

CIBERASSETJAMENT, CONDUCTA DE PERSECUCIÓ

Oficina de Relació amb la Comunitat

ABP Nou Barris. RPM Barcelona
Policia de la Generalitat - Mossos d'Esquadra

RESUMEN

Internet se ha convertido en una herramienta imprescindible entre los menores. Si no eres miembro de una red social, si no utilizas el messenger y no compartes con tus amigos fotografías, aficiones, preocupaciones o lugares de ocio, te pueden considerar una especie en extinción. Esta es una de las grandes virtudes de la red y uno de sus grandes peligros a la vez.

Los delitos relacionados con menores en Internet se están multiplicando de forma exponencial y eso genera repercusiones graves para unos jóvenes, que cada vez más sufren las consecuencias de actividades como el grooming, sexting o ciberbullying. Los jóvenes y adolescentes son muy vulnerables ante esta realidad virtual y es por este motivo que hace falta ayudarlos y orientarlos en el uso responsable de las nuevas tecnologías. ¿Que es el ciberacoso? ¿Qué papel juegan los padres y los docentes en la prevención de este fenómeno? ¿Qué acciones legales suponen este tipo de conducta?

La finalidad de este artículo es hacer llegar la importancia que tiene la detección y el trabajo de este fenómeno así como hacer llegar a padres y docentes estrategias para su tratamiento.

ABSTRACT

Internet has become an indispensable tool among the minors. If you are not a member of a social net, if you don't use the messenger and you don't share with your friends: pictures, worries, interests and leisure places can consider you an extinction specie. This is one of the great virtues of the net and some of their great dangers.

The crimes and offenses related with minors in Internet are multiplying in an exponential way and this generates severe repercussions for some youngsters, who every time more suffer the consequences of activities like grooming, sexting or ciberbullying. The youngsters and teenagers are very vulnerable in the face of this virtual reality and for this motive is necessary to help them and to orientate them in the use responsible for the new technologies. What is cyberbullying? Which role do the parents and the teachers play in the prevention of this phenomenon? Which legal actions mean this type of behavior?

The purpose of this article is to make arrive the importance that has the detection and the work of this phenomenon as well as to make strategies arrive at parents and teachers for its treatment.

1. INTRODUCCIÓ

Quan un agent de la Policia de la Generalitat – Mossos d'Esquadra s'adreça a un centre educatiu a fer una activitat preventiva -informativa sobre l'ús d'Internet per part dels menors, té la sensació i la seguretat de trobar-se davant d'una generació que ha crescut en un entorn clarament digital, que basa el coneixement i l'aprenentatge en la col·laboració entre iguals i que tot i conèixer les avantatges i desavantatges de l'ús de les noves tecnologies, no són conscients de la seva exposició a les diferents situacions de risc.

L'accés a missatgeria (WhatsApp, Messenger, Skype, Viber..), xarxes socials (Tuenti, Twitter, Facebook, Google +..), jocs online (a les pròpies xarxes socials, web o a través de vídeo-consola) cerca d'informació (Google, Bing..), correu electrònic (Gmail, Hotmail..) són les principals activitats on els joves inverteixen el seu temps lliure, conformant el seu entorn i la seva realitat diària.

Com a professionals de la seguretat, tenim el "repte" i l'objectiu de donar a conèixer els perills existents a la xarxa, el que és permès i el que constitueix una infracció, detectar abusos, ensenyar formes d'actuació en cas de ser víctima d'un il·lícit penal i sobretot tenir consciència de la pròpia identitat digital tot fent un ús responsable.

La realitat malauradament ens ensenya que per molt que insistim als joves en fer un ús responsable de les noves tecnologies,

el nostre discurs es troba condicionat pel paper que juguen els pares en l'educació tecnològica dels seus fills. Els joves d'aquesta generació són experts en tecnologia però estan molt sols. L'esclètxa digital en relació als pares i fins i tot els mestres fa que els nois encara es sentin més reforçats i no arribin a tenir present o mesurar l'abast d'aquests riscos a que estan exposats.

