers d'usuaris.

Tenint en compte aquesta possible vulnerabilitat a la xarxa i, concretament, la vulnerabilitat dels menors usuaris del programa Facebook, una organització informàtica txeca i l'ONG de protecció de menors Nebud Obet, amb el finançament del programa Life Long Learning de la Unió Europea, van endegar un experiment a la ciutat txeca d'Ostrava per analitzar la vulnerabilitat dels joves a la xarxa i a Facebook.

4. EL TALLER INTERNET SAFETY

En aquest apartat resumiré el desenvolupament i els resultats del treball de camp i l'estudi empíric duts a terme durant el Taller Internet Safety que va tenir lloc a Ostrava (República Txeca) entre els dies 20 i 26 de març de 2011, en el marc del programa Life Long Learning de la Unió Europea.[15]

13. Concepte conegut en anglès com a *cyberbullying*, Assetjament escolar que es produeix a través d'Internet o utilitzant altres tecnologies com el correu electrònic o els missatges de text dels telèfons mòbils (font: TERMCAT, en línia <http://www.termcat.cat/> [Consulta: 12 novembre 2012]) [Nota de l'ed.].

14. Aquests robots són programaris coneguts com a *socialbots*.

15. Vull agrair la invitació per participar en el taller Internet Safety, per les organitzacions Rizika Internetu a Komunikačních Technologií i Nebud Obět (Don't be a victim!), aquesta darrera dedicada a la prevenció de delictes mitjançant la xarxa i en especial la prevenció d'abusos a menors a través d'aquest mitjà.

4.1 OBJECTIUS DEL TALLER

L'objectiu principal del taller era comprovar la facilitat que hi ha per accedir a les dades de menors mitjançant la xarxa. Es volia comprovar així mateix la vulnerabilitat de les dades que els menors «pengen» a la xarxa i analitzar els mitjans o estratègies que hom pot utilitzar per tenir accés a aquests menors i a les seves dades. Per dur a terme l'estudi es va utilitzar el programa Facebook, que, com s'ha dit a l'apartat anterior, és un dels més utilitzats entre els joves per intercanviar informació i interactuar entre ells i els seus familiars a través de la xarxa, ja sigui amb l'ordinador o amb el seu telèfon mòbil. Al mateix temps, es volia analitzar la facilitat de l'accés a les dades personals de menors mitjançant el seu perfil. Les dades a les quals es volia tenir accés eren: telèfon, adreça, lloc de treball o estudi, fotos, vídeos... a part de l'adreça de correu electrònic.

Així mateix, el resultat de l'estudi havia de servir per a mostrar que fàcil havia estat aconseguir les dades d'un gran nombre de menors usuaris d'aquesta xarxa social i per a conscienciar menors i familiars de la conveniència d'evitar la publicació de dades personals a la xarxa. Aquest estudi, a més, pretenia conscienciar els propis joves participants del projecte en la necessitat d'explicar-ne els resultats als seus companys a través de la xarxa.

Un altre objectiu era atreure un nombre de menors o joves a l'hotel on estàvem hostatjats els participants per comprovar si s'havia pogut «enganyar» algun usuari amb un perfil fals.

4.2 METODOLOGIA

Per a la realització d'aquest treball empíric els organitzadors van convidar a participar-hi quinze investigadors de diversos països de la Unió Europea i que el seu camp de treball fos la prevenció de delictes en diferents àmbits. Per aquest motiu es varen seleccionar professionals del camp de la seguretat, enginyers informàtics, psicòlegs, educadors socials, etc.

Al mateix temps, un grup de trenta alumnes d'un institut d'educació secundària de la localitat d'Ostrava van realitzar el mateix treball de camp durant els mateixos dies que els investigadors europeus. A la meitat i al final de l'estudi es va mantenir contacte amb els estudiants.

Els mitjans emprats per a fer l'estudi van ser ordinadors, programari (en concret la xarxa Facebook), canons projectors i fitxes de control.

Prèviament a l'inici de l'estudi els pares i mares dels alumnes, ja que aquests eren menors, van donar la seva autorització perquè els seus fills hi participessin. Els organitzadors també van informar les autoritats policials de la ciutat sobre el desenvolupament d'aquest experiment.

Les diverses fases de l'estudi foren enregistrades en vídeo i d'aquest experiment se n'ha fet un documental que ha estat posat a disposició dels usuaris a la xarxa i repartit a organitzacions i escoles del país organitzador.

