UNIVERSITÀ DI PISA

Corso di Laurea in Informatica Umanistica

RELAZIONE

Internet safety: un'analisi sull'uso consapevole della Rete dei nativi digitali puri e dei loro genitori

Candidato: *Giulia Del Francia*

Relatore: *Maria Simi*

Correlatore: *Enrica Salvatori*

Anno Accademico 2015-2016

Indice

Introduzione 4
1. Il problema 6
1.1 I nativi digitali 6
1.2 L'obiettivo 7
2. La scuola secondaria di primo grado "G. Carducci" di Venturina Terme (LI) 9
2.1 I progetti 9
3. Rischi e soluzioni 20
3.1 Cyberbullismo 20
3.1.1 Bullismo e cyberbullismo 20
3.1.2 Tipologie di cyberbullismo 20
3.1.3 Prevenzione 23
3.1.4 Come affrontare un cyberbullo 24
3.1.5 Aspetti legali 25
3.2 Sexting 26
3.2.1 Definizione 26
3.2.2 Rischi 27
3.2.3 Prevenzione 28
3.2.4 Come fare in caso il materiale venga diffuso in Rete 29
3.2.5 Aspetti legali 29
3.3 Adescamento online 30
3.3.1 Definizione 30
3.3.2 Come avviene l'adescamento? 30
3.3.3 Prevenzione 31
3.3.4 Aspetti legali 32
3.4 Dipendenza 32
3.4.1 Definizione 32
3.4.2 Tipologie 34
3.4.3 Prevenzione e cura 36
3.5 Phishing 37

3.5.1 Definizione 37
3.5.2 Le fasi di un attacco di phishing 37
3.5.3 Come riconoscere un tentativo di phishing 38
3.5.4 Come difendersi dal phishing 38
3.6 Virus, Trojan, Malware 39
3.6.1 Definizione 39
3.6.2 Categorie di malware 40
3.6.3 Come difendersi dai malware 41
4. I prodotti 42
4.1 Primo prodotto: piccola guida per i genitori sulla sicurezza in Internet 43
4.2 Secondo prodotto: presentazione con Prezi 44
4.3 Terzo prodotto: questionari con Ninja Forms 45
5. Distribuzione dei questionari e risultati 47
5.1 Questionario genitori 47
5.2 Questionario ragazzi 58
Conclusioni 68
Ringraziamenti 70
Appendice 72
Bibliografia 82

Introduzione

Quando ero piccola, mi ricordo che per trovarsi con gli amici si usciva di casa e si andava a suonare alle loro porte, e poteva capitare di fare viaggi a vuoto. Non c'erano i cellulari, o almeno non con la diffusione che hanno oggi, quindi non c'era il messaggio su Whatsapp per mettersi d'accordo e non c'era la condivisione di foto sui social per far sapere al mondo cosa stessimo facendo. Andare a pranzo con gli amici era un modo per ritrovarsi e fare due chiacchiere, adesso se non si fa una foto al cibo per caricarlo su Instagram sembra che quel pranzo non ci sia mai stato. Così come i viaggi e tutte le altre attività: niente foto caricate significa che quelle attività non le hai mai fatte. Le nuove generazioni, soprattutto i cosiddetti *nativi digitali puri*, di cui si farà cenno nel corso di questa tesi, vivono così: sono nati e cresciuti con le nuove tecnologie, quindi per loro è una cosa normale usarle per integrarle con la loro vita reale. Attraverso i nuovi mezzi, comunicano con il mondo esterno e in un certo senso lo vivono, perché sono parte integrante delle loro relazioni sociali e cambiano il loro modo di vedere il mondo.

Lo scopo di questa tesi è fare un'analisi, mediante questionari, di quanto realmente i giovani conoscano il mondo digitale e i pericoli che possono incontrare, e ci si rivolgerà anche ai loro genitori, condividendo consigli sulle buone norme da seguire per una corretta navigazione in Rete. Perché non basta saper mandare un messaggio su Whatsapp o caricare una foto su Instagram per dire di saper usare le nuove tecnologie: bisogna soprattutto conoscere i rischi che si possono incontrare, per poterli evitare e navigare in tranquillità.
Come fare per insegnare ai giovanissimi il corretto uso della rete e soprattutto come avvertire loro e i loro genitori dei pericoli a cui possono andare incontro? La tematica della sicurezza in rete (Internet Safety) e dei pericoli più rilevanti che albergano nel Web è un tema relativamente recente, dato che nasce, sotanzialmente col Web 2.0. Soluzioni facili, per ora, non ne esistono in quanto il fenomeno implica ragionamenti di carattere giuridico (libertà dell'individuo, individuazione del colpevole, reato, pena) e di comunicazione.

In questa tesi si è scelto di affrontare il problema dal lato pratico: provando a creare strumenti informativi mirati a raggiungere un particolare target di utenti (studenti della scuola secondaria di primo grado e i loro genitori) e potenzialmente utili ad essere utilizzati su uno scenario più ampio all'interno del progetto Erasmus "A Digital Journey in Europe", che vede collaborare scuole primarie di 4 paesi europei.

Per produrre e testare il materiale ho avuto l'opportunità di stare a contatto con i ragazzi della scuola secondaria di primo grado di Venturina Terme per tre giorni, nel corso dei quali ho spiegato e distribuito loro questionari digitali, e con cui ho avuto modo di dialogare per comprendere meglio il loro punto di vista.

La tesi è così suddivisa. Nel primo capitolo viene presentato il problema che mi ha portata a scegliere il tema di questa tesi, la definizione di *nativo digitale* e l'obiettivo del lavoro.
Nel secondo capitolo si parla della scuola oggetto di questa tesi: la scuola secondaria di primo grado di Venturina Terme (LI), dei progetti svolti negli a.s. 2015/2016 e di quelli che svolgeranno nell'a.s. corrente 2016/2017; inoltre, ho raccontato di una giornata seminariale formativa a cui ho avuto l'opportunità di partecipare.
Nel terzo capitolo ho inserito il materiale che ho trovato riguardo i rischi che si possono correre navigando in Rete, con relative soluzioni e approfondimenti. Quel materiale è stato poi riassunto per creare il materiale per i genitori, e cioè la piccola guida e la presentazione Prezi.
Nel quarto capitolo ho presentato i prodotti creati per questa tesi: la guida per i genitori, la presentazione Prezi e i questionari creati con Ninja Forms, un plugin di Wordpress. Tutto il materiale è stato creato e rielaborato dalla sottoscritta usando Adobe InDesign, Adobe Photoshop e Adobe Illustrator. Alcune immagini sono state prese da freepik.com e iconmonstr.com per essere poi rielaborate.
Nel quinto capitolo, ho presentato i due questionari, uno per i genitori e uno per i ragazzi, e i relativi risultati correlati di qualche commento. Seguono poi le conclusioni.

1. Il problema

La scelta del tema di questo elaborato prende spunto dal progetto europeo "A Digital Journey in Europe"[1], nel quale partecipano quattro Paesi: Irlanda, Danimarca, Italia e Finlandia. L'obiettivo è la condivisione e lo sviluppo di buone pratiche per l'utilizzo delle nuove tecnologie nella scuola primaria.

Il problema che mi ha portata a scegliere questo tema è che ormai si sente parlare di "nativi digitali", di "Web 2.0" e di molti casi in cui la rete viene utilizzata in modo sbagliato, condividendo immagini o video sbagliati di cui poi ci si pente senza però poter tornare indietro. Un caso recente è stato quello di Tiziana Cantone, ragazza suicida dopo aver inviato ad altre persone, senza pensare che potevano finire in Rete, dei video hard che la ritraevano. Questo è solo uno dei tanti casi: altri esempi sono quelli di Carolina Picchio, Andrea Natali, Andrea (conosciuto come "il ragazzo dai pantaloni rosa"), la ragazzina conosciuta col nickname "Amnesia" su Ask.fm, tutti vittima di cyberbullismo. Ma ce ne sono molti altri, vittime per mancata prevenzione, per ignoranza, e quindi per l'impossibilità di capire la situazione o di poterla affrontare.

Per questo la scelta del tema di questa relazione: è importante la prevenzione, è importante far conoscere alle persone (studenti, genitori ed insegnanti) anche il lato oscuro della rete, per cercare di limitare casi come quelli citati sopra o anche meno gravi. E' importante partire dai nativi digitali, per far crescere delle generazioni responsabili dato che sono loro per primi ad essere circondati da mezzi tecnologici sin dalla più tenera età, così come è importante formare i genitori e i docenti per sapere come affrontare determinate situazioni e guidare così i ragazzi fin da piccoli all'utilizzo della rete in modo responsabile.

1.1 Nativi digitali

Nel mondo in cui viviamo oggi, è inevitabile che le tecnologie facciano parte della nostra vita quotidiana fin dalla più tenera età. Nel 2001 si è iniziato a parlare di *nativi digitali*, termine da attribuire allo scrittore statunitense Marc Prensky, innovatore nel

[1] http://adigitaljourney.labcd.unipi.it/

campo dell'educazione e dell'apprendimento. Per nativi digitali si intendono coloro che fin dalla nascita sono stati a contatto con i mezzi di comunicazione digitali e tutte le tecnologie emerse negli ultimi anni (smartphone, computer, social networks, blog).
Paolo Ferri, docente presso l'Università di Milano "Bicocca", è uno degli autori che conferma il fatto che le nuove generazioni si approccino alla vita in maniera del tutto differente rispetto a quelle precedenti. Secondo Ferri, i nativi digitali possono essere suddivisi in tre tipologie[2]:

- **Nativi digitali puri** (tra 0 e 12 anni);
- **Millennials** (tra 14 e 18 anni);
- **Nativi digitali spuri** (tra 18 e 25 anni).

I nativi digitali puri sono da considerarsi quelli veri, in quanto fin da piccoli hanno maturato un'esperienza diretta con gli schermi interattivi digitali come consolle, smartphone, tablet e con la navigazione in Internet. A differenza degli altri, i nativi digitali puri fanno uso del Web 2.0[3]. Per questi bambini, lo schermo (che sia dello smartphone o del computer) rappresenta un accesso alla realtà, uno spazio per comunicare con il mondo esterno. A loro disposizione infatti c'è una grande quantità di strumenti digitali di apprendimento e comunicazione: i social networks, le chat, i blog, la posta elettronica; sono parte integrante delle loro relazioni sociali e cambiano il loro modo di vedere il mondo. Ma sanno cosa possono incontrare su internet? A questo proposito esistono molti progetti, messi in atto sia dalle scuole in sé sia dalla Polizia Postale, dal MIUR e altre organizzazioni, per condividere le buone pratiche della navigazione in rete, puntando molto sulla prevenzione.

1.2 L'obiettivo

L'obiettivo di questo elaborato sono proprio i nativi digitali puri (in particolare gli studenti della scuola secondaria di primo grado "G. Carducci") e i loro genitori. Si andrà a verificare attraverso due questionari anonimi messi a disposizione sul sito www.adigitaljourney.labcd.unipi.it quanto sia studenti che genitori sono informati sui

[2] http://educationduepuntozero.it/tecnologie-e-ambienti-di-apprendimento/nativi-digitali-puri-nativi-digitali-spuri-404174180.shtml
[3] Termine introdotto nel 2004 da O'Reilly Media, indica la seconda fase di sviluppo e diffusione di Internet, caratterizzata da un forte incremento dell'interazione tra sito e utente. (Treccani.it)

rischi che possono incontrare in rete. Oltre a questo, verrà messo a disposizione del materiale informativo sui pericoli della rete e relative soluzioni.

Il suddetto materiale informativo sarà rivolto soprattutto ai genitori, in quanto solitamente i progetti sulla sicurezza in rete coinvolgono gli studenti e i docenti, quindi si presuppone che gli studenti, compilando il questionario, siano già informati sulla terminologia che incontreranno e le relative situazioni, mentre i genitori si possono trovare in difficoltà, in quanto la terminologia per loro potrebbe essere sconosciuta.

2. La scuola secondaria di primo grado “G. Carducci” di Venturina Terme (LI)

Prima di capire a chi rivolgere il materiale informativo, mi sono recata alla scuola secondaria di primo grado “G. Carducci” di Venturina Terme (LI), in particolare dalla I coll. vicaria Angela Marina Chiavaroli, dal vicepreside Angiolo Fedeli e dalla dirigente scolastica Daniela Toninelle per chiedere quali progetti avessero fatto o stessero per fare. Ho scoperto che i progetti sono quasi tutti rivolti a studenti e docenti, e solo uno parzialmente rivolto ai genitori (da qui il motivo per cui il materiale è rivolto soprattutto a loro). Tra questi, ho avuto l’opportunità di partecipare a una giornata seminariale formativa per docenti referenti/tutor a Livorno, chiamata “Cyberlivorno 2016/2017 per crescere e proteggere”.

2.1 I progetti

Incontro con gli studenti delle scuole medie di Venturina Terme sul tema: la sicurezza su internet.

Questo progetto è stato svolto nell’a.s 2015/2016 e ha coinvolto le classi prime. L’obiettivo è la tutela dei ragazzi durante la navigazione. L’incontro è stato organizzato a Piombino dal Lions Club International, la più grande associazione di servizio al mondo, con 1,35 milioni di soci in oltre 45000 club di 206 Paesi del mondo che dedicano una parte del loro tempo agli altri. Il socio lions Ing. Piero Fontana ha illustrato, attraverso un’attività interattiva e con l’ausilio di supporti audiovisivi, i pericoli e le insidie della rete per rendere i ragazzi maggiormente consapevoli dei rischi che affrontano ogni giorno e conoscere i comportamenti da adottare per una navigazione in sicurezza. Lo stesso incontro è stato ripetuto quest’anno, il 16 Gennaio 2017, coinvolgendo sempre le classi prime.

Concorso a livello nazionale sul tema "Bullismo e Cyberbullismo, quali le cause, il come e il perché…"

Motore di quest'azione sono i Rotary Club, i Club Rotaract e i Club Interact che nella loro autonomia associativa si sono attivati nei loro territori per favorire la partecipazione degli Istituti scolastici (Medie, Superiori, Università) al bando di concorso. Si è svolto nell'a.s 2015/2016, e l'iniziativa è culminata il 18 Marzo 2016, che ha visto protagonisti gli allievi delle scuole medie, medie superiori e studenti universitari e neo laureati che si sono classificati a vario livello in esito al concorso.

Il concorso è stato bandito a livello nazionale, il tema è: "Bullismo e Cyberbullismo, quali le cause, il come e il perché." Lo studente è invitato ad analizzare il fenomeno per capirne le cause e le conseguenze, aprire al dialogo, guardare al futuro con il fine di migliorare la società. Le attività da svolgere sono state le seguenti: realizzazione di uno spot/corto amatoriale; produzione di un manifesto originale, realizzato con tecnica a piacere; uno scatto fotografico originale, realizzato con tecnica a piacere, svolgimento di un elaborato scritto che sviluppi il tema. Le attività svolte dalla scuola secondaria di primo grado "G. Carducci" di Venturina Terme sono state le seguenti:

- Video: *Smontailbullo* (classe 2B), *Lo scherzo non è sempre divertente* (classe 3A)
- Manifesto: *Vogliono che io muoia* (classe 3A)
- Scatto fotografico: *Violento colpo* (classe 3B), *Ho paura* (classe 3B).

Il 22 marzo è uscito un comunicato stampa del Comune di Campiglia Marittima che elogiava la classe 3A della scuola secondaria di primo grado "G. Carducci" di Venturina Terme per la vittoria al concorso del loro video "Lo scherzo non è divertente". La premiazione è avvenuta nel salone d'onore della caserma "Gen. B. Sante Laria" a Roma, e i ragazzi sono stati accompagnati anche dal vicesindaco di Campiglia Jacopo Bertocchi. Al progetto è intervenuta anche la criminologa Lara Vanni e il colonnello Eugenio Cammarata. Il progetto non si svolgerà nell'a.s. 2016/2017.

Percorso formativo per docenti "Bullismo, Cyber-bullismo e i principali rischi virtuali: riconoscerli, prevenirli e attuarne gli effetti negativi.

L'obiettivo di questo corso è fornire ai docenti gli strumenti per attivare poi percorsi di sensibilizzazione e prevenzione destinati agli studenti. Interverrà il Dott. Andrea Bilotto, psicologo scolastico esperto in Cyberbullismo ed Educazione alla Salute. Il corso approfondisce tre aree tematiche:

- Le caratteristiche del bullismo "tradizionale" nell'ottica sistemica;
- Il cyber-bullismo e le sue principali forme e manifestazioni nei giovani;
- Come educare gli allievi a contrastare il fenomeno sia attivando le risorse del gruppo che stimolando nell'individuo una maggiore capacità di gestire le proprie emozioni.

Durante il corso si parlerà di: bullismo, il fenomeno del cyberbullismo, prevenire il cyberbullismo ed educare alla gestione delle emozioni nelle relazioni interpersonali, i principali rischi virtuali.

Il percorso si svolgerà nell'a.s. 2016/2017.

Progetto di prevenzione al cyberbullismo e rischi virtuali per i minori.

Il progetto si propone di contrastare i pericoli che derivano da un utilizzo improprio o non accompagnato di Internet, da parte di minori. Per gli adolescenti la rete rappresenta una straordinaria occasione di apprendimento e conoscenza, ma è anche un luogo in cui si possono fare "incontri" non proprio piacevoli.

L'intervento coinvolgerà gli alunni, i loro genitori e i loro insegnanti dell'Istituto Scolastico, e si svolgerà nell'a.s. 2016/2017. Gli obiettivi sono:

- Formare ad un corretto utilizzo di Internet (aspetti relazionali e sociali);
- Informare sui rischi: cyberbullismo, pornografia, pedopornografia, stalking, virus e spam, informare sulle leggi vigenti in fatto di privacy, diritti d'autore, furto di dati personali, furto di denaro, sui siti illegali (che inneggiano all'odio e alla violenza), sui rischi da dipendenza online;
- Fornire formazione sui sistemi per prevenire ed evitare i rischi;
- Collaborare alla raccolta di dati statistici per monitorare l'evoluzione degli stili di utilizzo del web da parte di ragazzi e famiglie;

- Aiutare nella costruzione di competenze che possano sostenere un uso consapevole e creativo dei media al fine di coglierne le opportunità e prevernirne gli abusi.

Interverrà uno psicologo iscritto all'Albo degli Psicologi esperto su Cyberbullismo e rischi virtuali.

Progetto Cyberlivorno a.s. 2016/2017.