El primer que ens ve al cap quan parlem d'amenaques a la xarxa són els maleïts virus, els pirates informàtics o hackers, el correu brossa i fins i tot els temuts estafadors que fan de la xarxa el seu hàbitat natural. Però més enllà d'aquests clàssics, cada vegada més, persones que no necessàriament són usuaris experts, recorren a la xarxa i a les noves tecnologies per utilitzar-les amb finalitats perverses. Parlem de conductes de persecució, de comportaments deliberats, repetitius i hostils d'una persona o grup amb la finalitat de danyar la reputació d'altres. Un fenomen, que emparat per l'anonimat, s'ha convertit en una de les principals preocupacions de la comunitat educativa, especialment de pares i mares.

Ens referim al **Ciberassetjament**, el qual quan parlem de menors pot englobar **diferents casuístiques** com per exemple:

- **Ciberassetjament a menors (Grooming):** Terme anglès utilitzat per descriure pràctiques en línia de certs adults per guanyar-se la confiança d'un menor fingint empatia, tendresa, falsa simpatia, etc. Amb

unes finalitats fraudulentess i sovint il·legals, aquest fenomen està relacionat amb l'obtenció d'imatges, vídeos de menors i amb pornografia.

- **Missatges ham (Trolling):** Terme anglès que defineix el comportament d'aquelles persones que escriuen missatges provocadors a la xarxa (correu electrònic, xarxes socials..) de manera intencionada i amb la finalitat de trobar polèmica.
- **Griefing:** Terme anglès vinculat als jocs en xarxa que serveix per definir el comportament d'aquells que perjudiquen de manera intencionada i sistemàtica un jugador en particular.
- **Sexting:** Terme anglès que consisteix en la difusió i/o publicació de continguts (principalment fotografies i vídeos) de tipus sexual, produïts per el mateix remitent, utilitzant el seu mòbil o un altre dispositiu electrònic. El contingut de caràcter sexual, generat de forma voluntària per un mateix, passa a mans d'un altre o altres persones, i a partir d'aquí es pot entrar en un procés d'enviament massiu fins arribar a les mans de l'assetjador.
- **Happy Slapping** o bufetada feliç: Terme anglès que consisteix en realitzar una agressió a un altre persona i gravar-la mitjançant l'ús de la telefonia mòbil, per després penjar-la a la xarxa. La víctima pot ser tant algú conegut com desconegut per l'agressor.

Però, sens dubte, la forma d'assetjament i agressivitat electrònica que es dona més entre un grup d'iguals en edat escolar és el **Ciberassetjament escolar (Ciberbullying o E-bullying)**.

2. QUÉ ENTENEM PER CIBERBULLYING?

És una pràctica que utilitza l'ús de les xarxes socials per humiliar, agredir, insultar, amenaçar o desprestigiar companys de classe o persones conegudes d'una edat semblant. Es tracta d'una nova manifestació del fenomen del bullying, amb el qual comparteix les característiques fonamentals com són la intenció deliberada de fer mal, la repetició en el temps i la desigualtat de forces, però que a diferència d'aquest, es desenvolupa a través, bàsicament, de l'ús de la telefonia mòbil i Internet.

3. QUINS SÓN ELS SEUS COMPORTAMENTS I CONDUCTES?

Actitud violenta, baix rendiment escolar, dificultats per assumir normes, manca d'empatia i necessitat imperiosa de dominar als altres són característiques que defineixen el perfil d'un assetjador.

A l'altre costat es troben les víctimes, joves indefensos sense unes característiques homogènies però que comparteixen conductes bàsiques com tancar-se en si mateix, estar més susceptible en les relacions paterno-filials i baix rendiment escolar.