4.3 DESENVOLUPAMENT

Cadascun dels participants europeus van fer una presentació dels projectes que realitzen en el seu país d'origen referents a la prevenció de delictes a través d'Internet. La Policia de la Generalitat-Mossos d'Esquadra va mostrar en la seva presentació la tasca que du a terme en els centres educatius a partir de la implantació, l'any 2008, del Pla d'Acció Internet Segura per a la protecció del menor.[16]

Durant aquesta sessió de presentació es va plantejar el projecte, es van presentar els objectius de la recerca i es va explicar la preparació prèvia que s'havia dut a terme amb les autoritats locals, familiars, professorat, etc.

Es va plantejar la creació de perfils falsos de Facebook per a contactar amb menors i dur a terme la recollida de dades personals. Cada participant era lliure de seguir la seva pròpia estratègia per tal de contactar amb els menors i emprar la informació que desitgés en el seu perfil (vídeos, fotos, etc.).

4.4 CONSIDERACIONS ÈTIQUES

Cal destacar que, ja en el plantejament de l'estudi, van aparèixer opinions d'alguns participants que discrepaven del caire ètic d'aquest tipus d'estudi: manifestaven que era reprovable fer un estudi científic empíric utilitzant l'engany i que la participació d'un grup de trenta estudiants de secundària podia portar problemes psicològics tant als propis participants com a les víctimes de l'estudi, en el cas que fossin menors.

La participant psicòloga va ser la que va plantejar més objeccions a la coparticipació de joves estudiants en l'estudi. Després d'un debat entre els participants, l'opinió de la majoria fou que, si amb el resultat de l'estudi es podia evitar la comissió d'algun delicte o conscienciar un gran nombre de joves i fer-los veure que fàcil és esdevenir víctima d'un engany a través de la xarxa, l'estudi pagava la pena de dur-se a terme. Es va creure que experiments realistes amb un risc mínim són l'única manera d'analitzar amb fiabilitat la viabilitat d'un atac d'aquestes característiques en el món real.

Aquesta postura sembla de l'opinió d'altres investigadors que comparteixen aquest punt de vista, com Bilge *et al*. (2009) i Jagatic *et al*. (2007).[17]

4.5 POSADA EN MARXA

Per tal de crear un perfil fals de Facebook, en primer lloc, cada participant va crear un nou compte de correu electrònic anònim, al qual es va vincular el perfil fals. La majoria de participants va fer aquesta operació en menys de vint minuts; d'altra banda, el grup d'estudiants de secundària ja havien començat a crear els seus perfils la setmana anterior. La majoria dels participants van crear una iden-

16. Amb la presentació de Power-Point *Safe Internet Acces*, elaborat pel cos de Mossos d'Esquadra.

17. Vegeu-ne les referències completes al final de l'article.

titat nova, lligada a aquest perfil de Facebook, en què es feien passar per joves d'entre quinze i divuit anys; per a aquesta nova identitat, van incorporar fotos descarregades de la web, per donar-li més veracitat. La creació de perfils no fou homogènia en el sentit que alguns participants masculins es van fer passar per nois o per noies a la xarxa.

L'idioma emprat en els perfils fou l'anglès ja que la totalitat dels participants era de procedència estrangera, per la qual cosa també es van haver d'inventar motius lògics per a l'estada al país i no aixecar sospites. Els estudiants participants utilitzaven la seva llengua, el txec. Algun participant va utilitzar el món de la música o dels esports per atreure els joves a una trobada a la ciutat el darrer dia de l'estudi.

La dificultat més gran a l'hora de donar veracitat al perfil de Facebook era el fet que es tractava de perfils nous, amb poques amistats afegides i amb un historial curt. Per minimitzar aquesta circumstància es van afegir com a amistats els mateixos membres del grup investigador, entre ells i amb el seu perfil fals.

Va aparèixer un altre problema amb el mateix programa Facebook, ja que va bloquejar alguns dels investigadors en fer aquests enviaments massius de sol·licitud d'amistat. Una de les estratègies per poder «accedir» a noves amistats va ser sol·licitar-la a equips juvenils de futbol locals, clubs de fans de grups musicals, etc. Per poder accedir a joves de la ciutat es va fer un filtratge a través de Facebook amb el nom de la ciutat i així es va acotar els possibles objectius.

Un dels primers fets que van destacar els investigadors va ser la rapidesa –immediatesa, en alguns casos– a l'hora d'acceptar les sol·licituds d'amistat dels perfils falsos dels diversos investigadors o dels estudiants de secundària participants en l'estudi.

Un altre fet destacable era la quantitat de dades personals que molts menors tenien en el seu perfil de Facebook: l'adreça del seu domicili, el seu número de telèfon, el seu lloc de treball o la classe i el centre educatiu on cursaven els seus estudis. D'altra banda, també es tenia accés a una gran quantitat de fotografies i vídeos on apareixien els menors i els seus amics també menors a la xarxa.