Si tratta di giornate formative per gli studenti: ci saranno, nei mesi di febbraio/aprile, degli incontri con la polizia postale, promossi all'interno del progetto cyberbullismo provinciale "Cyberlivorno 2016/2017: per crescere e proteggere".

Lo scopo è quello di stimolare la riflessione dei ragazzi, con interventi di sensibilizzazione, prevenzione e contrasto del fenomeno del bullismo e del cyberbullismo.

Nell'Istituto Comprensivo "G. Marconi" di Venturina Terme (LI) hanno comunicato l'adesione tutte le classi seconde e terze della scuola secondaria di I grado "G. Carducci" (Venturina Terme) e "L. Muratori" (Suvereto).

Giornata di Formazione/Informazione per docenti tutor/referenti. Progetto "Cyberbullo… formarci per essere Cyber-protetti".

Questo incontro, a cui io stessa ho avuto l'occasione di partecipare, si è svolto il 12 Gennaio 2017 dalle 09:00 alle 18:00 presso la Sala della Fondazione L.E.M. a Livorno. Si trattava della giornata inaugurale del progetto, promosso dal Ministero dell'Istruzione e della Ricerca. Il progetto è coordinato dall'USR Toscana Ambito territoriale di Livorno, in collaborazione con la Prefettura di Livorno, il CTS e il CTI della provincia di Livorno, il CIAF Centro Infanzia Adolescenza e Famiglie del Comune di Livorno, il Compartimento di Polizia Postale e delle Comunicazioni Toscana (sezione di Livorno), la Procura della Repubblica presso il Tribunale di Livorno, l'Università di Pisa, l'Università di Firenze, l'Ordine degli psicologi per la Toscana, la Fondazione L.E.M. Livorno Euro Mediterranea, il Comitato Provinciale di Livorno per l'UNICEF e il Corecom. Oltre a questa giornata, si svolgeranno incontri anche in altre sedi di Livorno,

Cecina e Portoferraio, e l'obiettivo è la formazione di 2 docenti tutor/referenti (3 per l'Isola d'Elba) per ogni istituzione scolastica.

A inizio incontro ci è stata consegnata una cartellina contenente alcuni fogli, il programma della giornata, due volantini della Polizia Postale con dei consigli per genitori e studenti e un libretto intitolato "Bullismi", creato da Giusi Marchetta, con una storia di un ragazzo che da vittima diventa cyberbullo senza volerlo del ragazzo che lo bullizzava, per capire alla fine che quello che ha fatto è sbagliato. Sia nel libretto che nei volantini appare il simbolo del progetto sulla sicurezza nell'uso della Rete "una vita da social[4]" creato dalla Polizia, rivolto agli utilizzatori dei social e in particolare agli studenti delle scuole secondarie di primo e secondo grado, ai loro insegnanti e ai loro familiari.

La giornata si è svolta dalle ore 9 alle ore 18, con interventi di esperti.

Saluti.

La giornata è iniziata con i saluti, ha introdotto il **dirigente USR Anna Pezzati**, che ha parlato dell'importanza della prevenzione e del fatto di insegnare l'uso responsabile dei mezzi multimediali già dalla scuola primaria. Ha poi aggiunto il bisogno di una formazione a 360°, che coinvolga studenti, genitori e docenti.

Hanno parlato poi il **prefetto di Livorno Anna Maria Manzone, il direttore USR Domenico Petruzzo, l'assessore regionale Cristina Grieco, il sostituto del vicesindaco di Livorno e il dirigente scolastico CTS Livorno Giuseppe de Puri.**

Prima relazione: "Bullismo e Cyberbullismo: cosa sappiamo e come possiamo intervenire".

Parla Ersilia Menesini, docente di Psicologia dello sviluppo – Dipartimento di Scienze Formazione e Psicologia dell'Università di Firenze.

Inizialmente c'è stata la visione del video "Solitudine dei numeri primi", in cui si vede il fenomeno del bullismo femminile. Nel video, si vede una ragazza che è costretta a spogliarsi da un gruppo di bulle, viene presa in giro per una cicatrice dopodiché è

[4] http://www.poliziadistato.it/articolo/31696/

costretta a mangiare una caramella che è stata precedentemente strusciata per terra. Si nota una profonda sottomissione della vittima.

Sono state elencate le tre component del bullismo: intenzionalità, ripetizione e squilibrio di potere, ed è stato affermato che i ragazzi delle scuole medie tendono a non capire le differenze, quindi una femmina è una femmina, un maschio è un maschio e così via. Sono stati poi elencati i diversi tipi di bullismo: cyberbullismo, omofobico, razzista, contro i disabili. Di questi, il più grave è il cyberbullismo: attraverso la visione di una tabella, si nota che è maggiore nei ragazzi di 11 anni rispetto a quelli di 13 e 15, e che il fenomeno è aumentato dal 2010 al 2015.

Il discorso è poi caduto sugli insegnanti: i dati dicono che il 50% spesso non interviene perché non vede o minimizza il problema. Se intervengono, spesso la strategia è parlare con tutta la classe, mettendo in pericolo la vittima ed esponendola ancora di più.

Sempre parlando di dati, è emerso che i programmi antibullismo sono efficaci: con essi si è notato circa il 20% di riduzione.

La relazione si conclude dicendo che, per affrontare questo tipo di situazioni, serve la presenza di un team specializzato nelle scuole.

Seconda relazione: "Uso consapevole e sicuro: internet e social network".

Parla Gianluca Massettini, direttore tecnico Capo Ing. del Compartimento Polizia Postale e delle Comunicazioni della Toscana.

La domanda che gli viene posta è: quali sono i rischi di internet e dei social network? È possibile un uso consapevole della rete?

La relazione è iniziata parlando dei genitori, che spesso sono convinti, sbagliando, che i figli a casa siano al sicuro; invece è proprio dalla Rete che viene il pericolo, e può raggiungerli ovunque, anche in camera loro.

Cyberlivorno va a creare un piano programmatico, legato ai programmi sul lungo termine e non solo emergenziali.

In passato, la prevenzione era solitaria, non c'era la sinergia che c'è oggi per combattere efficacemente il problema. Si continua a parlare dei genitori: danno uno scarso esempio, perché non possono insegnare le buone norme se loro per primi non le conoscono. Basta pensare a Whatsapp: viene usato malamente, soprattutto dagli adulti. Massettini afferma quindi che, se gli adulti sono indietro e non sanno usare la tecnologia o la usano peggio

dei ragazzi, questi ultimi perdono fiducia e non si aprono. Questo vale sia per i genitori che per gli insegnanti.

Massettini parla poi degli incontri che la Polizia Postale fa nelle classi: si parla di reati, e si cerca di far capire che la conseguenza a determinate azioni c'è, portando anche casi concreti.

A questo punto c'è stata la visione del video "Pericoli di Internet – reale e virtuale – dov'è Klaus?" In cui si vede una madre che, aprendo la porta di casa, si ritrova una serie di individui poco raccomandabili che chiedono dove siano i suoi figli, e lei senza problemi li chiama o indica a queste persone la loro stanza. Ad esempio, si vede un pedofilo che chiede della figlia, e la madre gliela chiama e la fa uscire come se fosse una cosa normale. Il senso di questo video è che, come nella vita reale i genitori avrebbero protetto i loro figli da persone del genere, la stessa cosa dovrebbe succedere su Internet.

Abbiamo visto anche un altro video, un trailer di 4 minuti circa di "Cuori connessi" in cui si raccontano due storie di due ragazze, una vittima di bullismo e una vittima di sexting, che sono riuscite comunque a reagire (anche se la ragazza vittima di sexting ha poi dovuto cambiare scuola) e a stare bene. Si sono visti poi esempi di interventi-video che la Polizia Postale fa vedere in classe, in cui ci sono delle domande a cui seguono delle risposte, e con i quali fanno parlare i ragazzi.

A questo punto ci sono stati più interventi: il primo a parlare è stato **Lauro Mengheri, presidente ordine degli psicologi per la Toscana**, che ha parlato dell'importanza della famiglia e della prevenzione. A seguire, è intervenuta **Letizia Vai, pedagogista CIAF (Centro Infanzia Adolescenza e Famiglia) del Comune di Livorno**, che ha parlato di come, dalle classi terze delle scuole secondarie di primo grado, si sia passati a lavorare sui bambini delle classi prime e poi, siccome ritenuti anche loro troppo grandi, siano passati a lavorare alle scuole primarie, giudicati dell'età giusta per poter lavorare sul tema della sicurezza in Rete, e sui loro genitori.

A questo punto c'è stata la visione di un video, in cui si vede una bambina di un anno che prima sfoglia e ingrandisce immagini con l'iPad, successivamente i genitori le danno una rivista cartacea e la bambina prova a sfogliare e ingrandire le foto come se fosse con l'iPad, ovviamente senza successo, e quindi si mette a piangere. Per lei, la rivista

cartacea è un iPad che non funziona. Questo significa che si dovrebbe comunque insegnare che esiste altro, oltre alla tecnologia.

Vai afferma che spesso gli adulti sono uno specchio e sono incoerenti sui loro figli: possono criticargli l'uso sbagliato di Internet quando sono loro i primi a farlo. Basta vedere che spesso i ragazzi sono disturbati dall'uso che i genitori fanno delle loro foto, condividendole su Facebook e in altri social. Per questo si dovrebbe ampliare lo spicchio sulla famiglia, lavorando con i genitori e i bambini sin da piccoli.

Per ultimo hanno parlato **Ettore Gagliardi, presidente UNICEF Livorno** e **Rita Franchi della Fondazione LEM**.

Terza relazione: "La rete come risorsa e il rischio del suo cattivo uso: educare per prevenire."

Parla Maria Antonella Galanti, docente di Pedagogia generale – Dipartimento di Civiltà e forme del sapere, Università di Pisa.

Anche Galanti inizia parlando dell'importanza della prevenzione, ma sposta il discorso dicendo che non si può dire bene o male di qualcosa che non si conosce. Secondo lei non si deve vietare, perché si rischia di fare come il frutto proibito dell'Eden.

Prima di criticare i ragazzi per il tempo che passano al computer, i genitori dovrebbero prima guardarsi per sè: ce ne sono molti, infatti, che sono sempre a guardare la televisione, eliminando i contatti umani. Nel 2008 è stato visto che, confrontando dei genitori e dei bambini di terza elementare in due condizioni (classe in silenzio e classe in condizione di caos), per gli adulti nel caos pensare non era fattibile, mentre per i bambini fare i compiti in silenzio o in situazione di caos non faceva differenza. Questo esempio Galanti lo ha fatto per dire che chiunque ha le proprie abitudini, e i genitori prima di criticare i propri figli (ad esempio quando viene detto "spegni tutto quando fai i compiti!") dovrebbero prima porsi delle domande.

A questo punto il discorso si sposta su un confronto tra presente e passato: in un contesto globalizzato, la rete è il mezzo comunicativo equivalente a quello di un contesto più piccolo. In altri termini, al giorno d'oggi una notizia si espande in tutto il mondo perché siamo in un contesto globalizzato, in passato invece la notizia si sarebbe sparsa solo nel paese dell'accaduto o al massimo in quelli vicini.

Si torna a parlare dei genitori: il problema del cyberbullismo è che, come nella pedofilia, i ragazzi non si confidano per paura di sentirsi dire dai genitori che la colpa è loro. I genitori dovrebbero capire il mondo dei ragazzi, magari raccontando ai propri figli ciò che facevano in gioventù: in questo modo potrebbero instaurare un rapporto di fiducia e complicità che permetterebbe una più facile apertura da parte dei figli.

La domanda che viene fuori a questo punto è: "Perché si ha paura?" Si ha paura perché non si conosce. Bisogna sapere usare la rete, altrimenti si rischia di fare come Frankenstein e il mostro, di cui ha perso il controllo.

Viene fatto a questo punto un altro esempio tra passato e presente, per dire che in un certo senso il virtuale è sempre esistito (ad esempio le favole delle nonne, non erano reali, ma c'erano). L'esempio è quello della piazza del paese, che si può benissimo mettere a confronto con la Home di Facebook: ad esempio passa una bella ragazza nella piazza, si fanno apprezzamenti, è come mettere like a una foto. Altro esempio, così come le persone nell'antichità si facevano ritrarre nei quadri eliminando alcuni difetti, così si fa oggi nelle foto usando Photoshop. Tutto questo per arrivare a una considerazione: ogni epoca ha i suoi mezzi, attraverso cui si esprimono le bellezze e le brutture della vita. Cose come la rete e tutto ciò che comporta in un certo senso sono sempre esistiti, anche se in altre forme: basta saperla usare.

Quarta relazione: "La rilevanza penale delle condotte di bullismo e cyberbullismo".

Parla Giuseppe Rizzo, sostituto Procuratore della Repubblica presso la procura di Livorno.

La domanda che viene posta è: Qual è la responsabilità penale del bullo?

Rizzo inizia elencando i punti che toccherà nel discorso:

- Chiarimento giuridico: cos'è il bullismo e cyberbullismo?
- Bullismo inquadrato dal punto di vista storico – giuridico
- Ruolo della storia in questa materia
- I reati che rientrano nel fenomeno del bullismo rientrano nel tribunale dei minorenni
- Quali sono i reati che compie il bullo? Cosa si attua nei confronti di questi soggetti?

- Tematica dell'introduzione di un reato autonomo che punisca questi comportamenti.

Il bullismo (e forme moderne) è un fenomeno che in qualche modo esiste da molto tempo: il termine non è giuridico, perché è un fenomeno sociale. È sempre importante andare a verificare quali sono i reati configurabili.
È importante sottolineare il modo di vedere di questo fenomeno da parte dei pubblici ufficiali. Esiste il bullismo anche tra gli adulti.
Nella storia del diritto e in generale (il bullismo sono una serie di comportamenti vessatori) è sempre esistito. Nell'epoca precedente c'erano metodi diversi, addirittura pene corporali. La scuola risolveva il problema in questi termini. Il problema tra minori era sottovalutato, come le violenze di genere. Un tempo, il marito aveva il potere di correggere il figlio o la moglie, così come esisteva l'attenuante per il diritto d'onore. Il punto è che l'atteggiamento nei confronti della violenza era sottovalutato, il bullismo era considerato semplicemente una ragazzata.
Sono poi aumentate le denunce anche per i reati fatti tra minori. Oggi è normale che ci si occupi di queste cose, prima era considerato tempo perso: non ci si occupava infatti di violenze familiari o tra ragazzi. Negli ultimi anni però ci sono stati notevoli passi avanti: addirittura la Polizia Postale è specializzata in questo campo. Il problema è che Internet consente di commettere reati senza comparire: materialmente, la vittima non può far niente. Fortunatamente, però, queste oggi sono attività criminali e vanno punite: è un'evoluzione positiva.
Il discorso continua con i reati. Rizzo spiega che gli atti di bullismo possono dare luogo a più ipotesi di reato: percosse e lesioni, lesioni aggravate, diffamazione (che è il reato tipico), minacce, stalking (introdotto come reato solo nel 2009, e ha fatto aumentare le denunce di chi è vittima di cyberbullismo), estorsione, violenza sessuale, accesso abusivo al sistema informatico.
Le sanzioni per reati di media o lieve entità sono minime, solo pecuniarie, mentre se sono gravi (stalking, estorsione, violenza sessuale) ci sono anche dai 5 ai 10 anni di carcere.

L’autore tipico è un minore, quindi c’è un problema di fondo: il problema esiste anche nelle scuole elementari e medie, ma i minori di 14 anni non sono imputabili. In quel caso, c’è la responsabilità civile dei genitori.

Su questo tema ci sono delle proposte di riforma sull’abbassamento della soglia per cui si è imputabili (ad esempio in Texas lo si è a 10 anni), ma questo contrasterebbe la Costituzione. Anche per i soggetti imputabili, l’art. 18 c.p. stabilisce che per i minori di 18 anni l’imputabilità non è presunta, deve essere accertata. Il tribunale dei minori per valutare l’imputabilità deve capire attraverso uno psicologo se il minore è capace di intendere e di volere. Se con la perizia non lo risulta, allora non è imputabile.

Bisogna comunque tener conto, afferma Rizzo, che nei Paesi dove le pene sono più aspre di quelle italiane, non ci sono stati risultati migliori.

Quello che più è utile per contrastare il fenomeno sono le misure cautelari. C’è però un problema giuridico: quando è stata introdotta la norma, sono state introdotte anche altre due norme (divieto di avvicinamento e allontanamento dalla casa familiare) concepite per gli adulti, ma non per i minori. Una cosa utile, secondo Rizzo, sarebbe quella di estendere per il 612 bis (stalking) la norma di divieto di avvicinamento anche nel codice minorile, e modificare la norma da “allontanamento dalla casa familiare” a “allontanamento dall’istituto”, e inserire anch’essa nel codice.

Per quanto riguarda l’introduzione di un reato specifico, Rizzo spiega che ciò comporterebbe uno stravolgimento del diritto penale, perché comprenderebbe molti reati già presenti. Essendo il “bullismo” un termine generico, si rischierebbe di inserire tutto.

Rizzo conclude dicendo che le scuole, in caso di bullismo, dovrebbero avvisare immediatamente la polizia ed evitare di effettuare un’indagine interna, e che comunque insegnanti e genitori possono fare molto.

La giornata si è conclusa qui.

3. Rischi e soluzioni

3.1 Cyberbullismo

3.1.1 Bullismo e cyberbullismo.

"*Il cyber-bullismo è una forma di prevaricazione messa in atto da una persona o da un gruppo contro una vittima. Avviene tramite tecnologie digitali e per essere tale occorre che sia prolungata nel tempo.*"[5]

Bullismo e cyberbullismo sono spesso confusi e in effetti hanno molto in comune essendo entrambi forme di violenza e di sopraffazione. Mentre le caratteristiche tipiche del bullismo tradizionale sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno, nel cyberbullismo intervengono anche altri elementi. Il cyberbullismo infatti si attua attraverso l'uso dei nuovi media (smartphone e tutto ciò che si può connettere ad Internet) e con l'allargamento degli effetti che questo comporta. Viene meno la violenza "fisica", ma con la presenza della componente digitale per la vittima c'è la possibilità di essere colpita 24 ore su 24 e in qualsiasi luogo si trovi. Questo significa essere in pericolo anche in casa propria, luogo che con il bullismo tradizionale è considerato sicuro. Altro fatto importante è che la diffusione del materiale tramite Internet non è controllabile, è a disposizione di tutti e rimane per sempre. Questo significa che, se per la vittima la situazione dovesse migliorare, le foto/video rimarrebbero comunque in circolazione. Inoltre, la componente della rete aggiunge un altro vantaggio al cyberbullo: la possibilità di rimanere anonimo, o comunque di non poter essere raggiunto fisicamente, il che gli conferisce una sorta di immunità.[6] Nonostante queste differenze, però, bullismo e cyberbullismo sono sempre più collegati: avviene molto spesso infatti che atti di bullismo reale vengano fotografati o filmati e diffusi sul web tramite social network, blog, forum, chat e molto altro.