Els **comportaments** que defineixen aquest fenomen, realit-

zats a través d'aquests mitjans electrònics, fan que:

- Els agressors puguin mantenir-se en l'anonimat. L'agressor es fa invisible per avergonyir, fustigar o amenaçar als seus companys o altres víctimes.
- L'autor té una clara sensació d'impunitat per la seva condició de menor i per la poca concienciació del fet delictiu.
- Els atacs es poden realitzar a qualsevol hora del dia i des de qualsevol lloc, sense necessitat que el perseguidor i la víctima coincideixin, per la qual cosa és molt difícil defensar-se contra aquest assetjament (no veure la cara i la reacció del receptor fa més fàcil l'atac).
- Les víctimes tinguin una sensació de desemparament emocional i fins i tot legal, ja que encara que tanquin una pàgina web amb continguts inapropiats, l'assetjador pot obrir-ne una altra immediatament.
- Les dosis de violència són escalades i repartides, i per tant passen inadvertides als ulls de professors, familiars i fins hi tot dels cossos policials.
- L'assetjament es fa públic i s'obre a més persones ràpidament.
- Aparició de rols diferents entre els protagonistes. A diferència d'una baralla al pati de l'escola en què un assetjador agredeix o intimida a una víctima, el ciberassetjament sovint implica la participació d'altres menors amb papers i rols diferents. Entre aquests tenim els que prenen part activa (assetjadors), les víctimes , els espectadors (no es posicionen però coneixen l'assetjament) i per últim els defensors (ajuden i defensen al perjudicat)

Les **conductes** més usuals d'un assetjador poden ser:

- Manipular o exposar públicament fotografies a Internet per humiliar i avergonyir les "seves víctimes". De vegades, o bé les exposen en webs on es vota la persona més lletja o la més tanoca o bé utilitzen les imatges com a arma per amenaçar a les víctimes a través del xat argumentant que ensenyaran les fotografies si no fan el que ells diuen.
- Amb les dades d'una altra persona editen perfils o pàgines web amb comentaris ficticis sobre les seves experiències sexuals, manies o altres comportaments per fer-ne burla. Es fan passar per aquesta persona en fòrums i pàgines on escriuen opinions que ofenen altres persones o comentaris violents que provoquen la seva expulsió immediata de la pàgina i que no puguin tornar a accedir-hi.
- Se serveixen de missatges o vídeos per amenaçar i insultar la víctima.
- S'introdueixen dins del correu electrònic per manipular-lo, llegir els missatges i registrar la persona que n'és propietària en pàgines on pot ser víctima de correus brossa o de virus informàtics.
- Fan circular entre els coneguts de la víctima rumors en els quals se li suposa un comportament reprotxable i ofensiu amb l'objectiu de buscar polèmica i

enemistats.

- Utilitzen la telefonia mòbil i les seves àmplies possibilitats com instrument d'assetjament. Trucades perdudes i ocultes a qualsevol hora del dia, missatges intimidadors sms o a través del whatsapp.
- Captació d'imatges per la seva posterior difusió a les xarxes socials, on es produeix una agressió a la víctima o bé s'enregistren imatges íntimes d'aquesta.

4. QUÉ POT FER UN PARE SI DETECTA QUE EL SEU FILL HO PATEIX?

Actualment la bretxa digital entre pares i fills és un fet. Si abans la transferència de tecnologies es feia de pares a fills, avui tot ha canviat. Ens trobem davant la primera generació en la història de la humanitat que els nens ensenyen com funcionen les tecnologies a pares i avis. Per tant, la referència per aprendre tecnologies ja no són els grans sinó els mateixos companys o amics i això inevitablement canvia les pautes d'aprenentatge. Pares, mares, tiets, germans, en definitiva, persones que estan en relació amb petits i joves tenen la responsabilitat i el compromís d'estar a la última en les noves tecnologies. Només d'aquesta manera podran estar a prop del seu fill i despertar-li un esperit crític que l'ajudarà a fer un ús responsable d'aquestes.

Des de la Policia de la Generalitat – Mossos d'Esquadra, en el seu objectiu de fer d'Internet un espai segur pels menors i millorar l'ús responsable de les noves tecnologies, es treballa amb aquest col·lectiu establint estratègies i donant consells per evitar aquestes situacions de risc.