L'objectiu de la fase d'estudi era aconseguir atreure, a l'hotel on s'allotjaven els investigadors, possibles víctimes o possibles autors d'assetjament o altres delictes contra la immunitat sexual i conscienciar aquestes víctimes potencials del risc que comporta acudir a trobades amb persones que no coneixen.

Per tal de fer venir joves a l'hotel, cada investigador va crear un «esdeveniment« al Facebook relacionat amb la temàtica i les característiques que cada investigador va configurar en el «seu» perfil; així doncs, hi va haver investigadors que van crear esdeveniments com que un cantant conegut assistiria a signar autògrafs durant una campanya de promoció o que hi assistiria un determinat jugador de futbol famós per promocionar algun producte, etc. S'ha de destacar que l'estratègia establerta per la majoria dels estudiants participants es va basar en la proposició directa d'un contacte d'amistat o de convidar a conèixerse personalment després d'uns dies de diàleg mitjançant el Facebook amb un contingut de marcat component sexual. El fet que l'hotel fos de gamma alta va fer pensar que podia ser un obstacle per donar veracitat a algunes estratègies o ser un factor positiu per a altres. També hi havia el perill que diversos joves que

tinguessin afegits uns quants investigadors sospitessin de diversos actes en el mateix hotel o que s'ho comentessin entre ells.

La qüestió de l'idioma fou també un obstacle per als investigadors ja que, en les converses a través de Facebook amb alguns joves, s'havien d'utilitzar serveis de traducció com el Google Traductor,[18] programa que els joves utilitzaven amb facilitat. Aquest obstacle idiomàtic no el tenien, en canvi, els participants del centre educatiu d'Ostrava ja que interactuaven amb el seu perfil fals i els altres joves, en el seu idioma nadiu.

A la finalització de la quarta sessió els resultats eren els següents:

Taula 4. Resultats dels perfils de Facebook creats a l'efecte d'aquest taller

Sol·licituds d'amistat enviades	2.403
Sol·licituds d'amistat confirmades	1.592
Amistats cancel·lades	52
Nombre de trobades planejades	34

4.6 FINALITZACIÓ DEL TALLER

El darrer dia de l'estada a la ciutat va ser la que proporcionava els resultats pràctics de l'estudi, com s'ha comentat anteriorment; en aquest punt es va analitzar les persones que van acudir a les diverses convocatòries dels participants en l'estudi. La major part dels assistents eren joves que havien acudit per contactar amb els «falsos amics» que havien conegut a Facebook.

S'ha de destacar la presència de dos adults que havien contactat amb una de les investigadores del projecte i que, sorpresos per les característiques de l'estudi, van participar en el desenvolupament final i van explicar la seva visió de Facebook.

Igualment cal destacar la presència d'un adult als voltants de l'hotel que havia contactat amb una estudiant de l'institut de secundària i que podia relacionar-se el seu perfil amb un sospitós de conductes pedòfiles: en primer lloc fou requerit per donar explicacions per la seva presència al lloc i va manifestar que havia estat un error; així mateix un mitjà de comunicació local va entrevistar aquest individu i ell no va voler explicar cap de les seves motivacions per trobar-se al lloc esmentat.

D'altra banda, s'ha de remarcar la quantitat indeterminada però nombrosa d'individus que es van aproximar a l'hotel però que finalment no hi van accedir i que van estar controlats per membres del grup organitzador.

Als menors que havien concorregut a la convocatòria, ja en el lloc, es va aprofitar per presentar-los material relacionat amb els perills a Internet i es va fer una xerrada informativa sobre l'estudi realitzat.

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

Al final del taller, i un cop analitzades les diverses observacions, es va donar per finalitzat l'experiment d'Ostrava. Sobre totes les fases de l'experiment i sobre els resultats obtinguts es va realitzar i enregistrar un vídeo documental,[19] que ja ha estat utilitzat per les diverses ONG del país i per la comunitat educativa per a realitzar els seus plans de prevenció de delictes a Internet.

5. CONCLUSIONS

Aquest estudi ha posat de manifest la facilitat per accedir a les dades personals d'altres usuaris del programa Facebook, i concretament dels menors. Les dades personals que es poden obtenir amb facilitat i sempre des de l'anonimat que proporciona un perfil d'usuari fals són, entre d'altres: adreça del domicili, telèfon, adreça electrònica, lloc on es cursen estudis, lloc de treball, fotos, vídeos, etc.