3.1.2 Tipologie di Cyberbullismo

Il cyberbullismo è suddivisibile in più tipologie:[7]

[5] www.generazioniconnesse.it
[6] Manualesuperkids
[7] www.cyberbullismo.com in Willard, 2007a, 2007b, Pisano, Saturno, 2008

Flaming – Da flame, "fiamma", con questo termine si intende l'invio di messaggi violenti mirati a scatenare "battaglie" online tra due o più contendenti, per una durata temporale determinata dall'attività online condivisa. Può accadere sia nelle app di messaggistica online (Whatsapp, ad esempio) sia nei social network, come anche nei videogiochi online. In questi ultimi, di solito è preso di mira il principiante che, commettendo errori da inesperienza, diventa oggetto di discussioni aggressive.

Il divertimento sta nell'insultare il nuovo arrivato e far sì che quest'ultimo risponda in modo fortemente aggressivo alle provocazioni, alimentandole. Nonostante il flaming sia caratterizzato dall'anonimato (o comunque dall'irraggiungibilità fisica dei partecipanti), un flame prolungato, chiamato flame war, potrebbe causare un'aggressione vera e propria nella vita reale.

Harassment – Dal verbo inglese to harass, "molestare", consiste nell'invio di messaggi offensivi in un lungo arco di tempo e in modo ripetitivo tramite sms o telefonate (talvolta mute). La differenza con il flaming sta nella persistenza, infatti nell'harassment il comportamento aggressivo è reiterato nel tempo, e nell'asimmetria di potere tra il cyberbullo e la vittima. Si dice in questo caso che la vittima è in posizione one down[8], cioè subisce passivamente le molestie o prova senza successo a convincere il persecutore a porre fine alle aggressioni. Questa è un'altra differenza con il flaming, nel quale i messaggi venivano inviati con l'intento di rispondere alle provocazioni; nell'harassment i messaggi vengono inviati unicamente per far cessare i comportamenti molesti.

Può capitare di imbattersi nel fenomeno chiamato harassment con reclutamento volontario[9], cioè quando il cyberbullo coinvolge i propri contatti online che, pur non conoscendo la vittima, si prestano a partecipare alle aggressioni online.

Cyberstalking – Si può definire come un'evoluzione dell'harassment. Si parla di cyberstalking quando la vittima di harassment inizia a temere per la propria sicurezza a causa di messaggi particolarmente insistenti e intimidatori. Questo fenomeno si può riscontrare in relazioni fortemente conflittuali o in rapporti sentimentali interrotti.

In questo caso, il cyberbullo oltre alle minacce fisiche può diffondere materiale riservato della vittima in Rete.

[8] Watzlawick, Beavin, Jackson, 1971
[9] Pisano, 2008

Denigration – L'obiettivo del cyberbullo in questo caso è il danneggiamento della reputazione della vittima tramite diffusione online di pettegolezzi e/o altro materiale offensivo. Possono essere creati fotomontaggi nei quali si rende la vittima protagonista di scene sessualmente esplicite, oppure si può modificarne il viso o il corpo allo scopo di ridicolizzarla. Chi riceve il materiale o lo visualizza su internet è considerato spettatore: può essere passivo (nel caso si limiti a visualizzarlo) o attivo (nel caso in cui scarichi il materiale, lo segnali ad altre persone o lo commenti).

Impersonation – Si parla di questo fenomeno quando il cyberbullo riesce a violare l'account di qualcuno (ottenendo la password consensualmente oppure in altri modi) impersonandosi nella vittima e inviando messaggi con l'obiettivo di danneggiarla o metterla in pericolo.

Non è necessario però che il cyberbullo riesca ad entrare nell'account della vittima per essere considerato impersonation, basta anche che si crei un profilo falso con la foto del bersaglio, impersonandolo e parlando male di qualcuno.

Outing and Trickery – Con il termine outing si intende una forma di cyberbullismo attraverso la quale il cyberbullo, dopo aver salvato le confidenze o immagini private di un coetaneo, decide di pubblicarle online. Con il termine trickery, dall'inglese trick, "inganno", il cyberbullo riesce a convincere la vittima a condividere online informazioni imbarazzanti su sé stesso o un'altra persona, per poi diffonderli ad altri utenti della rete o minacciare di farlo.

Inizialmente quindi il rapporto tra cyberbullo e vittima è bilanciato, successivamente si dice che il cyberbullo assume una posizione one up.

Exclusion – Questo fenomeno si manifesta quando il cyberbullo decide di escludere volontariamente un coetaneo da un gruppo online (ad esempio una chat di gruppo su Whatsapp). Per indicare questa modalità, viene usato anche il termine bannare, dall'inglese ban, "bandire". Siccome ormai la popolarità di una persona si misura non solo in base agli amici che ha nella vita reale, ma anche in base a quelli che ha online, l'exclusion è visto come una grave offesa che mina la popolarità, e quindi il potere, della vittima.

Happy slapping – Dall'inglese "schiaffeggiamento allegro", è un fenomeno osservato per la prima volta nel 2004 in Inghilterra.[10] E' una forma di cyberbullismo recente, nella quale compare anche la componente del bullismo tradizionale. Si manifesta quando un ragazzo viene picchiato da un ragazzo o da un gruppo, mentre il resto delle persone filma il tutto con lo smartphone. Successivamente queste immagini o video finiscono in Rete alla mercé del popolo di Internet, facendo in questo modo partire la condivisione incontrollata del materiale che verrà anche commentato, votato, consigliato ad altri.

3.1.3 Prevenzione.

La prevenzione del cyberbullismo avviene sia da parte dei ragazzi che da parte dei genitori e insegnanti.

Per quanto riguarda i ragazzi, può capitare che agiscano da cyberbulli senza che se ne accorgano. L'importante è evitare di commentare o condividere materiale che possa risultare offensivo per qualcuno. Se dovesse capitargli di vedere materiale di questo genere, dovrebbero parlarne con un adulto e segnalarlo, e in caso anche parlarne con la vittima e aiutarla a reagire.

Altro concetto importante è quello di navigare responsabilmente: vivendo ormai in un mondo tecnologico nel quale contano sempre più i like alle proprie foto sui Social, i ragazzi dovrebbero imparare a condividere il giusto e non postare materiale privato, perché non si sa mai chi potrebbe impossessarsene e che uso potrebbe farne.

Pe quanto riguarda i genitori e gli insegnanti, invece, hanno il dovere di guidare i ragazzi nel mondo di Internet e insegnargli un concetto fondamentale: ciò che viene messo in Rete rimane per sempre e non se ne può controllare la diffusione. È importante quindi la privacy: va bene condividere foto e informazioni proprie, ma sempre con criterio.

Oltre alla privacy, ai ragazzi andrebbe trasmesso un sistema di valori basato sulla democrazia, il rispetto e contro la violenza: il cyberbullo approfitta infatti di un pubblico che a volte è spaventato e incapace di prendere una posizione.

Ultimo ma non per importanza, il dialogo: deve stabilirsi un rapporto di fiducia sia con i genitori che con gli insegnanti, in modo che se dovessero mai presentarsi problemi o

[10] www.ilcyberbullismo.it

situazioni particolari, il ragazzo si aprirebbe molto più facilmente e si potrebbe affrontare la situazione sin dall'inizio.

3.1.4 Come affrontare un cyberbullo.

Il problema va affrontato sia da parte dei ragazzi che da parte dei genitori e insegnanti.
Per quanto riguarda i ragazzi, inizialmente dovrebbero provare a bloccare i messaggi o a ignorarli: dopo un po' solitamente il cyberbullo smette, in quanto spesso cercano solo attenzione. In ogni caso dovrebbero comunque parlarne con un adulto oppure con un amico: è fondamentale non isolarsi, perché da soli non se ne esce. Se invece il ragazzo non se la sente di parlarne con qualcuno che conosce, sono stati creati dei siti web appositi, in cui sono presenti chat online e linee di ascolto gratuite.
Importante è anche salvare i messaggi o i post che vengono pubblicati: essendo il cyberbullismo un reato, saranno utili in caso di denuncia.
Per quanto riguarda i genitori e gli insegnanti il piano d'azione è simile. Se tra loro e il ragazzo si è creato un rapporto di fiducia allora sarà lui stesso a raccontare tutto, e a quel punto il ruolo degli adulti sarà quello di tranquillizzarlo e di fargli capire che niente è irreparabile: troveranno una soluzione insieme e il cyberbullo sarà punito.
Se invece il dialogo manca, ci sono comunque dei segnali che possono evidenziare il comportamento di un ragazzo vittima di cyberbullismo:

- Appare nervoso quando riceve messaggi;
- Sembra a disagio nell'andare a scuola o finge di essere malato;
- Riluttanza a condividere le informazioni su attività online;
- Rabbia o depressione inspiegabile dopo essere stato online;
- Mal di stomaco inspiegabile o mal di testa;
- Disturbi del sonno;
- Inspiegabile perdita o aumento di peso;
- Ideazione suicidaria o tentativi di suicidio.

Una volta capito che si tratta di cyberbullismo (riuscendo quindi anche a instaurare un rapporto con il ragazzo), la modalità d'azione è quella descritta sopra.

3.1.5 Aspetti legali

In Senato, a Maggio 2015, è stato approvato con voto unanime un disegno di legge assegnato alle commissioni riunite di Giustizia e Affari Sociali. Definisce il cyberbullismo, regola la rimozione dei contenuti offensivi dalla rete, stabilisce quando debba intervenire il Garante della privacy e regola l'ammonimento nel caso di reati commessi da minorenni, ma con età superiore ai 14 anni[11].

Il Ministro della Pubblica Istruzione, nel 30 Novembre 2007, ha emanato una circolare relativa al Cyberbullismo, di cui viene riportata una parte:

Gli studenti, i docenti o altri soggetti della comunità scolastica che vorranno scattare delle fotografie o effettuare registrazioni audio o video all'interno delle istituzioni scolastiche, con il proprio telefono cellulare o altri dispositivi, e successivamente utilizzare, divulgare, inviare i dati personali acquisiti sono obbligati a porre in essere due adempimenti:

***A** – si deve informare la persona interessata circa:*

- le finalità e le modalità del trattamento che si intende effettuare in relazione a tali dati;

- i diritti di cui è titolare in base all'art. 7 del Codice , quali, ad esempio, il diritto di ottenere la cancellazione o la trasformazione in forma anonima dei dati personali;

- gli estremi identificativi di colui che usa il telefono cellulare o altri dispositivi per raccogliere i dati.

***B** – deve acquisire il consenso espresso dell'interessato. Nel caso in cui il trattamento riguardi dati di tipo sensibile, occorre acquisire il consenso in forma scritta, fermo restando il predetto divieto di divulgare i dati sulla salute.*

L'inosservanza dell'obbligo di preventiva informativa all'interessato comporta il pagamento di una sanzione amministrativa che va da un importo minimo di 3.000 euro sino ad un massimo di 18.000 euro ovvero, in caso di dati sensibili o di trattamenti che comportino situazioni di pregiudizio, di grave detrimento anche con eventuale danno, la sanzione va da un minimo di 5.000 euro sino ad un massimo di 30.000 euro (cfr. art. 161 del Codice).

[11] www.senato.it – Fascicolo Iter DDL S. 1261 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo.

In alcuni casi basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale, in altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela). Ecco alcuni casi in cui è necessario segnalare all'Autorità Giudiziaria[12] (Circolare 30 Novembre 2007, Ministero della Pubblica Istruzione):

- *L'indebita raccolta, la rivelazione e la diffusione di immagini attinenti alla vita privata che si svolgono in abitazioni altrui o in altri luoghi di privata dimora (art. 615 bis codice penale);*
- *Il possibile reato di ingiurie, in caso di particolari messaggi inviati per offendere l'onore o il decoro del destinatario (art. 594 codice penale);*
- *Le pubblicazioni oscene (art. 528 codice penale);*
- *La tutela dei minori riguardo al materiale pornografico (art. 600-ter codice penale; legge 3 agosto 1998, n. 269)*

Attenzione:
Se l'autore del reato è un minorenne la competenza è del Tribunale per i minorenni e procede la Procura della Repubblica presso tale Tribunale.
Se l'autore è maggiorenne (ha compiuto 18 anni), la competenza è del Tribunale ordinario e procede la Procura della Repubblica presso tale Tribunale.

3.2 Sexting

3.2.1 Definizione

"Il termine sexting deriva dall'unione di "sex" (sesso) e "texting" (pubblicare testo) e indica lo scambio o la condivisione di testi, video o immagini sessualmente espliciti (via cellulare o tramite Internet) che spesso ritraggono se stessi. Il sexting è un fenomeno ampiamente diffuso tra gli adolescenti."[13]

Ormai, Internet fa parte della vita quotidiana di ognuno di noi, in particolar modo della maggioranza dei giovani. I media svolgono un ruolo importante nella formazione della

[12] www.informagiovani-italia.com/bullismo_reato.htm
[13] www.generazioniconnesse.it

loro identità, dei legami di amicizia o di amore e, quindi, anche della sessualità. Se esiste il *sexting* non c'è da stupirsi o allarmarsi: è una cosa normale, se si considera che i ragazzi attraverso la Rete scoprono e sperimentano la propria sessualità. La cosa cambia quando, dal semplice invio di una foto al proprio partner, si passa alla condivisione online.

3.2.2 Rischi

Può capitare, spesso dopo un litigio, che per vendetta il partner carichi online il materiale multimediale inviatogli dalla vittima. Questo momento si può definire come un punto di non ritorno, in quanto il materiale una volta online è impossibile prevedere dove e in che mani finirà; oltretutto non è mai cancellabile totalmente, nemmeno a situazione risolta: è probabile che qualcuno che non sia la vittima o l'autore del gesto salvi le foto o i video e li ricondivida, non mettendo mai fine alla storia. Questo gesto rischia di causare danni sia a livello psicologico che di immagine pubblica della persona ritratta.

Attualmente si sta ancora indagando sulle conseguenze del *sexting*, ma ragionevolmente si ritiene che siano le seguenti[14]:

- Diminuzione dell'autostima della vittima;
- Insorgenza di episodi depressivi o di sintomi ansiosi;
- Paura;
- Frustazione;
- Problemi scolastici e/o familiari;
- Idee suicidarie o vera e propria messa in atto.

Il *sexting* può essere collegato anche al fenomeno del *cyberbullismo*, in quanto le foto e i video messi online possono essere usati per ridicolizzare e perseguitare la vittima.

Un altro rischio che corre chi condivide le proprie foto in Rete (o comunque il protagonista di determinato materiale) è quello di attirare malintenzionati, incentivati ad accedere ai loro dati personali o a tentare un adescamento.

[14] www.azzurro.it

Ultimo ma non per importanza, far girare certe foto può essere considerato diffusione di immagini pedo-pornografiche: non per chi le ha fatte, ma per chi le ha condivise e rese pubbliche.

3.2.3 Prevenzione

Per prevenire il presentarsi di situazioni spiacevoli, è importante che sia i ragazzi che i genitori adottino determinati accorgimenti.

Per quanto riguarda i genitori, un primo modo per affrontare probabili situazioni scomode è quello di informarsi. Non sempre gli adulti conoscono il fenomeno oppure tendono a sottostimarlo. Una volta informati, dovrebbero instaurare un dialogo con i propri figli, parlando di sessualità, dei cambiamenti del corpo e dell'identità sessuale: in questo modo i ragazzi potrebbero aprirsi più facilmente, parlando anche del *sexting* in particolare. L'argomento deve essere affrontato in maniera tranquilla, altrimenti i ragazzi potrebbero chiudersi in sé stessi per paura o vergogna.

Se capitasse a un genitore di scoprire sullo smartphone del figlio foto sessualmente esplicite che lo ritraggono, dovrebbe assicurarsi che il figlio sia consapevole dei rischi; allo stesso modo, se dovesse trovare immagini che ritraggono un altro adolescente, dovrebbe assicurarsi che non la invii a nessun altro. Queste ultime due situazioni possono essere sfruttate per capire perché il ragazzo invii proprie foto/video. È possibile che sia dovuto alla ricerca di feedback sul proprio corpo, oppure per l'avvio/mantenimento di una relazione.

Altro fatto importante è informare i propri figli sulle conseguenze di questo tipo di comportamenti: i genitori dovrebbero insegnargli che tutto ciò che finisce in Rete è per sempre e che possono essere accusati di produzione e distribuzione di materiale pedopornografico.

Per quanto riguarda i ragazzi, invece, sarebbe meglio se non accettassero né mandassero foto/video sessualmente allusivi, che ritraggano loro stessi o amici, in quanto potrebbero essere accusati del reato di produzione o distribuzione di materiale pedopornografico. Dovrebbero anche pensare al danno psicologico, alle conseguenze emotive e sulla reputazione propria o della persona ritratta nelle foto che potrebbero derivare se quel materiale finisse nelle mani di chiunque (compresi sconosciuti o malintenzionati).

Altro comportamento da adottare è evitare di diffondere materiale di sexting ad altre persone in caso di ricezione, e di parlarne con i genitori o di un adulto.

3.2.4 Cosa fare in caso il materiale venga diffuso in Rete

Il tempo di azione è fondamentale: prima si agisce, meno tempo avrà il materiale per diffondersi. I ragazzi dovrebbero parlare immediatamente con qualcuno di cui si fidano, che sia un adulto (genitori, insegnanti) o un coetaneo per avere un punto di vista. Se dovessero vergognarsi, esistono dei siti web creati appositamente per queste situazioni, come il Safer Internet Center italiano che mette a diposizione due canali a cui rivolgersi: la linea di ascolto gratuita e la chat.

3.2.5 Aspetti legali.

La Corte di Cassazione, con sentenza del 21/03/2016 n. 11675 approfondisce la questione relativa alla cessione online di materiale pedopornografico.