Estratègies pels pares

- Fomentar l'educació, el respecte i la responsabilitat
- Ensenyar als joves a no contestar missatges que duguin contingut ofensiu així com evitar discussions amb altres usuaris que portin al insult o menyspreu.
- Ajudar-los a crear polítiques de privacitat adients.
- Fomentar l'ús de contrasenyes segures, identitats anònimes, perfils segurs a les xarxes, perfils segurs a les xarxes socials, utilització correcta de la webcam...
- Preguntar al fill sense complexos per tot allò que ell sap molt més bé que els propis pares per tal d'establir un clima de confiança i també per aprendre'n més (per norma els joves no explicaran mai als seus pares o educadors sobre coses que no entenen).
- Ubicar l'ordinador en espais comuns, que no afavoreixin l'aïllament.
- Evitar que donin dades personals.
- Insistir als fills que MAI han de facilitar informació privada, adreces, telèfons, horaris, contrasenyes d'ordinador, fotografies... a persones estranyes.

- Ensenyar a ignorar l'spam (correu brossa) i a no obrir arxius dels que no en coneixem la procedència o no confiables. Un virus pot malmetre tot l'ordinador.
- Si no es necessita, no instal·lar una webcam. Hi ha programes que poden activar i controlar-la externament.
- Si s'observa que el fill està trist o enfadat després d'usar Internet, està deprimat, restringeix el contacte amb els seus amics o que evita anar a escola, poden ser indicadors que hi ha algun problema.
- Cal informar-se sobre les eines de control. Eines que bloquegen continguts, que limiten el temps de connexió o que registren els webs visitats us poden ajudar perquè la navegació dels joves sigui més segura. Tot i així no cal ser excessivament crítics o pessimistes envers la xarxa ja que els joves transgrediran les regles que se'ls hi imposi si s'apliquen controls o sistemes de seguretat.
- Davant d'un possible problema, cal reaccionar a temps. Si hi ha indicis que els fills estan en risc o es localitzen continguts il·legals cal informar immediatament a la policia.

Aquestes estratègies han de servir als pares per substituir solucions vagues contra el ciberassetjament. Exigir als fills que eliminin el seu perfil de Facebook o treure els telèfons mòbil, no funcionarà. Les eines de comunicació en línia són part del teixit de la vida dels joves. Això també vol dir que les famílies han d'acceptar que encara que el menor sigui una víctima, pot ser que no sempre hagi actuat correctament en línia.

Quin paper juga l'escola en la prevenció d'aquest fenomen?

Les escoles -albergs de nadius digitals- juguen un paper cabdal en l'alfabetització digital dels menors i en la lluita contra aquestes pràctiques de persecució. El seu repte és difondre els bons usos de les xarxes, educant als joves mitjançant campanyes de sensibilització tot demostrant que a Internet no existeix la impunitat i de la mateixa manera que obrir correspondència de la bústia d'una casa és delictiu, també ho és mirar el correu electrònic o entrar al compte d'un company i mirar el què ha escrit.

Durant les nostres sessions informatives, són molts els professionals de la docència que ens han demanat o preguntat com guiar als alumnes cap a un ús responsable de les noves tecnologies. La veritat és que no hi ha cap model ni vareta màgica que puguem emprar en aquest propòsit. La majoria de cops, la millor eina és la pròpia experiència, el coneixement profund de la realitat digital i un toc de sentit comú. En aquest sentit, aprendre tot el que sigui possible de tecnologies com Internet, interessar-se pels hàbits "online" dels alumnes i conèixer els perills d'Internet, ajudaran a professors/es en aquesta tasca pedagògica.

Però per assolir aquests objectius i ser capaç d'equiparar els seus coneixements amb els dels seus alumnes, es fa del tot necessari que el docent i l'escola disposi d'eines, se'ls expliqui què és Internet i com utilitzar-lo, aprendre quins són els principals perills de l'ús de les xarxes socials (problemes relatius a la protecció de la privacitat, la protecció de dades personals, els virus..), com detectar abusos i conductes de persecució i sobretot com actuar davant certs comportaments digitals. En aquest sentit, fins i tot hi ha opinions que defensen la introducció d'una assignatura a les escoles sobre "Seguretat a les xarxes socials".

Una qüestió ens ha de fer reflexionar:

- Per què la gent condueix una moto amb el casc posat ? Per obligació.