Cal conscienciar molt més els menors a l'hora de crear els seus perfils i d'introduir-hi la informació que proporcionen a la xarxa. Cal fer-los entendre que aquesta informació pot ser fàcilment accessible, que se'n pot fer mal ús i posar-se ells mateixos en perill. Realment hi ha una manca de conscienciació a l'hora d'analitzar la privadesa de les seves dades: moltes vegades el jovent accepta com a amistats altres persones de manera automàtica sense fer-ne una mínima anàlisi.

És necessària una supervisió del pare, la mare o tutor/a de l'activitat desenvolupada pels joves a la xarxa i de la informació que aquests hi aporten o «pengen», ja siguin dades personals o arxius gràfics com fotos i vídeos.

Les mesures de control de les empreses creadores del programari utilitzat a les xarxes socials no apliquen mesures de seguretat suficientment eficaces a l'hora de prevenir-ne un mal ús, impedir-ne el registre a menors de tretze anys –catorze anys a Espanya– o mesures poc eficaces com el bloqueig de sol·licituds massives d'amistat.

La prevenció de delictes a través d'Internet que tenen menors com a víctimes és una qüestió de gran interès a escala mundial; per això, s'han posat en marxa iniciatives per a intentar millorar la prevenció, com l'experiment que s'ha presentat en aquest article.

La Policia de la Generalitat-Mossos d'Esquadra és un dels cossos policials capdavanters en la prevenció de delictes a la xarxa amb programes com el Pla d'Acció Internet Segura, que es presenta als centres educatius, entre altres llocs. Aquesta tasca en altres països és duta a terme pel mateix professorat dels centres o altres especialistes.

L'aplicació de tècniques conduents a la reducció d'oportunitats, englobades dins la prevenció situacional del delicte, com ara:

– incrementar l'esforç que ha de dur a terme l'infractor per cometre el delicte,

– incrementar el risc que l'infractor ha d'afrontar per cometre el delicte, o

19. Accessible, per exemple, a la web de l'ONG Nebud Obet <http://www.nebudobet.cz/?lang=en> [Consulta: octubre 2012].

– reduir els beneficis o recompenses que el delinqüent aspira a aconseguir amb la consecució del delicte,

pot fer disminuir els fets delictius a la xarxa i alhora reduir la victimització de menors en aquest entorn.

Exemples de l'aplicació d'aquestes tècniques de prevenció situacional adreçades a modificar una situació per tal de reduir les oportunitats de cometre delictes en l'àmbit d'Internet podrien ser:

a) controlar l'accés i l'ús de les xarxes socials per part dels menors i, alhora, establir un lloc a l'habitatge on col·locar l'ordinador per facilitar-ne la supervisió. D'aquesta manera dificultem l'accés il·lícit al menor i evitem converses amb persones inadequades, així com que els joves assumeixin el rol de víctimes propiciatòries;

b) informar els menors de la necessitat de no introduir a la xarxa dades personals, fotos, adreces, telèfons, costums, ja que poden ser utilitzats per a actes preparatoris de delictes;

c) evitar, en la xarxa social on s'intervé, la participació de persones la identitat de les quals no es coneix amb seguretat o senzillament es desconeix.

Aquestes tècniques relacionades amb la prevenció situacional del delicte van encaminades, com ja s'ha dit, a reduir la recompensa, incrementar el risc del possible infractor a ser detectat i incrementar el seu esforç per aconseguir la seva finalitat delictiva. En definitiva, a evitar que en un entorn virtual, igual que s'ha defensat que cal evitar en un espai físic, es puguin trobar un delinqüent motivat amb una víctima potencial amb l'absència d'un guardià eficaç (Cohen i Felson, 1979).

Amb la implementació d'aquestes mesures es pretén, doncs, evitar l'oportunitat de cometre el delicte i en conseqüència la victimització de menors en l'àmbit de la xarxes socials.

6. AGRAÏMENTS

Vull agrair al Long Life Learning Program de la Unió Europea la possibilitat de participar en el programa desenvolupat a Ostrava (República Txeca) i a l'organització Nebud Obet d'aquesta ciutat la seva direcció. També agraeixo les aportacions i correccions de la Dra. Carolina Villacampa, directora de la meva tesi doctoral i professora titular de dret penal de la Universitat de Lleida. Així mateix, agraeixo al cos de Mossos d'Esquadra l'accés a les dades de l'article referents a Catalunya, especialment a l'Àrea Central de Proximitat i Atenció al Ciutadà. Finalment vull agrair l'inestimable ajut de la Lola Vallès i la Conxita Gandia, de l'Institut de Seguretat Pública de Catalunya, per les seves apreciacions i correccions finals.

7. REFERÈNCIES

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 línia], 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.