Il caso vedeva una minorenne che, dopo essersi scattata immagini sessualmente esplicite, le aveva inviate ad altri minorenni di sua conoscenza. Questi ultimi, però, ad insaputa della protagonista e senza quindi il suo consenso, condividevano gli scatti con altre persone. I giudici del Tribunale per i Minorenni dell'Aquila, con sentenza del 10/11/2014 di *"non luogo a procedere nei confronti dei ragazzi perché il fatto non sussiste"* (Corte di Cassazione, Sezione III penale - Sentenza 21 marzo 2016, n. 11675 Data udienza 18 febbraio 2016), ritennero che la condotta non fosse punibile poiché le immagini erano state effettuate dalla minorenne stessa senza l'intervento di terze persone. Il Procuratore della Repubblica, però, presentò ricorso in Cassazione ritenendo che l'attività vietata dalla norma riguarda la diffusione "*del materiale raffigurante un minore tout court, indipendentemente da chi e come l'abbia prodotto"* (Corte di Cassazione, Sezione III penale - Sentenza 21 marzo 2016, n. 11675 Data udienza 18 febbraio 2016). La Suprema Corte, però, ha sostenuto che l'art.600-*ter* comma 1 c.p. (richiamato dai successivi commi 2, 3 e 4) disciplina "*esclusivamente quel materiale formato attraverso l'utilizzo strumentale dei minori ad opera di terzi"* (Corte di Cassazione, Sezione III penale - Sentenza 21 marzo 2016, n. 11675 Data udienza 18

febbraio 2016). Quindi, la cessione di materiale pedopornografico a terzi è punibile "*a condizione che lo stesso sia stato realizzato da soggetto diverso dal minore raffigurato*" (Corte di Cassazione, Sezione III penale - Sentenza 21 marzo 2016, n. 11675 Data udienza 18 febbraio 2016), dal momento che la normativa distingue l'utilizzatore dal minore utilizzato.

Pertanto, per essere punito, l'autore della condotta deve essere soggetto altro e diverso rispetto al minore da lui utilizzato[15].

3.3 Adescamento online

3.3.1 Definizione

Per adescamento online, o *grooming*, si intende il tentativo, da parte di una persona malintenzionata o di un pedofilo, di avvicinare un bambino o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della Rete. L'intenzione è di iniziare una relazione o avere incontri dal vivo.[16]

La Rete ha eliminato i confini geografici, e questo permette molti scambi e contatti tra persone. Questo possiamo classificarlo come uno dei grandi traguardi di Internet, ma dobbiamo vedere anche l'altro lato della medaglia che comprende tutta una serie di persone con profili falsi che navigano in Rete alla ricerca di contatti con bambini e ragazzi, i pedofili.

Il pedofilo è in genere un criminale piuttosto lucido che sa come manipolare i ragazzi attraverso la comunicazione online. E' anche un profondo conoscitore del mondo infantile e adolescenziale, e questo lo avvantaggia poiché sa come ottenere confidenze da utenti minori della Rete[17].

3.3.2 Come avviene l'adescamento?

L'adescamento ha inizio nel momento in cui l'adulto mostra interesse nei confronti del minore, con l'intenzione di creare un legame che è il presupposto per arrivare a incontri a sfondo sessuale nella vita reale. Inizialmente l'adulto mente sulla propria età, conversa

[15] www.diricto.it
[16] www.azzurro.it
[17] www.poliziadistato.it

su temi di interesse della vittima, si pone come confidente e grande amico. Il processo per ottenere la fiducia del minore è molto lento, e può durare diversi mesi.
A volte, però, le richieste di confidenze sessuali arrivano subito, altre volte invece sono precedute da dichiarazioni di trasporto sentimentale. La richiesta di immagini osé è il passo successivo, a cui segue la richiesta di un incontro reale.
Il pedofilo comunque, in genere, prima di arrivare a ciò cerca un contatto sempre più isolato col bambino in modo graduale, cercando di ottenere informazioni personali (numero di cellulare, indirizzo della scuola frequentata), fino ad arrivare ad argomenti riguardanti la sfera sessuale. Dopo l'abuso, l'obiettivo del pedofilo è di ottenere il silenzio della vittima attraverso il ricatto e l'abuso psicologico, facendo credere ad esempio che quanto avvenuto sia normale, o che sia stata colpa del minore, o peggio si minaccia di mostrare a genitori e amici o condividere su Internet immagini/video che lo ritraggono.

3.3.3 Prevenzione

Per i genitori. I genitori dovrebbero informarsi e avere un minimo di conoscenza informatica: solo così possono prevenire certi rischi. Anche un dialogo con il proprio figlio è importante, in questo modo si può capire se sono in grado di riconoscere un pericolo e, soprattutto, si aprirebbero più facilmente in caso di situazioni spiacevoli.
Nel caso di bambini più piccoli, è utile usare dei software di protezione per monitorare l'uso che viene fatto di Internet; oltre a ciò, il computer dovrebbe trovarsi in una posizione comune all'interno della casa, così che i genitori possano monitorare tutte le attività in Rete del proprio figlio.
Importante è insegnare ai propri figli a non fornire troppi dati personali, non si sa mai chi potrebbe usarli e per quale scopo; così come evitare di condividere foto sessualmente esplicite o imbarazzanti, dato che ciò che finisce su Internet non è cancellabile.
Se non dovesse esserci abbastanza dialogo con i propri figli, i segnali da prendere in considerazione sono i seguenti:

- Uso eccessivo del computer o dello smartphone, cambio rapido della pagina quando vengono scoperti;
- Nervosismo o aggressività quando non possono usare computer o smartphone;

- Comportamento più sessuato nel modo di fare, di vestirsi e nel linguaggio;
- Auto-isolamento;
- Regali ricevuti da qualcuno che non conosci: in particolare webcam o smartphone.

Per i ragazzi. I consigli per i ragazzi sono simili a quelli per i genitori: deve esserci dialogo, non devono condividere foto osé di sé stessi né troppe informazioni personali.
Se dovessero essere contattati da una persona sospetta, devono salvare immediatamente la conversazione (uno screenshot è sufficiente) per eventuali denunce; inoltre devono ricordarsi che molte chat o social danno la possibilità di bloccare i contatti.

3.3.4 Aspetti legali.

Il delitto di adescamento di minorenni è punito con la reclusione da uno a tre anni[18], è stato recentemente introdotto nel nostro codice penale (art. 609 *undecies* c.p. - introdotto dalla L. n. 172 del 01/10/2012) e non deve essere necessariamente andato a buon fine per essere condannato, è sufficiente anche solo il tentativo da parte di un adulto di conquistare la fiducia di un bambino o di un adolescente per fini sessuali.
Inoltre, il decreto legislativo del 4 marzo 2014 n.39, che recepisce la Direttiva 2011/93/UE, ha introdotto modifiche al codice penale in tema di reati concernenti l'abuso e lo sfruttamento sessuale dei minori: ha inasprito le pene già previste e ha introdotto nuove aggravanti.

3.4 Dipendenza

3.4.1 Definizione

La dipendenza da Internet può essere una vera e propria sindrome: riguarda ragazzi e ragazze che non riescono a farne a meno e, privati della Rete, provano un forte disagio che non attenuano in nessun altro modo. Patologia o meno, un abuso di Internet e delle tecnologie è sempre negativo.

[18] Il delitto di adescamento di minorenni, ART. 609-*UNDECIES*

Internet dovrebbe rappresentare un'attività di contorno rispetto a quelle del mondo reale, come coltivare hobby, fare sport o divertirsi con gli amici. In molti casi però questo non accade e la Rete assume un ruolo "sostitutivo", rappresentando quindi un problema.
Se il concetto di dipendenza inizialmente era usato per descrivere una dipendenza fisica verso una sostanza, recentemente è stato applicato all'uso eccessivo di Internet. È stata definita **internet-dipendenza**, **retomania** o **Internet Addiction Disorder (I.A.D.)**, termine coniato dallo psichiatra americano Ivan Goldberg nel 1995, prendendo come modello di riferimento il gioco d'azzardo patologico[19].
I principali sintomi individuati come caratteristici dell'I.A.D. sono i seguenti, e sono generici per tutte le dipendenze da Internet:

- Bisogno di trascorrere un tempo sempre maggiore in rete per ottenere soddisfazione;
- Marcato disinteresse per altre attività che non siano Internet;
- Necessità di accedere alla rete sempre più frequentemente o per periodi più prolungati e, in caso di sospensione o diminuzione dell'uso della Rete, sviluppo di ansia, depressione e pensieri ossessivi su cosa accade online;
- Impossibilità di interrompere o controllare l'uso di Internet, nonostante la consapevolezza che questo può comportare o sta comportando problemi.

Oltre a quelli sopracitati, esistono altri problemi che si manifestano nell'individuo che diviene dipendente dalla rete, e sono:

- Ritiro dalla vita sociale: isolamento dagli amici, abbandono dello sport;
- Sovraffaticamento per la mancanza di ore di sonno;
- Crollo del rendimento scolastico;
- Manifestazione di un'assoluta dedizione per un particolare sito o videogioco;
- Presenza di veri e propri sintomi fisici come tunnel carpale, dolori diffusi a collo e schiena, problemi alla vista;
- Mancanza di igiene;
- Aumento dello stress;
- Aumento di peso.

[19] www.benessere.com

Vi sono poi tre tappe principali nello sviluppo dell'I.A.D.[20]:

- Tolleranza: attenzione continua e ossessiva verso gli strumenti tecnologici e la navigazione;
- Astinenza: nascita di sensazioni di malessere, disagio quando si è scollegati. Perdita del senso di confine tra Sé reale e Sé virtuale;
- *Craving* o tossicomania: bisogno compulsivo e irrefrenabile di connettersi. Se non soddisfatto causa intensa sofferenza psichica e fisica. Si arriva a percepire il mondo reale come un ostacolo all'esercizio della propria illusoria onnipotenza virtuale.

3.4.2 Tipologie

Esistono diversi tipi di dipendenza: cybersessuale, shopping compulsivo online, gioco d'azzardo, dipendenza da videogiochi online e cyber-relazionale. Le più comuni tra i giovani sono queste ultime tre.

Gioco d'azzardo.

Il gioco d'azzardo, o *gambling*, risulta essere un fenomeno in crescita tra i più giovani. Consiste nello scommettere denaro sul futuro esito di un evento. Nonostante però il gioco d'azzardo sia consentito solo ai maggiori di 18 anni (così come le scommesse sul web), secondo quanto emerge dall'ultima Indagine nazionale sulla Condizione di Infanzia e Adolescenza realizzata da Telefono Azzurro in collaborazione con Eurispes (2012), il 23,3% dei bambini ha giocato a soldi, e il 39% degli adolescenti dichiara di aver giocato d'azzardo.

Videogiochi online.

Ad oggi, il mercato dei videogiochi online sta vivendo un periodo di massimo boom economico: RPG (Role-Playing Game, gioco di ruolo), Sparatutto (FPS – First Person Shooter, TPS – Third Person Shooter), giochi di strategia, MMORPG (Massively Multiplayer Online Role-Playing Game) e molte altre tipologie; ce n'è per tutti i gusti e si può giocare su console (Playstation, XBOX, Wii), su smartphone o su PC. Quelli maggiormente usati sono i MMORPG, cioè giochi di ruolo in cui è possibile connettersi simultaneamente da tutte le parti del mondo e a qualsiasi ora. Il più famoso è World of

[20] www.centromoses.it

Warcraft (abbreviato WoW), sviluppato dalla Blizzard Entertainment, ed è un fantasy tridimensionale[21].

Nella dipendenza da videogiochi (soprattutto di ruolo, in cui il giocatore viene impersonato da un avatar), il soggetto si relaziona con altri utenti attraverso un personaggio virtuale, a volte già preimpostato, altre volte invece viene creato in modo da rappresentare chi lo gioca. Questo personaggio ha bisogno di aumentare di livello e migliorare quindi le proprie abilità, ed è una fase che richiede molto tempo (da qualche ora a giorni interi) e spesso anche interazioni con altri personaggi, con cui l'utente comunica attraverso chat.

L'ambiente è quindi quello di una vera e propria comunità virtuale, costituita da gruppi (*gilde*), in cui ogni membro ha un determinato ruolo. Più una persona si immedesima nel personaggio, più è probabile che il mondo virtuale venga idealizzato (così come le relazioni nate e vissute all'interno dello stesso), sostituendo la realtà e favorendo l'alienazione[22].

Cyber-relazionale.

Consiste nell'instaurare relazioni esclusivamente – o quasi – attraverso il web. Di solito le persone affette da questo tipo di dipendenza trascorrono la stragrande maggioranza del loro tempo nelle cosiddette Chat Room, oppure all'interno di Social Network o servizi di Instant Messaging. Proprio i Social Network sono diventati parte integrante della vita di moltissime persone, ma non bisogna confondere l'abitudine ad utilizzarli con la dipendenza da essi. L'utilizzo ossessivo di Facebook e simili, in quest'ultimo caso, non rappresenta più un mezzo per condividere e comunicare con persone reali che si conoscono (o si vogliono conoscere) ma diventa il fine della gratificazione: le relazioni reali diventano meno importanti, vengono limitate o addirittura interrotte, e le uniche gratificanti diventano quelle instaurate via Internet.

[21] www.istitutobeck.com
[22] www.escteam.net

3.4.3 Prevenzione e cura

Un buon metodo per prevenire la dipendenza da Internet è quello, da parte dei genitori, di imporre dei limiti d'uso; allo stesso tempo è importante proporre al ragazzo alternative reali alla vita online, come sport, hobby o viaggi.

Per quanto riguarda la cura, è nato al Policlinico A. Gemelli di Roma (in collaborazione con la Facoltà di Medicina e Chirurgia dell'Università Cattolica) un centro multidisciplinare per aiutare bambini e adolescenti preda della rete, chiamato Centro Pediatrico Interdipartimentale per la Psicopatologia da web. Può essere un'ottima soluzione, ed è così descritto dal Prof. Tonioni dell'Istituto di Psichiatria dell'Università Cattolica del Sacro Cuore: "*Il Centro, il primo in Italia che integra discipline diverse nello stesso percorso clinico, nasce dalla collaborazione tra l'Area Neuroscienze e l'Area Pediatrica del Policlinico A. Gemelli, per la presa incarico di un numero crescente di patologie legate alla grande diffusione di internet e delle applicazioni digitali*", mentre il Prof. Eugenio Mercuri, Direttore dell'Istituto di Psichiatria e Direttore dell'UOC di Neuropsichiatria Infantile - Fondazione Policlinico Universitario A. Gemelli, conclude dicendo che, per il modo in cui è stato ideato, *"rappresenterà un'esperienza pilota in grado di affrontare il problema delle dipendenze da rete a 360 gradi, riuscendo a coprire non solo gli elementi psicologici legati alla dipendenza ma anche le ripercussioni a livello fisico e cognitivo. Per la prima volta si offrirà una presa in carico completa aiutando i ragazzi e le loro famiglie nell'affrontare tutte queste problematiche."*[23] Il Centro comprende:

- Un ambulatorio per la Dipendenza da Internet e Cura-Prevenzione Cyberbullismo;
- Gruppi di Riabilitazione e di Sostegno;
- Un ambulatorio di Pediatria;
- Un ambulatorio di Neuropsichiatria infantile.

In totale, al centro sono presenti 3 psicologi, 3 psicoterapeuti e medici specialisti.

In tutto il mondo ci sono diversi modi di affrontare la dipendenza da Internet, come racconta il Prof. Tonioni in un'intervista di UniromaTv: *"Negli Usa i pazienti sono obbligati a curare una gallina: un animale ipercinetico. Diverso dal computer che è*

[23] www.policlinicogemelli.it

immobile. In Cina sono picchiati, ci sono stati anche due morti. In Olanda li portano a passeggiare nella natura". Al Gemelli invece la terapia consiste in due incontri settimanali: uno individuale e uno in gruppo. Spesso, però, all'incontro in gruppo si giunge col tempo: i ragazzi che vanno in ambulatorio infatti non sono più abituati né al contatto visivo né al confronto diretto. Tonioni racconta infatti che "*due ragazzini si sono seduti accanto per diverse sedute senza mai guardarsi, ma fissando la psicologa come fosse uno schermo. Dopo sei mesi, giocavano a carte."* Oltre alle sedute per i ragazzi, ci sono anche quelle per i genitori, in cui vengono dati consigli su come comportarsi. Inoltre, siccome qualsiasi dipendenza è sempre sintomo di problemi più profondi, la terapia deve necessariamente coinvolgere tutta la famiglia. Capita infatti che alla base della dipendenza dei figli ci siano questioni irrisolte tra i genitori: c'è bisogno quindi di un confronto, che è la cura migliore: si deve parlare, capire, fare piccoli passi insieme[24].

3.5 Phishing

3.5.1 Definizione

Il phishing (dall'inglese *fishing*, "pescare") è una truffa realizzata sulla rete Internet, che ha lo scopo di carpire informazioni riservate e sensibili come username, password, numeri di conto corrente. Non vengono utilizzati virus, spyware o malware, ma email sotto forma di messaggi di spam, con caratteristiche molto simili ai messaggi degli istituti bancari, postali o servizi di pagamento online[25].

3.5.2 Le fasi di un attacco di phishing

Un attacco di phishing si articola in quattro fasi:

- **Invio di falsi messaggi di posta elettronica da parte del truffatore**. Usando una *botnet* (rete di computer controllata a distanza da un hacker) vengono inviate decine di migliaia di email che simulano, nella grafica e nel contenuto, comunicazioni da parte di un istituto bancario, postale o di qualsiasi altra istituzione nota all'utente;

[24] www.huffingtonpost.it
[25] www.commissariatodps.it

- **Ricezione del messaggio**. Questo messaggio informa l'utente simulando situazioni che potrebbero verificarsi realmente, ad esempio la scadenza di una password, il rinnovo della carta prepagata o di credito, problemi a conti online. Nel messaggio si trova un link su cui l'utente deve cliccare per risolvere il problema.
- **Accesso al sito fasullo**. Il link però rimanda a un sito ospitato su di un server controllato dal phisher, che riproduce le sembianze del portale ufficiale.
- **Ricezione delle credenziali**. Una volta effettuato il login sul sito-copia, i dati vengono archiviati nel database del server del truffatore. Può accadere, inoltre, che visitando il portale si sia infettati da trojan horse o malware di vario tipo: in questo caso lo scopo è prendere possesso di nuovi computer così da arricchire il parco macchine della botnet[26].

3.5.3 Come riconoscere un tentativo di phishing

Per riconoscere un tentativo di phishing è necessario prestare molta attenzione ai messaggi di posta che si ricevono e una buona dose d'intuito, dato che i messaggi sembrano provenire da servizi web solitamente utilizzati e sono contraffatti quasi alla perfezione.