Temps al temps

6. ACCIONS LEGALS I MESURES

Internet és una eina de comunicació caracteritzada per ser una font d'informació inesgotable. Les possibilitats de comunicació que actualment ofereix Internet, sobretot gràcies a les xarxes socials, han convertit la pantalla de l'ordinador i del "smartphone" en porta d'accés a un món virtual on quasi tot és possible d'una forma còmoda i senzilla. Des de que va esclatar el boom d'Internet fa 15-20 anys tot ha evolucionat tan ràpidament que el sistema dista encara de ser perfecte, sobretot en el camp de la seguretat on cada vegada hi ha més internautes i més víctimes potencials.

El actual marc legal o d'actuació és encara força deficient. Tot i que el codi penal s'ha pogut actualitzar aquest últims anys cada cop es produeixen més delictes informàtics i és inevitable que el nombre augmenti dia a dia. Aquesta fragilitat és aprofitada per delinquir, sobretot per persones cada vegada més joves que s'aprofiten de la "ignorància" de molts usuaris de la xarxa.

Ens trobem davant d'una nova forma de delinqüència on els delictes, en molts casos, són els mateixos que en el món NO virtual. Tot i que a dia d'avui el ciberassetjament no està encara tipificat en el Codi Penal, això no impedeix que la major part dels delictes comesos a través de les tecnologies de la informació sí ho estigui, com per exemple:

- Injúries i Amenaces
- Violació del dret a la intimitat
- Alteració de dades
- Delictes contra la integritat moral
- Delictes contra el dret a la pròpia imatge
- Delictes contra les falsedats -usurpació
- Descobriments i revelació de secrets
- Tracte degradant, etc.

Per poder identificar el més aviat possible l'autor d'un il·lícit penal es recomana guardar totes les proves existents. Un exemple seria gravar una imatge de la pantalla de l'ordinador o del telèfon mòbil on apareguin els missatges insultants o bé imprimir una conversa de xat. Si els fets revesteixen gravetat

suficient, les víctimes han de formalitzar oficialment la denúncia a qualsevol de les comissaries de la Policia de la Generalitat - Mossos d'Esquadra. A partir d'aquest moment s'informa al jutjat, que pot sol·licitar al proveïdor d'Internet l'adreça IP des de la qual s'han escrit els comentaris (les dades IP es guarden en els operadors un temps limitat per la qual cosa, es demana celeritat alhora de fer els tràmits).

Una vegada identificat l'autor dels fets el jutge de menors imposarà les mesures pertinents. És habitual l'aplicació de l'ordre d'allunyament que suposarà la prohibició de comunicació sigui de forma visual, verbal o escrita, per qualsevol mitjà de comunicació o medi informàtic. Així mateix altres mesures són la llibertat vigilada, la realització de tasques socioeducatives, les prestacions en benefici de la comunitat i les permanències de caps de setmana en domicili o en centre educatiu de menors.

La realitat malauradament ens diu que als menors els hi costa molt denunciar, per la qual cosa ens trobem davant una bossa de criminalitat oculta molt important i això, òbviament, preocupa als cossos de seguretat.

7. ALGUNS SUGGERIMENTS PER A LES VÍCTIMES

- Feu servir les preferències o les eines de privadesa per bloquejar l'assetjador. Si és en un xat, deixeu la conversa. La manca de reacció causa els agressors i fa que deixin de molestar.
- Guardeu les proves, fins i tot si són poc importants. La situació pot empitjorar.
- És bo implicar en el problema a un dels teus pares, però si no pots, el professor de l'escola també pot ajudar-te.
- Feu servir les eines que et donen les xarxes socials per informar/denunciar l'abús o ús inadequat del servei.
- Configureu correctament les polítiques de privacitat dels vostres comptes i no pengeu imatges que us puguin comprometre.
- No menyspreu mai els coneixements tecnològics de cap usuari de la xarxa. Vosaltres en sabeu molt, però hi ha altres internautes que en saben molt més.

Referències a tenir en compte:

Policia de la Generalitat - Mossos d'Esquadra

www.gencat.cat/mossos
internetsegura@gencat.cat

CESICAT

Centre de Seguretat de la Informació de Catalunya

www.internetambseny.cesicat.cat
info@cesicat.cat

IQUA - Agència de Qualitat d'Internet

www.iqua.cat
iqua@iqua.net
Butlletí.jove.cat