Solitamente, i tentativi di phishing contengono messaggi allarmanti, ad esempio "Verifica il tuo account" o "Se non rispondi il tuo account verrà chiuso in 48 ore", invitano a inserire informazioni personali su portali esterni e sono scritti in un italiano poco corretto. I messaggi di phishing, infatti, sono scritti in inglese e tradotti con strumenti web, quindi raramente la forma del testo sarà corretta.

3.5.4 Come difendersi dal phishing?

Tutti i metodi per difendersi dal phishing sono basati sul buon senso. Innanzitutto, si deve pensare che nessuna istituzione seria chiederà mai i dati personali di un utente tramite email. Si deve controllare poi che l'indirizzo del mittente e il link corrispondano

[26] www.fastweb.it

al sito web ufficiale e non contengano qualche errore di battitura: questo perché una delle tecniche più usate è quella di utilizzare url civetta, dove la differenza tra l'indirizzo ufficiale e quello fasullo è di una sola lettera (paipal.com anziché paypal.com, ad esempio). Per avere la certezza che il proprio account non corra rischi, è bene usare la pagina di login usuale, evitando di accedere tramite il link presente nel messaggio di posta elettronica.

Con il crescere dei tentativi di attacchi phishing, i provider di posta elettronica hanno dotato i loro prodotti di filtri antispam e antiphishing. Non sempre però questi riescono a rintracciare le email truffaldine: per questo bisogna comunque fare molta attenzione.

Google Safe Browsing è un sistema di sicurezza messo a punto da Google per provare ad estirpare il phishing direttamente dalle radici. Vengono analizzate le pagine web alla ricerca di programmi o script pericolosi, ogni URL infetto viene registrato nel database di Google ed entra a far parte di un Indice dei siti proibiti, restando virtualmente inaccessibile. Agli utenti è data la possibilità di verificare la sicurezza di un sito visitando la seguente pagina: https://www.google.com/transparencyreport/safebrowsing/diagnostic/index.html

3.6 Virus, trojan horse, malware

Virus, trojan horse e malware sono oggi diffusissimi. Questi software, a volte non più grandi di poche righe di codice, sono capaci di diffondersi come fossero dei virus biologici. Il primo virus della storia è datato 1971.

3.6.1 Definizione

Per virus, trojan e malware si intendono quei programmi creati con l'intenzione di causare danni a un computer o un sistema informatico rendendolo inutilizzabile, oppure trafugandone i dati presenti all'interno del disco rigido. In particolare, il malware (dall'unione delle parole inglesi *malicious* e *software*, "programma malvagio") è un programma creato con l'intenzione di danneggiare macchine o utenti. Sotto questa definizione abbiamo diverse categorie.

3.6.2 Categorie di malware

- **Virus.** Tipologia di malware che ha bisogno di un altro software per funzionare e replicarsi. Si diffonde copiandosi all'interno di altri programmi così da essere eseguiti ogni volta il file o programma infetto è aperto. La loro trasmissione avviene tramite spostamento di file infetti da un computer all'altro per opera degli utenti.
- **Worm.** Parola inglese che significa "verme". Questa categoria è capace di sopravvivere e diffondersi anche senza infettare un secondo programma. Modificano il sistema operativo della macchina ospite, così da essere eseguiti automaticamente all'avvio del computer e diffondersi attraverso internet. Di solito sono quasi inoffensivi: hanno lo scopo di rallentare il funzionamento della macchina ospite.
- **Trojan horse.** Prendono il nome dallo stratagemma usato per entrare nella città di Troia e ne imitano le funzioni. Un trojan horse è caratterizzato da diverse forme di disturbo: può far comparire *pop up* nel corso della navigazione web, cancellare file dalla memoria, trafugare informazioni e favorire la diffusione di altri malware. Può anche creare un accesso illegale all'interno del sistema informatico ma, a differenza di virus e worm, è l'utente stesso a scaricarlo e installarlo sulla propria macchina. Per questo, si nasconde all'interno di software "legittimi" e viene scaricato con loro.
- **Adware.** Software pubblicitari, mostrano all'utente pubblicità mentre naviga in rete o usa un programma gratuito. A parte il fastidio, non sono pericolosi: lo diventano dal momento in cui sono legati a degli spyware e iniziano a tracciare le abitudini online degli utenti e a comunicarle a server remoti.
- **Backdoor.** Come i trojan, creano varchi nel sistema di difesa di un computer e consentono un accesso non autorizzato alle risorse della macchina su cui sono in esecuzione.
- **Spyware.** Utilizzati per trafugare informazioni dal sistema su cui è installata. I dati vengono poi inviati verso server centrali, dove sono usati per gli scopi più disparati: dalle ricerche di marketing al furto d'identità, passando per prelievi non autorizzati da conti correnti bancari.

- **Ransomware.** Sono una delle ultime evoluzioni dei malware. La loro forma più conosciuta è quella dei *cryptolocker*, e hanno rappresentato una delle peggiori minacce informatiche del 2014. Sono software che prendono il controllo della macchina su cui sono installati, e ne bloccano il funzionamento crittografando tutti i dati presenti all'interno dell'hard disk. Se l'utente vuole tornare in possesso del suo computer e dei dati contenuti al suo interno è costretto a pagare un riscatto (dall'inglese *ransom*).
- **Bot.** Abbreviazione di *robot*, è un processo automatizzato che interagisce con altri servizi di rete. Possono essere usati sia per scopi leciti (*web crawler*) sia per scopi illeciti (*botnet*) al comando di uno o più hacker. Reti di questo genere possono essere utilizzati per gli scopi più vari: dagli attacchi DDoS alla diffusione di spam su larga scala.
- **Rootkit.** Hanno lo scopo di nascondere, sia all'utente che al software antivirus, la presenza di altri file o programmi. Sono utilizzati per nascondere virus, trojan horse o worm e favorirne così la diffusione.
- **Keylogger.** Hanno la capacità di registrare tutto ciò che un utente digita su tastiera, così da rendere possibile il furto di password e altre informazioni sensibili.

Esistono anche i malware per dispositivi mobili: sono travestiti da app e sono presenti sia nell'App Store sia nel Google Play Store, e si comportano come i malware per pc.

3.6.3 Come difendersi dai malware

La soluzione più utile, sia per prevenire che per rimediare, è quella di installare un anti-virus e un anti-malware valido. Se invece si desidera rimuovere le infezioni manualmente, è sufficiente una ricerca su Google: si troveranno molti modi per riconoscere e rimuovere i malware. Se preferisce, però, il proprietario del computer infetto può affidarlo a un esperto e far risolvere la questione a lui.

4. I prodotti

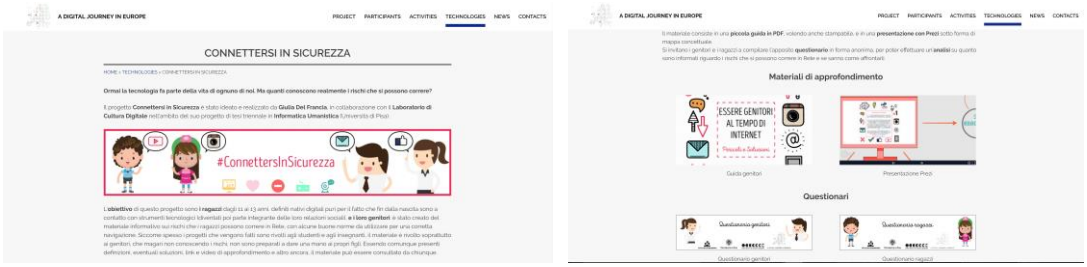
L'idea alla base dei prodotti creati è quella di informare genitori, ragazzi e chiunque altro ne abbia bisogno riguardo l'argomento della sicurezza in rete.

Guardando i progetti fatti dalla scuola, ho notato che solamente uno era rivolto parzialmente ai genitori, quindi ho pensato di produrre del materiale rivolgendomi più che altro a loro, in quanto è possibile che non conoscano la terminologia usata nel questionario e quindi potrebbero non capire le domande. Anche ascoltando i vari relatori alla giornata "Cyberlivorno", a cui ho partecipato, si parla anche dei genitori ma per il momento i progetti fatti sono rivolti solo a studenti e docenti. Essendo materiale informativo, comunque, è adatto a tutti, perché sono presenti definizioni e consigli su come affrontare i rischi che si possono incontrare in Rete e molto altro.

Per quanto riguarda i genitori c'è da aprire una parentesi. Essendo loro a crescere i propri figli e comunque appartengono a loro i primi strumenti tecnologici che i bambini vedono fin dalla nascita, è importante che i genitori, per primi, sappiano come usarli e conoscano i rischi che possono correre in Rete, in modo da insegnare ai propri figli come usare Internet in modo responsabile. Se sono loro i primi a sbagliare, di conseguenza anche i figli useranno la Rete ignorandone i rischi, ed è possibile che in caso di problemi preferiscano tacere perché la considererebbero una loro colpa.

Sono stati creati due prodotti: una piccola guida e una presentazione con Prezi, creata in modo da rappresentare una mappa concettuale dell'argomento, corredata di link e video di approfondimento. Il materiale è stato creato, oltre per dare solo un'infarinatura generale in caso non si conosca l'argomento, anche per unirlo al questionario, presentando i concetti che vi compaiono.

Oltre alla guida e alla presentazione ci sono anche due questionari, uno per i ragazzi e uno per i genitori, che saranno caricati nella sezione "Technologies" del sito *A Digital Journey* insieme alla guida e alla presentazione. Successivamente, il link sarà inserito all'interno del sito dell'Istituto Comprensivo "G. Marconi" di Venturina Terme (LI), in modo che i ragazzi e i genitori possano leggere il materiale e compilare i questionari, e successivamente controllarne i risultati.



Screenshot della pagina

I materiali caricati in *A Digital Journey* rimarranno disponibili per chiunque vorrà utilizzarli (o semplicemente dargli un'occhiata), così come i questionari rimarranno aperti. La guida è fatta in modo da poter essere anche stampata, oltre ad essere visualizzata in PDF, in modo da poter, in caso, essere divulgata anche in forma cartacea se dovesse esserci bisogno. Link al sito:

http://adigitaljourney.labcd.unipi.it/technologies/connettersi-in-sicurezza/

4.1 Primo prodotto: piccola guida per genitori sulla sicurezza in internet.

Il titolo della guida è: "Essere genitori al tempo di internet: pericoli e soluzioni". Al suo interno si trovano descritti i pericoli che un ragazzo può incontrare su internet, correlato di consigli e link di approfondimento. La guida è stata pensata per i genitori che lavorando non hanno tempo di leggere molto materiale, quindi è molto concentrata e sono presenti i concetti base. Se poi il genitore dovesse avere tempo e voglia di approfondire l'argomento, sono presenti link per farlo.

Copertina e sommario della guida

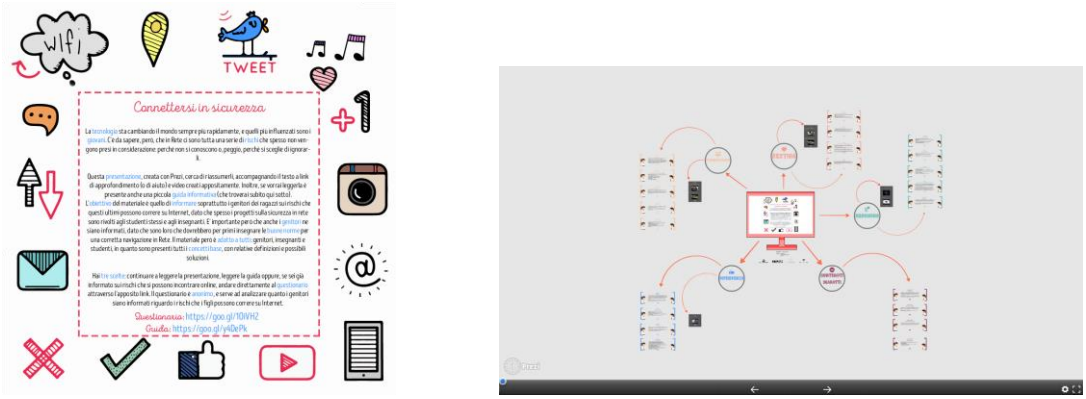
Per creare questa guida, inizialmente è stato raccolto il materiale da più siti che si occupano dell'argomento (citati in fondo a ogni paragrafo per approfondimenti): Generazioni Connesse, Azzurro, Polizia Postale sono solo alcuni da cui sono state prese informazioni. Successivamente, usando Adobe Photoshop e Adobe Illustrator, ho creato e rielaborato le immagini da inserire nella guida, e mi sono aiutata con vettori e icone trovate su Iconmonstr e Freepik (citandoli alla fine della guida). Il passo successivo è stato la creazione vera e propria del PDF usando Adobe InDesign.
Il PDF è pensato sia per essere visualizzato online sia per essere stampato, in modo da essere utilizzabile da chiunque.

4.2 Secondo prodotto: presentazione con Prezi

Per creare la presentazione, inizialmente si è presentata l'indecisione se usare PowerPoint o Prezi. Non conoscendo quest'ultimo, mi sono informata e ho deciso che era più adatto rispetto a Powerpoint per i seguenti motivi:

- Innanzitutto, Prezi ha una funzione di zoom che permette di creare delle presentazioni più accattivanti rispetto a Powerpoint;
- Non è lineare, quindi c'è la possibilità di modificare il percorso in base alle necessità rendendolo più fluido;
- È creato per il web, quindi si prestava perfettamente allo scopo, dovendola comunque caricare su un sito per essere visibile da chiunque;
- È possibile importare immagini, video da YouTube, link e molto altro.

In poche parole, Prezi è più interattivo rispetto a Powerpoint, e si presta bene ad essere usato per spiegazioni in cui è necessaria la visione di video, l'ascolto di audio o il rimando a link esterni.



Copertina e visione d'insieme della presentazione

Rispetto alla guida, i link inseriti sono maggiori e più precisi: se ad esempio nella guida c'è il rimando alla Home di un sito, nella presentazione il rimando è direttamente al PDF presente in quel sito o a una pagina specifica. Inoltre, sono stati inseriti uno o più video da YouTube per ogni argomento.

La forma della presentazione è una mappa concettuale: in questo modo si capiscono meglio i collegamenti, e le informazioni presenti sono le stesse della guida, anche se riassunte in modo da non creare riquadri troppo ricchi, così da non far stancare il lettore.

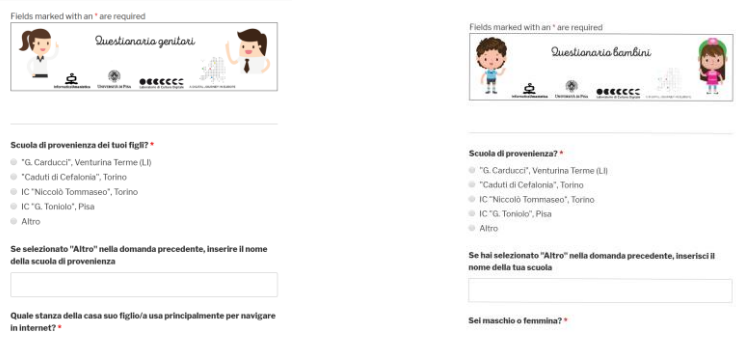
Come si può notare dall'immagine di copertina, la presentazione è stata creata in modo da poter essere visionata oppure saltata in base alle esigenze: se si è interessati si prosegue, se si preferisce visionare la Guida per avere più informazioni ma comunque sempre brevi si può cliccare sul link apposito, altrimenti se si conoscono già i concetti e si preferisce andare direttamente al questionario si può cliccare sul link apposito.

4.3 Terzo prodotto: questionari con Ninja Forms

Anche per quanto riguarda i questionari, inizialmente c'è stata l'indecisione se usare Google Moduli o Ninja Forms. La scelta è ricaduta su Ninja Forms, un plugin per Wordpress che permette di creare dei moduli di contatto e altro. Ha un'interfaccia drag and drop semplice ed intuitiva e permette anche la creazione di sondaggi o questionari. Ci sarebbero anche molte altre funzioni, ma sono tutte a pagamento.

La scelta è ricaduta su questo plugin perché, oltre ad essere visivamente migliore rispetto a Google Moduli, c'è la possibilità di inserirlo direttamente nella pagina del sito

senza rimandi a siti esterni (come sarebbe accaduto con Google Moduli). Inoltre, è possibile esportare i risultati in formato .csv e analizzarli con Excel.



Screen dei due questionari

Dopo aver creato le domande dei due questionari (uno per i genitori e uno per i ragazzi), ho installato Wordpress in locale, installando prima XAMPP. A quel punto ho scaricato e installato Ninja Forms e ho fatto qualche prova, per assicurarmi che non ci fossero problemi.

La copertina dei due questionari l'ho creata usando Adobe Illustrator e l'ho inserita grazie al campo "HTML" del Form. Dopo aver creato le pagine dei due questionari, le ho esportate per essere poi usate per creare la pagina nel sito *A Digital Journey*.

5. Distribuzione dei questionari e risultati.

5.1 Questionario genitori

Per far arrivare il questionario anche ai genitori dei ragazzi, ho scritto un avviso includendo il link al sito, spiegando le finalità della raccolta dati, informazioni sul progetto di tesi e ho spiegato che il questionario sarebbe stato anonimo e che poi avrei pubblicato i risultati sul sito della scuola. L'avviso è stato poi fotocopiato e consegnato a tutti i ragazzi, che lo hanno poi consegnato ai loro genitori. In precedenza, comunque, i genitori erano stati avvisati dal vicepreside ai consigli di classe.

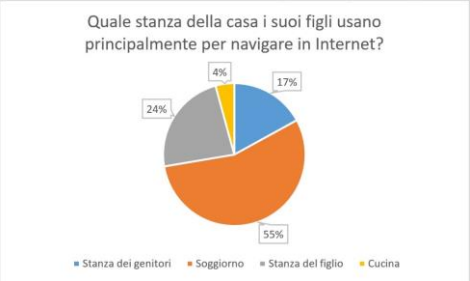
Gli scopi del questionario erano diversi:

- Comprendere come, quando e con quale frequenza gli studenti si connettessero alla rete
- Comprendere in quale misura i genitori fossero consapevoli della "vita digitale" dei loro figli
- Comprendere quanto e di cosa fossero preoccupati i genitori riguardo la relazione dei loro figli con la Rete
- Comprendere se i genitori fossero a conoscenza della situazione dei loro figli, se fossero mai stati vittima di cyberbullismo o adescamento e, in caso, in che modo avessero risolto
- Comprendere se ci fossero eventuali problemi di dipendenza, attraverso segnali specifici
- Non solo recuperare le informazioni precedentemente elencate ma utilizzare la stessa compilazione del questionario come un processo di presa di consapevolezza, da parte del target, del problema in sé

Il questionario è composto da 23 domande, di cui: 3 a risposta aperta, 5 a risposta multipla e 15 a risposta singola. Il numero totale delle famiglie a cui è stato proposto è 316, di cui solo 47 hanno partecipato. Mi aspettavo un numero minore, considerati i probabili impegni dei genitori e i lavori, quindi mi ritengo abbastanza soddisfatta.

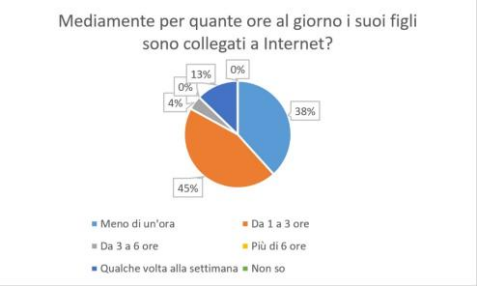
Le prime due domande non vengono inserite poiché si richiede la scuola di provenienza, e dato che tutte e 47 le famiglie hanno i figli alla scuola secondaria di primo grado "G. Carducci" di Venturina Terme, ritengo inutile un'analisi dei grafici.

Nella terza domanda si chiede in che stanza della casa solitamente i figli navighino in Internet, e si può notare dal grafico che la maggioranza, cioè il 55%, ha risposto "Soggiorno", seguito dal 24% "Stanza del figlio", dal 17% "Stanza dei genitori" e solo 4% "Cucina". I ragazzi, quindi, si suppone che rimangano sempre o quasi sotto l'occhio dei genitori.



Terza domanda

Nella quarta domanda si chiede, in media, quanto tempo i figli passino su Internet. Dal grafico, notiamo che la maggior parte dei ragazzi, secondo i genitori, passano da 1 a 3 ore connessi (il 45%), a seguire il 38% si collega meno di un'ora, il 13% solo qualche volta alla settimana, il 4% da 3 a 6 ore al giorno e lo 0% dei ragazzi secondo i genitori sta connesso più di 6 ore al giorno oppure non ne ha idea.



Quarta domanda

Nella quinta domanda si chiede quando solitamente avviene la connessione. La maggior parte dei ragazzi (il 72%) si connette di pomeriggio, a seguire il 17% di sera, il 9% più volte nel corso della giornata, il 2% non ne ha idea e lo 0% di notte.

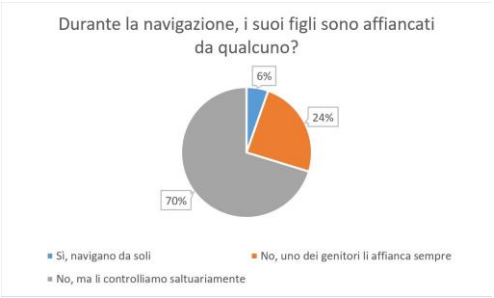
Quinta domanda

E' stato chiesto, nella sesta domanda, secondo i genitori per quali attività i loro figli utilizzino Internet. La maggioranza, il 31%, dice che i figli usano Internet per il download dei file, ad esempio musica o film. A seguire, il 25% dichiara che i figli usano Internet per ricercare informazioni, il 21% gioca online, il 16% comunica attraverso social network, il 4% usa Internet per attività che non sono tra le risposte possibili, il 2% manda o riceve email e l'1% partecipa a gruppi di discussione.

Sesta domanda

Nella sesta domanda, è interessante vedere come i genitori siano sempre o quasi accanto ai figli quando navigano in Internet. Infatti, come si nota dal grafico, la maggioranza (70%) controlla saltuariamente i figli mentre navigano, il 24% dei genitori li affianca sempre e solo il 6% dei genitori lascia che i figli navighino da soli. Questo risultato è simile a quello della quarta domanda, nella quale si chiedeva in quale stanza della casa

solitamente i figli navighino su Internet. La maggioranza aveva risposto “in soggiorno”, cioè in un luogo dove possono essere sempre – o quasi – sotto il controllo dei genitori.



Settima domanda

Secondo i genitori, il rischio principale a cui sono esposti i ragazzi quando navigano su Internet è quello di visitare siti dal contenuto non adatto o rischioso (53%). Subito dopo c’è il rischio di essere contattati da malintenzionati (24%), mentre preoccupano meno la possibilità di cadere in truffe (11%), di prendere virus (5%), di farsi rubare dati bancari o giocare d’azzardo (3%). A differenza di cosa si possa pensare, un possibile tentative di adescamento online è meno preoccupante di una pagina dai contenuti pornografici o violenti.

Ottava domanda

Come si nota dal grafico, la stragrande maggioranza dei genitori dà consigli ai propri figli su come navigare in Internet in modo sicuro (98%), mentre solo il 2% non si preoccupa dell’argomento.

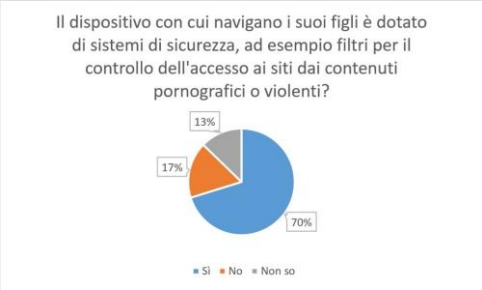
Nona domanda

Tra i consigli più dati ai ragazzi per una corretta navigazione in Internet, c'è quello di evitare siti pornografici o dal contenuto non adatto alla loro età (14%), risposta che è perfettamente in linea con il maggiore rischio di ciò che possono trovare in Rete secondo i genitori. A parità troviamo il non rivelare a sconosciuti informazioni personali (sempre 14%), e a seguire si consiglia: di non parlare con gli sconosciuti (12%), di informare genitori o insegnanti in caso di messaggi minacciosi (10%), di informare genitori o insegnanti in caso di messaggi che possono mettere a disagio (10%), di non inviare foto/video proprie o della famiglia (10%), di non rivelare i luoghi abitualmente frequentati (10%). Infine, i consigli meno frequenti sono di non giocare d'azzardo (5%) e di non inserire il numero di carta di credito in siti sconosciuti.

Decima domanda

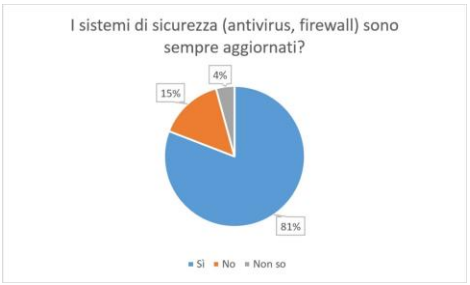
Come si nota dal grafico, il 70% dei dispositivi su cui navigano i ragazzi sono dotati di sistemi di protezione (ad esempio il Parental Control), mentre il 17% ne sono sprovvisti

e il 13% non ne ha idea perché probabilmente non ne conosce l'esistenza. Anche in questo caso, si dovrebbe fare più informazione.



Undicesima domanda

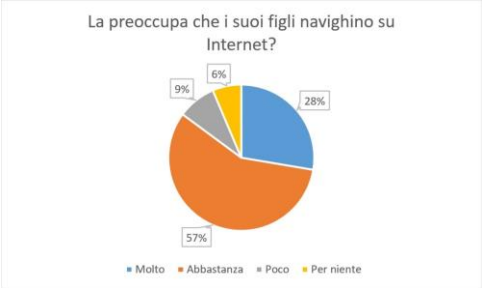
Il discorso è simile anche per i sistemi di sicurezza come antivirus o firewall: notiamo dal grafico che l'81% dei genitori provvede a tenerli sempre aggiornati, mentre il 15% non lo fa e solo il 4% li ignora. E' un risultato migliore rispetto alla domanda precedente ma non soddisfacente, perché almeno gli antivirus è importante che siano presenti e sempre aggiornati e non va bene che se ne occupi solo l'81% dei genitori.



Dodicesima domanda

Notiamo dal grafico come la maggior parte dei genitori siano abbastanza o molto preoccupati dal fatto che i figli navighino su Internet. Vediamo infatti che il 57% è abbastanza preoccupato, il 28% molto preoccupato mentre solo il 9% e il 6% lo sono poco o per niente. Sarebbe buono che questo grafico mostrasse valori inversi, e cioè che la maggioranza sia poco o per niente preoccupata e la minoranza molto o abbastanza. Questo perché vuol dire che probabilmente c'è ancora molta insicurezza e ignoranza sull'argomento "sicurezza in Internet", non si conoscono i rischi oppure si conoscono male, si danno pochi consigli e non si parla abbastanza con i propri figli. Di

conseguenza, si ha paura di cosa gli possa succedere, cosa che sarebbe quasi inesistente se convinti di aver formato i propri figli in modo sufficiente per evitare i vari rischi che possono trovare.

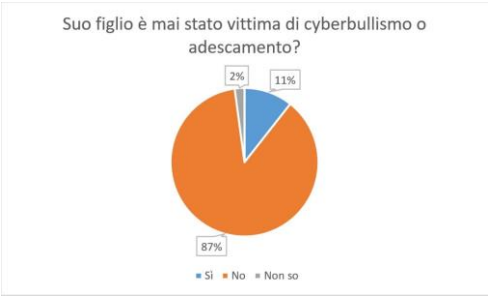


Tredicesima domanda

Dal grafico, vediamo che la maggior parte dei genitori (15%) è preoccupata che i propri figli possano perdere il contatto con la realtà (e quindi sviluppare una dipendenza), oppure che possano incontrare qualche pedofilo. A seguire, troviamo il 13% che ha paura che i figli possano diventare vittima di cyberbullismo, l'11% è preoccupato dell'invasione della pornografia, il 9% a parità preoccupano i brutti incontri che i figli possono fare e la facilità con cui vengono scaricati contenuti di ogni tipo, l'8% è preoccupato che possano fornire dati personali ad estranei, il 7% ha paura dei virus che possono intaccare i dati presenti sui vari dispositivi, il 6% si preoccupa per la salute dei ragazzi, e per ultimo troviamo il 4% che non sa cosa facciano i figli su Internet e il 3% che si preoccupa della salute dei figli.

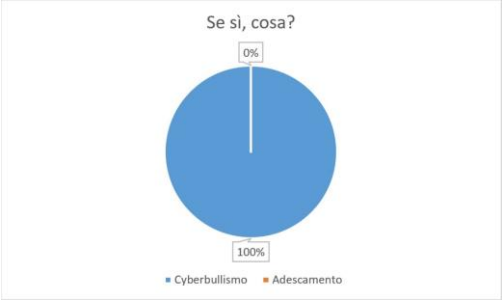
Quattordicesima domanda

Questo grafico è molto positivo. Vediamo infatti che l'87% dei ragazzi non è mai stato vittima di cyberbullismo o adescamento, mentre l'11% dichiara che i propri figli lo sono stati e solo il 2% dei genitori ignora la situazione.



Quindicesima domanda

Dell'11% della domanda precedente, tutti sono stati vittima di cyberbullismo e non di adescamento. Nella domanda successiva, che non inserirò poiché si tratta di una domanda aperta, ho chiesto di raccontare l'esperienza vissuta. Tra i racconti, si leggono esperienze di bullismo e cyberbullismo, e che comunque i genitori hanno capito, notando il comportamento strano dei figli (ad esempio nervosismo), che c'era qualcosa che non andava. Nella maggioranza dei casi, comunque, sono stati i figli a raccontare le loro preoccupazioni. I genitori hanno poi parlato con gli insegnanti, con i genitori degli altri ragazzi coinvolti e qualcuno anche con la psicologa, riuscendo nel 100% dei casi raccontati a risolvere la situazione.



Diciassettesima domanda

In questo grafico notiamo come il 79% dei genitori non permette ai propri figli di usare la propria carta di credito/postepay per far effettuare acquisti online, mentre il 19% lo permette e solo il 2% possiede una carta di credito/postepay personale. Per i ragazzi,

sarebbe utile prendergli una carta prepagata, come appunto una Postepay, in modo che possano fare acquisti online in modo sicuro, ricaricando di volta in volta l'importo che serve per quel determinato acquisto, senza lasciare un fondo. In questo modo, in caso di truffa o furto, non ci sarebbero problemi, poiché la carta sarebbe vuota.

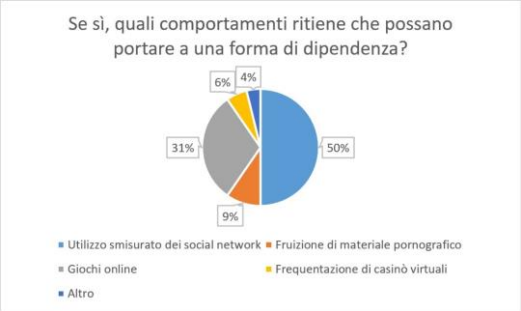
Diciannovesima domanda

Dal grafico, notiamo che il 70% dei genitori ha paura che possano verificarsi problemi di dipendenza da Internet, mentre il resto non lo pensa o non se ne preoccupa. La percentuale che pensa che sia possibile una dipendenza andrebbe drasticamente diminuita, e i genitori in questione dovrebbero conoscere meglio cosa fanno i propri figli, aprire un dialogo con loro e, in caso pensino che passino troppo tempo collegati, proporgli alternative al di fuori del mondo della Rete. La cosa più sbagliata sarebbe minacciare di togliere i dispositivi con cui si connettono i ragazzi: questo renderebbe il loro interesse verso la Rete maggiore, e non farebbe altro che peggiorare le cose.

Ventesima domanda

Secondo i genitori, il comportamento che può maggiormente portare alla dipendenza da Internet è l'utilizzo smisurato dei social network (50%). Seguono i giochi online (31%),

la fruizione di materiale pornografico (9%), la frequentazione di casinò virtuali (6%) e altre opzioni non presenti (4%).



Ventunesima domanda

Guardando il grafico, notiamo che solo il 23% dei genitori ha notato nei figli un importante calo del rendimento scolastico e una tendenza all'isolamento. Il restante 77% non lo ha notato. Questo comportamento può portare alla dipendenza, alle reazioni violente se si prova a separare il ragazzo dal computer e all'isolamento totale. E' importante in questo caso intervenire subito, proporre al ragazzo alternative che non siano il pc (ad esempio sport, uscite con gli amici) e aprire soprattutto un dialogo per capire il motivo per cui c'è il calo del rendimento e la tendenza all'isolamento. E' probabile che, oltre alla dipendenza, ci sia dietro anche altro: ad esempio il ragazzo può essere vittima di cyberbullismo o adescamento.

Ventiduesima domanda

Questi comportamenti sono già più orientati verso una probabile futura dipendenza. Il 66% dei genitori, come si nota dal grafico, dichiara che i propri figli non ne sono interessati, mentre il 34% sì. Anche in questo caso, è importante aprire un dialogo con i

ragazzi per capire il motivo per cui stiano troppo tempo al computer. Si devono inoltre proporre alternative valide, e stimolarli proponendogli attività interessanti che non riguardino il computer.

Ventitreesima domanda

In generale, il risultato di questo questionario è abbastanza positivo: gli obiettivi prefissati sono stati raggiunti, e i risultati sono migliori di quelli sperati. Non so se abbiano prima letto il materiale messo a disposizione oppure sapessero già di cosa si sarebbe parlato, però hanno dimostrato per la maggior parte di conoscere ciò che bisognerebbe fare in determinate situazioni: dare consigli ai propri figli su ciò che bisogna o non bisogna fare su Internet, controllarli saltuariamente durante la navigazione (non troppo, altrimenti si rischierebbe di farli sentire soffocati), sanno riconoscere nella maggior parte delle volte quando i figli hanno dei problemi e, parlandone con loro, riescono a trovare una soluzione insieme, anche parlandone con gli insegnanti e i genitori dei ragazzi coinvolti.

C'è però una piccola percentuale che andrebbe ulteriormente diminuita, e cioè quella che non saprebbe riconoscere i segnali di un eventuale attacco di cyberbullismo o di un eventuale tentativo di adescamento, quella che non dà consigli ai propri figli su come navigare correttamente in Internet, chi è ancora molto preoccupato se i figli navigano in Rete e quelli che dichiarano che i figli assumano comportamenti violenti se si prova ad allontanarli dalla Rete. È soprattutto per questi genitori che si dovrebbe puntare sul loro coinvolgimento nei progetti sulla sicurezza in Rete, per diminuire ulteriormente questa piccola percentuale e far sì che i ragazzi siano sempre al sicuro, perché così come i genitori si impegnano a proteggerli nella vita reale, così dovrebbero farlo anche in quella virtuale, e per farlo non c'è niente di meglio della prevenzione e dell'informazione.

5.2 Questionario ragazzi

Per somministrare il questionario ai ragazzi mi sono recata personalmente a scuola, occupando per tre giorni il laboratorio di informatica. Ho acceso tutti i computer e ho aperto in tutti la pagina del questionario, in modo che le classi potessero arrivare e andarsene senza preoccuparsi di connettersi ad Internet e di cercare la pagina, evitando così di far perdere tempo a loro e agli insegnanti.

Una volta che la classe arrivava in laboratorio, gli spiegavo brevemente chi ero, cosa stavo facendo lì e per cosa mi servisse il questionario, dopodiché li avvisavo se ci fossero state domande di chiedere senza problemi e davo il via con i questionari. Con le classi prime ho dovuto spiegare brevemente alcuni concetti, in particolare un ragazzo mi ha chiesto cosa fosse il cyberbullismo, perché i progetti sulla sicurezza in Rete sarebbero partiti solo nel secondo quadrimestre, quindi su alcuni argomenti non erano preparati. Per quanto riguarda i ragazzi delle classi seconde e terze, invece, non ho avuto problemi in quanto sapevano già ampiamente i concetti che avrebbero trovato nel questionario.

Questo discorso delle classi prime che ho trovato leggermente impreparate mi porta a fare una considerazione, e cioè che i progetti sulla sicurezza in Rete dovrebbero partire già dalla scuola primaria, in modo da far crescere generazioni responsabili e consapevoli di cosa possono trovare navigando in Internet.

Gli scopi del questionario erano diversi:

- Comprendere come, quando e con quale frequenza gli studenti si connettessero alla rete
- Comprendere come avrebbero reagito in determinate situazioni (mail da parte di sconosciuti, casi di cyberbullismo, tentativi di adescamento online)
- Comprendere se ci fossero mai stati casi di cyberbullismo, sia da parte loro, sia diretti a loro o a loro amici
- Comprendere se i ragazzi fossero a conoscenza che ciò che viene condiviso in Rete rimane per sempre
- Non solo recuperare le informazioni precedentemente elencate ma utilizzare la stessa compilazione del questionario come un processo di presa di consapevolezza, da parte del target, del problema in sé

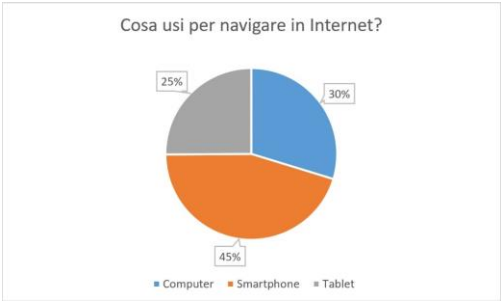
Il questionario per i ragazzi è composto da 22 domande, di cui: 3 a risposta aperta, 3 a risposta multipla e 14 a risposta singola. Ho avuto modo di somministrare il questionario a tutte e 14 le classi dell'istituto, in particolare tutto il corso A, B, C, D e le classi 2E e 3E (la 1E non esiste). In totale, i ragazzi sono 316, ma ci sono stati alcuni assenti per cui il questionario è stato compilato da 272 ragazzi.

Le prime due domande non vengono inserite poiché si richiede la scuola di provenienza, e dato che tutti e 272 i ragazzi frequentano la scuola secondaria di primo grado "G. Carducci" di Venturina Terme, ritengo inutile un'analisi dei due grafici.

Nel grafico della terza domanda, si nota come ci sia una leggera disparità tra maschi e femmine nella scuola, con prevalenza di maschi (52%).

Terza domanda

Nel grafico, notiamo come il dispositivo più usato dai ragazzi per navigare in Internet sia lo smartphone, con il 45% delle risposte. A seguire, con poca differenza tra loro, il computer (30%) e il tablet (25%). Questo indica che i ragazzi sono potenzialmente sempre a contatto con Internet, dato che comunque lo smartphone è un dispositivo che è sempre con loro, sia fuori che dentro casa.

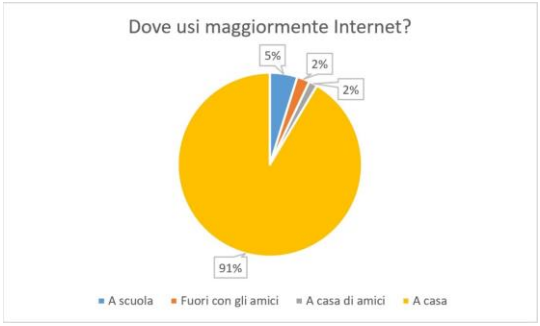


Quarta domanda

Dei ragazzi intervistati, il 63% dichiara di connettersi ad Internet per un periodo compreso tra 1 e 2 ore, il 27% tra le 2 e le 4 ore e solo il 10% passa su Internet più di 4 ore.

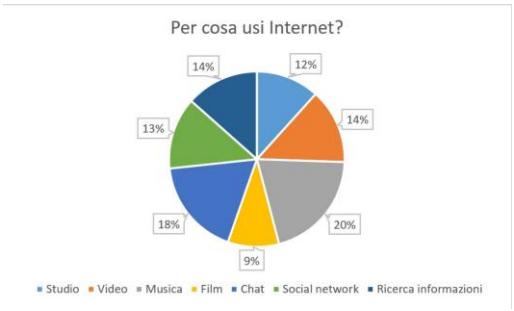
Quinta domanda

Interessante il risultato di questa domanda: il 91% dei ragazzi dichiara di usare Internet soprattutto a casa, il 5% a scuola e per ultimo a casa di amici e fuori con gli amici con il 2%. Questo significa che fuori casa si dedicano ad altre attività, il che è buono per evitare fenomeni di dipendenza.



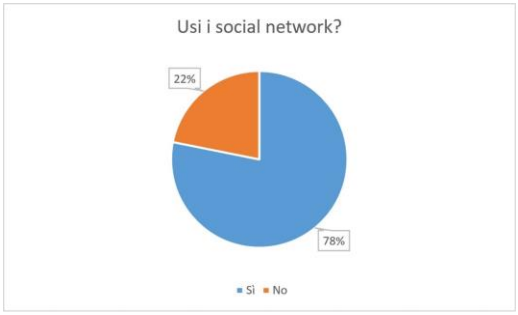
Sesta domanda

A parte per la maggioranza (20%) della musica, il grafico degli usi di Internet risulta abbastanza equilibrato: il 18% dell'uso di Internet è rappresentato dalle chat, il 14% dalla ricerca informazioni e dai videogiochi, il 13% dai social network, il 12% dallo studio e il 9% dai film.



Settima domanda

Anche questo risultato è interessante: si può osservare dal grafico che il 78% dei ragazzi usa i social network, mentre un buon 22% no. Da questa domanda ci si aspetterebbe uno stacco maggiore tra il sì e il no.

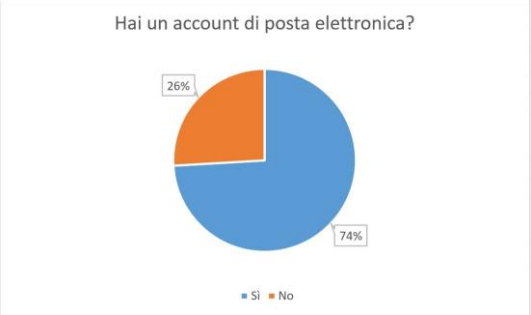


Ottava domanda

Dei ragazzi che usano i social network, quello più popolare è senza dubbio Instagram, con il 52% delle risposte; seguono Snapchat con il 27%, Facebook con il 17% e Twitter con il 4%.

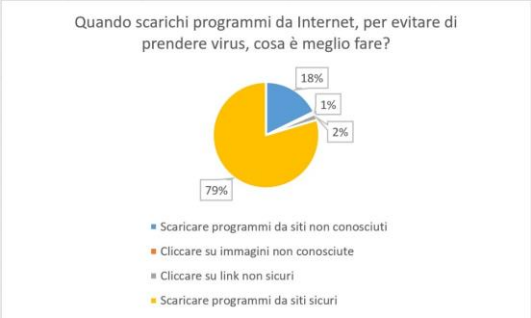
Nona domanda

Dal grafico, notiamo che i ragazzi hanno per la maggioranza un account di posta elettronica (il 74%), mentre il restante 26% non ce l'ha oppure usa quello dei genitori. E' interessante il fatto che, durante il questionario, mi venisse chiesto di continuo cosa fosse la "posta elettronica": i ragazzi infatti la conoscono come "indirizzo email", oppure sanno cosa sia citando i servizi di webmail (ad esempio *Gmail*, *Outlook*).



Decima domanda

Notiamo dal grafico come i ragazzi, per scaricare programmi, sappiano che per evitare di prendere virus devono scaricare da siti sicuri (il 79%). Il 18% scarica da siti non conosciuti, rischiando così di prendere virus, così come chi clicca su link non sicuri (2%) o su immagini non sicure (1%).

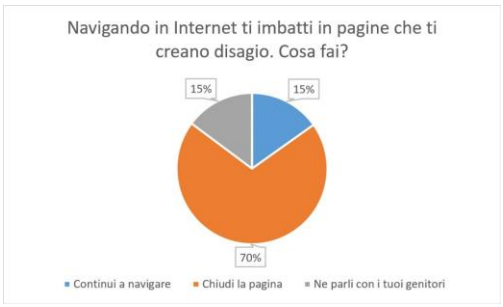


Undicesima domanda

Anche per quanto riguarda le mail da sconosciuti, i ragazzi sanno per la maggior parte cosa devono fare: il 66% infatti la eliminerebbe subito, mentre il 23% la aprirebbe per poi eliminarla. Solo il 6% cliccherebbe sul link all'interno della mail e il 5% farebbe altro. Nessuno scaricherebbe l'immagine.

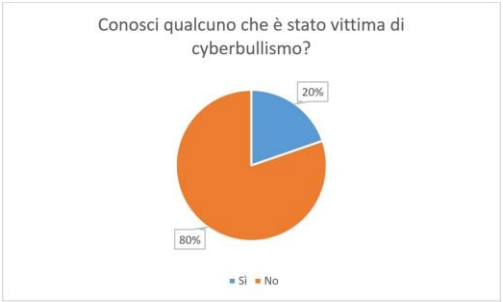
Dodicesima domanda

Come si nota dal grafico, solo il 15% continuerebbe a navigare in caso si imbattesse in pagine con contenuti che possono creare disagio. Il 70% chiuderebbe la pagina, mentre il restante 15% ne parlerebbe con i genitori.



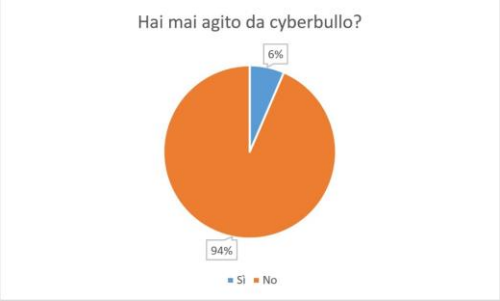
Tredicesima domanda

Il risultato di questo grafico è buono, ma non soddisfacente: una buona fetta di ragazzi, l'80%, non conosce nessuno che sia mai stato vittima di cyberbullismo, mentre il 20% sì. Sarebbe buono abbassare ulteriormente questo 20%, attraverso progetti e attività di prevenzione e dialogo coinvolgendo anche le famiglie.



Quattordicesima domanda

Anche questo risultato è buono, sia per il fatto che il 94% dichiara di non essersi mai comportato da cyberbullo, sia perché il 6% dichiara di averlo fatto. Indica un'ammissione di colpevolezza, che probabilmente ha portato alla soluzione del problema con la vittima.



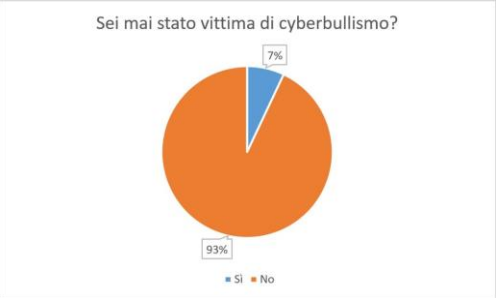
Quindicesima domanda

Dal grafico, si nota come i ragazzi, in una situazione di cyberbullismo, aiuterebbero la vittima (64%) o informerebbero i genitori o gli insegnanti (29%). Solo il 7% aiuterebbe il cyberbullo, magari perché considerato uno scherzo, e quindi non si renderebbero conto delle possibili conseguenze.

Sedicesima domanda

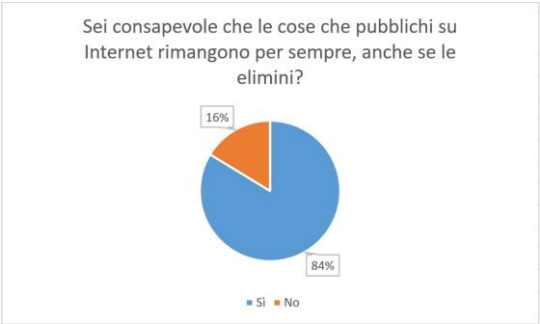
Il risultato del grafico è buono, ma non soddisfacente: il 93% dei ragazzi non è mai stato vittima di cyberbullismo, mentre il 7% sì. Insieme a questa domanda, c'era un campo di testo in cui veniva chiesto di raccontare la propria esperienza. Pochi hanno scritto casi di bullismo, altri invece hanno raccontato di gruppi di Whatsapp creati appositamente per offenderli ma comunque la situazione si è risolta grazie all'aiuto di amici. In questo campo di testo, poi, mi hanno scritto anche persone che hanno aiutato la vittima a

uscirne: ad esempio un ragazzo, la cui amica veniva presa in giro di continuo tramite telefono o whatsapp, le ha bloccato il numero e ha risolto. Mi ha anche sorpresa, in positivo, un ragazzo che in quel campo di testo ha raccontato di come inizialmente avesse bullizzato un suo coetaneo, per poi pentirsi e risolvere insieme la situazione.



Diciassettesima domanda

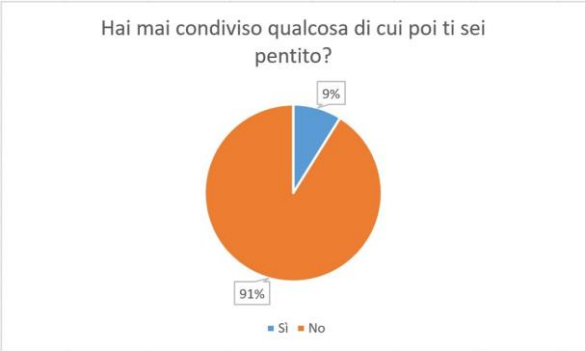
Dal grafico, notiamo che l'84% è consapevole che ciò che pubblicano su Internet rimane per sempre, mentre il 16% no. Alcuni ragazzi, durante il questionario, mi hanno detto che la domanda era sbagliata, perché secondo loro se elimini una foto questa automaticamente non esiste più in Rete. Dopo avergli spiegato, tra le altre cose, che comunque quando si carica qualcosa in Rete non si sa mai dove può andare a finire, e che qualcuno potrebbe essersi salvato la foto per poi averla ricaricata senza il nostro consenso, ci hanno pensato su e hanno capito.



Diciannovesima domanda

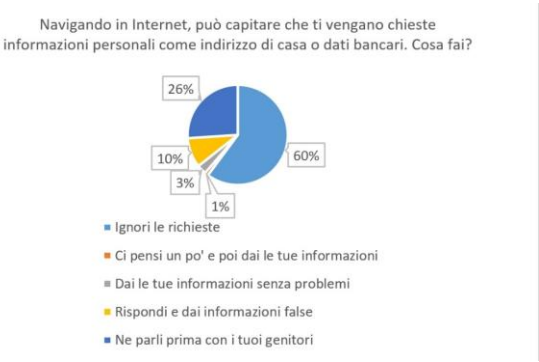
Dal grafico notiamo che solo il 9% si è pentito di aver condiviso qualcosa in Rete. Insieme a questa domanda, chiedevo in un campo di testo di scrivere nello specifico di

cosa si trattasse: si va dalle semplici foto su Instagram a video caricati su Youtube, quindi materiale utilizzabile da malintenzionati per cyberbullismo o altro.



Ventesima domanda

Guardando il grafico, si nota che la maggioranza dei ragazzi non darebbe informazioni personali in Rete: il 60% ignorerebbe le richieste, il 26% ne parlerebbe prima con i genitori e il 10% darebbe informazioni false. Solo il 3% darebbe le proprie informazioni senza problemi, mentre l'1% prima ci penserebbe.



Ventunesima domanda

Per quanto riguarda i tentativi di adescamento online, si nota dal grafico come i ragazzi nel 32% ne parlerebbero con i genitori e il 46% non accetta richieste da sconosciuti, quindi non avrebbe di questi problemi. Il 14%, invece, a richieste strane chiuderebbe la chat non cercando più l'altra persona, ma tenendosi tutto per sé senza parlarne con i genitori. Il 3% continuerebbe il rapporto mantenendolo online, mentre un preoccupante

5% ci instaurerebbe un rapporto d'amicizia anche esterno alla Rete, col rischio quindi di incappare in situazioni molto spiacevoli.

Ventiduesima domanda

Gli obiettivi anche in questo caso sono stati raggiunti, e con buoni risultati. Si è verificato come i ragazzi si connettano per la maggior parte tra 1 e 2 ore a giorno, soprattutto a casa dove possono essere controllati dai genitori. Si è anche visto come reagirebbero in determinate situazioni: nella maggior parte dei casi saprebbero cosa fare, ad esempio scaricare programmi da siti sicuri, eliminare una mail da parte di sconosciuti con contenuti di cui non si è sicuri, aiutare a contrastare il cyberbullismo denunciando il fatto a genitori o insegnanti e stando vicini alla vittima, non accettare richieste da sconosciuti o in caso non fornire mai informazioni personali. Un'altra cosa positiva è il fatto che comunque, in caso di situazioni spiacevoli, l'opzione di parlarne con i genitori è stata sempre tra le più votate.

Oltre a questo, però, c'è una percentuale ancora troppo alta di casi di cyberbullismo, di ragazzi che reagirebbero in modo sbagliato a situazioni particolari (ad esempio si incontrerebbero con chi tenterebbe un adescamento online o manterrebbe comunque un rapporto online senza dirlo ai genitori), non sono consapevoli che ciò che viene condiviso su Internet, anche se poi eliminato, rimane per sempre (anche ciò che è stato detto in laboratorio dagli studenti stessi lo conferma). Questa percentuale andrebbe ulteriormente diminuita attraverso progetti che coinvolgano insieme studenti, docenti e genitori. Si dovrebbe fare un lavoro a 360°, meglio se fin dalla scuola primaria in modo da fissare immediatamente i concetti prima che sia troppo tardi, e prima che i ragazzi inizino a usare la Rete in modo più abituale.

Conclusioni

Nel corso della tesi, abbiamo visto come ci si stia muovendo per un futuro in cui ci sia sempre più consapevolezza nell'utilizzo della Rete in modo responsabile. Si stanno attuando molti progetti rivolti a docenti e a studenti, e si sta pensando anche a coinvolgere i genitori.

Attraverso i questionari abbiamo visto che i progetti attuati stanno avendo un effetto positivo: solo una piccola percentuale è stata vittima, si è comportata come tale o conosce qualcuno vittima di cyberbullismo, così come solo una piccola percentuale non darebbe ascolto a possibili pedofili e preferirebbe parlare con i genitori in caso di problemi o situazioni che possono comunque creare disagio.

La situazione però è migliorabile, si deve fare in modo che quella piccola percentuale diminuisca ulteriormente, continuando a lavorare sui ragazzi (meglio se a partire dalla scuola primaria), sui docenti e sulle famiglie. Per quanto riguarda i genitori, nel questionario una delle domande che mi è rimasta più impressa è quella sulla loro preoccupazione dei figli che si connettono a Internet: la maggioranza è risultata abbastanza o molto preoccupata, e questo è un risultato che dovrebbe ribaltarsi. Deve esserci la consapevolezza, da parte dei genitori, di aver trasmesso ai propri figli le buone norme per una corretta navigazione in Rete; in questo caso la preoccupazione dovrebbe essere minima, perché saprebbero che in caso di problemi saprebbero come reagire. Non si comporterebbero da cyberbulli, se vedessero un episodio di cyberbullismo aiuterebbero la vittima denunciando il fatto ai genitori o agli insegnanti, non risponderebbero a malintenzionati e non caricherebbero online materiale di cui si potrebbero pentire, perché consapevoli che potrebbe finire nelle mani di chiunque. E, soprattutto, sarebbero pronti ad aprirsi e a parlare dei loro problemi, cosa che eviterebbe situazioni spiacevoli.

Per quanto riguarda il materiale informativo (guida e presentazione), è servito per dare un'infarinatura generale dei concetti presenti nel questionario dei genitori, per questo sono collegati e ho consigliato di leggere guida e presentazione prima della compilazione del questionario, in caso non si conoscessero determinati concetti. Si è

notato poi che i genitori sapessero di cosa si stesse parlando, non so se per aver letto prima la guida o la presentazione oppure per conoscenze preesistenti.

Il suddetto material, insieme ai questionari, è stato caricato sul sito di *A Digital Journey in Europe*, al link http://adigitaljourney.labcd.unipi.it/technologies/connettersi-in-sicurezza, e rimarrà disponibile per chiunque ne dovesse avere bisogno in futuro, sia per le scuole che vorranno utilizzare i questionari per verificare il successo o meno dei loro progetti, sia per chi vorrà scaricare il materiale informativo. Nei questionari, infatti, ho appositamente inserito come prima domanda "Qual è la tua scuola di provenienza?" inserendo tra le possibili risposte, a parte la scuola "G. Carducci" oggetto della mia tesi, tutte le scuole facenti parte del progetto. Se invece il questionario venisse utilizzato da una scuola che non sia nella lista, è presente un campo di testo per inserire il nome della scuola.

Ringraziamenti

Alla mia famiglia in primis: grazie per avermi permesso di iniziare e concludere il mio percorso universitario, per essermi stati vicini superando le varie situazioni che si sono presentate e supportandomi in ogni cosa decidessi di fare. Mi avete dato molto più di quello che credete e non vi ringrazierò mai abbastanza.

A Federico: grazie perché, nonostante i punti di vista diversi, mi hai sopportata durante le sessioni (e non è poco) e mi sei comunque stato vicino, anche se non te ne sei accorto. Ne abbiamo passate veramente tante, siamo cresciuti insieme durante questi anni e ti ringrazio per ogni singola cosa.

Ai miei nonni, zii, cugini: vicini o lontani non ha fatto differenza, ci siete comunque stati. Grazie anche a chi è venuto a mancare e non può essere presente in questo giorno, ma sono sicura che lo avrebbe voluto.

Grazie ai miei amici:

Sara, Jessica, Denny, lo Sbano, Giulio, Marco e Gregorio. Ormai sono anni che ci conosciamo, chi più chi meno, e ne abbiamo passate di tutti i colori: i viaggi in motorino sotto il diluvio, i capodanni a base di stracchino e salsiccia, le lunghissime giornate in magazzino, i finesettimana sull'Amiata, le giornate su quella panchina all'Altobelli e tutto il resto.

Ilaria e Irene: con voi ci conosciamo da un'eternità, ricordo le serate in discoteca e soprattutto quando dormivamo insieme, con relativi discorsi; le giornate di shopping e i giri in motorino, con Ilaria che non arrivava mai. Ci siamo allontanate ma ultimamente la situazione è decisamente migliorata, e sono contenta di come stiano andando le cose.

Beatrice e Benedetta: menziono nuovamente anche Ilaria, siete le mie coinquiline storiche. Ursy, l'adolescente, le girate in Corso Italia, Dolce Notte, la caccia alle zanzare del dopo cena, la simpatia che sembra non ci sia e infatti non c'è proprio, la dilusione di diludendo e molte altre cose. Siamo state solo un anno insieme, ma sembra molto di più, soprattutto perché poi siamo riuscite a rimanere in contatto.

Andrew, Pako, Eleonora: compagni delle superiori e poi amici, nonostante le nostre vite abbiano preso vie totalmente diverse stiamo comunque riuscendo a rimanere in contatto.

Vi ringrazio tutti, anche chi ho conosciuto da poco e quindi non ho nominato singolarmente. Siamo cresciuti insieme, ne abbiamo passate tante e mi fa piacere avervi con me a festeggiare questo mio traguardo.

Ringrazio anche i miei compagni universitari: tra sushi, giornate in aula studio, giri per negozi e in Piazza dei Miracoli avete reso questi anni decisamente più leggeri.

Ringrazio Angela Marina Chiavaroli, Angiolo Fedeli, la dirigente scolastica e il resto dei docenti della scuola secondaria di primo grado "G. Carducci" per la loro grande disponibilità e per avermi permesso di rientrare nei tempi, e gli studenti e i genitori per essersi prestati a partecipare al mio progetto di tesi.

Ringrazio Tiziano Arrigoni: dopo essere stato il professore che mi ha trasmesso di più alle superiori, è stato anche quello che non ci ha pensato due volte a darmi una mano in caso avessi bisogno durante i miei anni universitari.

Ringrazio in generale tutti i presenti alla mia discussione (e anche chi non è riuscito ad esserci): chi mi ha vista nascere, chi mi ha seguita da quando ero un rotolino di grasso fino ad ora e chi mi ha conosciuta da poco.

Questo è un traguardo per me, ho iniziato questo percorso avendo tutt'altre idee e aspettative: il percorso che volevo intraprendere era del tutto diverso, ma non mi pento di aver fatto questa scelta. Se c'è una cosa che ho imparato è che niente va come si programma: bisogna tener conto delle infinite variabili, che possono modificare il percorso in positivo o in negativo.

Durante questi anni, oltre a studiare, ho lavorato, ho viaggiato, ho imparato: è strano pensare che il mio cammino ufficiale da studentessa sia ormai giunto al termine, e che adesso inizi il difficile. Ma a questo ci penserò.

Grazie ancora a tutti quelli che ho nominato, a chi è venuto a vedermi, e mi scuso se ho dimenticato qualcuno.

Giulia

Appendice

Questionario ragazzi

Scuola di provenienza?

"G. Carducci", Venturina Terme (LI)

"Caduti di Cefalonia", Torino

IC "Niccolò Tommaseo", Torino

IC "G. Toniolo", Pisa

Altro

Se hai selezionato "Altro" nella domanda precedente, inserisci il nome della tua scuola

_____

Sei maschio o femmina?

Maschio

Femmina

Cosa usi per navigare in internet?

Computer

Smartphone

Tablet

Quanto tempo passi su internet?

Da 1 a 2 ore al giorno

Da 2 a 4 ore al giorno

Più di 4 ore

Dove usi maggiormente internet?

A scuola

Fuori con gli amici

A casa di amici

A casa

Altro

Per cosa usi internet?

Studio

Videogiochi

Musica

Film

Chat

Social Network

Ricerca informazioni

Usi i Social Network?

Sì

No

Se sì, quali?

Facebook

Twitter

Instagram

Snapchat

Hai un account di posta elettronica?

Sì

No

Quando scarichi programmi da internet, per evitare di prendere virus/trojan/worm, cosa è meglio fare?

Scaricare programmi da siti non conosciuti

Cliccare su immagini non conosciute

Cliccare su link non sicuri

Scaricare programmi da siti sicuri

Apri la mail e ne trovi una da parte di uno sconosciuto, che ha per allegati un link e un'immagine. Cosa fai?

La apri, ma poi la elimini

La elimini subito

Clicchi sul link per vedere cos'è

Scarichi l'immagine

Altro

Navigando su internet ti imbatti in pagine che ti creano disagio. Cosa fai?

Continui a navigare

Chiudi la pagina

Ne parli con i tuoi genitori

Conosci qualcuno che è stato vittima di cyberbullismo?

Sì

No

Hai mai agito da cyberbullo?

Sì

No

Quale potrebbe essere un buon comportamento per aiutare la vittima?

Aiutare il cyberbullo a prendersi gioco della vittima contattandolo sui social o tramite whatsapp

Aiutare il cyberbullo a prendersi gioco della vittima, condividendo a tua volta foto/video della persona sui social o su whatsapp

Aiutare la vittima di cyberbullismo a reagire, magari incoraggiandolo a parlare con i genitori o insegnanti

Informare i genitori o insegnanti se un amico è vittima di un cyberbullo

Sei mai stato vittima di cyberbullismo?

Sì

No

Se sì, cosa hai fatto? Ti hanno aiutato a reagire? Racconta la tua esperienza.

_____

_____

_____

Sei consapevole che le cose che pubblichi su Internet rimangono per sempre, anche se le elimini?

Sì

No

Hai mai condiviso qualcosa di cui poi ti sei pentito?

Sì

No

Se sì, cosa?

_____

Navigando in internet, può capitare che ti vengano richieste informazioni personali come ad esempio l'indirizzo di casa, il numero di telefono, informazioni bancarie o dati di carte di credito tramite moduli, minichat o persone sconosciute. Cosa fai?

Ignori le richieste

Ci pensi un po' e poi dai le tue informazioni

Dai le tue informazioni senza problemi

Rispondi e dai informazioni false
Ne parli prima con i tuoi genitori

Frequentando i social oppure una chatroom, vieni contattato/a da qualcuno che non conosci e che inizia a dirti cose strane, ti chiede di inviargli delle foto o ti invita ad un appuntamento, tranquillizzandoti dicendoti che non è niente di male e di non dire niente ai tuoi genitori. Come ti comporti?

Non sei turbato dal comportamento dello sconosciuto, continui a parlargli tranquillamente e ci instauri un rapporto d'amicizia online, inviandogli anche foto se richieste e accettando gli inviti a uscire, non informando i tuoi genitori
Non sei troppo turbato dal comportamento dello sconosciuto, ma preferisci che rimanga un rapporto d'amicizia online, senza vedersi mai dal vivo e non informi i tuoi genitori
Sei turbato dal comportamento dello sconosciuto quindi chiudi la chat non cercandolo più, preferendo tenere tutto per te senza parlarne con i tuoi genitori o con qualche amico
Sei turbato dal comportamento dello sconosciuto, quindi chiudi la chat e parli con i tuoi genitori dell'accaduto
Non accetti richieste d'amicizia da sconosciuti, quindi non ti preoccupi che ti possano succedere queste situazioni

Questionario genitori

Scuola di provenienza dei tuoi figli?

"G. Carducci", Venturina Terme (LI)
"Caduti di Cefalonia", Torino
IC "Niccolò Tommaseo", Torino
IC "G. Toniolo", Pisa
Altro

Se hai selezionato "Altro" nella domanda precedente, inserisci il nome della tua scuola

_____

Quale stanza della casa i tuoi figli usano principalmente per navigare in internet?

Stanza dei genitori

Soggiorno

Stanza del figlio

Cucina

Mediamente per quante ore al giorno i suoi figli sono collegati ad internet?

<1 ora

1-3 ore

4-6 ore

Oltre 6 ore

Qualche volta alla settimana

Non so

La connessione, abitualmente, avviene:

Di pomeriggio

Più volte nella giornata

Di sera

Di notte

Non so

Per quanto le risulta, per quale delle seguenti attività i suoi figli utilizzano abitualmente internet?

Ricercare informazioni

Mandare/ricevere e-mail

Download file (musica, video, ecc)

Comunicare attraverso social network

Giocare online

Partecipare a gruppi di discussione (forum, community...)

Altro

Durante la navigazione, i suoi figli sono affiancati da qualcuno?

No, navigano da soli

Sì, uno dei genitori li affianca sempre

No, ma li controlliamo saltuariamente

Secondo lei, quali sono i principali rischi a cui sono esposti i ragazzi quando utilizzano internet?

Visitare siti dal contenuto non adatto/rischioso

Essere contattati da malintenzionati

Prendere virus

Farsi rubare dati bancari

Cadere in truffe

Il gioco d'azzardo

Altro

Avete dato ai vostri figli dei consigli sul comportamento da mantenere per navigare in modo sicuro?

Sì

No

Se sì, che tipo di consigli avete fornito?

Evitare siti pornografici o dal contenuto non adatto alla loro età

Non rivelare a sconosciuti informazioni come e-mail, n.telefono o altri dati personali

Evitare le comunicazioni con gli sconosciuti

Non inviare foto/video loro o della famiglia

Informare genitori e insegnanti se arrivano messaggi minacciosi

Informare genitori e insegnanti della ricezione di messaggi che li fanno sentire a disagio

Non fornire a nessuno le password, perché sono personali

Non giocare d'azzardo

Non inserire il n. carta di credito in siti sconosciuti

Evitare di comunicare i luoghi abitualmente frequentati

Altro

Il dispositivo con cui navigano i vostri figli è dotato di sistemi di sicurezza come ad esempio filtri per il controllo dell'accesso ai siti dai contenuti pedopornografici, pornografici e/o violenti?

Sì

No

Non so

I sistemi di sicurezza (firewall, antivirus ecc.) sono sempre aggiornati?

Sì

No

Non so

La preoccupa che i suoi figli navighino su internet?

Molto

Abbastanza

Poco

Per niente

In particolare quali sono i rischi a cui sono esposti i suoi figli legati all'utilizzo della rete che la preoccupano di più?

L'invasione della pornografia

La pedofilia

I brutti incontri che possono fare

Il fatto che possano fornire dati personali ad estranei

I virus che possono intaccare i dati presenti sui diversi dispositivi

La perdita di contatto con la realtà

Il fatto che i figli ci “perdano” tanto tempo

La facilità con cui vengono scaricati contenuti di ogni tipo

Si rovinano la salute/occhi

Non sapere cosa fanno

Il fatto che possano diventare vittima di cyberbullismo

Altro

I suoi figli sono mai stati vittima di qualcuna di cyberbullismo o adescamento?

Sì

No

Non so

Se sì, quale?

Cyberbullismo

Adescamento

Come lo avete capito e poi risolto? Racconti la sua esperienza.

_____

_____

_____

Lei permette o ha mai permesso ai suoi figli di effettuare acquisti online utilizzando la sua carta di credito?

Sì

No

Utilizzano autonomamente una carta di credito

Crede che possano verificarsi problemi di dipendenza da internet?

Sì

No

Non credo

Se sì, quali comportamenti ritiene che possano portare a una forma di dipendenza?

Utilizzo smisurato dei social network

Fruizione di materiale pornografico

Giochi on-line

Frequentazione di casinò virtuali

Altro

Ha notato negli ultimi 6 mesi un importante calo di rendimento scolastico e una tendenza all'isolamento (rimangono chiusi nella stanza del computer, manifestano riduzione d'interessi che prima avevano, calo dei rapporti con gli amici)?

Sì

No

I suoi figli reagiscono con aggressività o tendono a non rispondere se gli fa notare che passano troppo tempo al computer trascurando le altre attività?

Sì

No

Bibliografia

Sito di Generazioni Connesse, progetto coordinato dal MIUR
http://www.generazioniconnesse.it/site/it/home-page/

Manuale per insegnanti, creato da Save the Children Italia ONLUS
http://www.sicurinrete.it/superkids/manuale-superkids.pdf

Sito specializzato sulla navigazione on line a rischio e sul cyberbullismo. Creato da IFOS, in collaborazione con il dipartimento di giustizia minorile
http://www.cyberbullismo.com/ da *Smith, 2007, Willard, 2007, Pisano, Saturno 2008, Pisano 2014*
http://www.cyberbullismo.com/ da *Watzlawick, Beavin, Jackson, 1971*

Sito del Rotary in collaborazione con l'Ordine Ufficio Minori, Questura di Venezia
http://www.ilcyberbullismo.it/

Sito del Senato della Repubblica
http://www.senato.it/

Sito Informagiovani Italia
http://www.informagiovani-italia.com/bullismo_reato.htm

Sito Telefono Azzurro
http://azzurro.it/

DirICTo raggruppa esperti e studiosi, di tutta l'Italia, in materia di Diritto dell'Informatica e di Informatica Giuridica.
http://www.diricto.it/

Sito della Polizia di Stato
https://www.poliziadistato.it/

Rivista online ad accesso libero. Nasce dall'idea di creare uno spazio di discussione tra magistrate e avvocati e il mondo dell'accademia italiana e internazionale. In particolare, il PDF riguarda il delitto dell'adescamento di minorenni, a cura di Matteo Vizzardi
http://www.penalecontemporaneo.it/upload/1441990390VIZZARDI_2015a.pdf

Articolo a cura della dott.ssa Monica Monaco, ospitato sul sito Benessere.com
http://www.benessere.com/psicologia/arg00/dipendenza_internet.htm

Centromoses opera a Treviglio (BG) e a Milano. È formato da psicologi, psichiatri, terapeuti della famiglia che operano nel campo del miglioramento della salute fisica e psichica. In particolare, al link sottostante si trova un articolo sulla dipendenza da Internet
http://www.centromoses.it/disturbi/la-dipendenza-da-internet.html

L'istituto Beck opera nel settore della salute mentale, in particolare al link sottostante si trova un articolo sulla dipendenza da internet.
http://www.istitutobeck.com/dipendenza-da-internet.html

Il lavoro dell'ESC Team è centrato sull'Internet Addiction Disorder. In particolare, al link sottostante si trova un articolo sulla dipendenza da videogiochi online.
http://www.escteam.net/game/

Sito del Policlinico Gemelli di Roma, presso il quale si trova il centro pedriatrico interdipartimentale per la psicopatologia da web.
http://www.policlinicogemelli.it/

Sito dell'Huffington Post, giornale in collaborazione con il gruppo Espresso. Al link sottostante troviamo un'intervista al Dott. Tonioni del Policlinico Gemelli, a cura di Antonia Laterza.
http://www.huffingtonpost.it/2013/10/14/dipendenza-internet--gemelli-cura-tonioni_n_4095506.html

Sito della Polizia Postale
https://www.commissariatodips.it/

Sito di Fastweb, in particolare della sezione del digital magazine, in cui si trova un articolo sui malware.
http://www.fastweb.it/web-e-digital/cosa-sono-i-virus-i-trojan-e-i-malware/

Sito del MIUR
http://www.istruzione.it/

Sito del progetto Erasmus+ *A Digital Journey in Europe*
http://adigitaljourney.labcd.unipi.it/

Paolo Ferri, *Nativi digitali puri e nativi digitali spuri*, 2011
http://educationduepuntozero.it/tecnologie-e-ambienti-di-apprendimento/nativi-digitali-puri-nativi-digitali-spuri-404174180.shtml