9. I DECALOGHI EDUCATIVI ELABORATI PER IL CORECOM

di *Samanta Stanco* e *Giovanni Ziccardi*

Una delle prime attività svolte, già nei mesi iniziali del progetto di ricerca con Corecom Lombardia, è stata quella di redigere dei "decaloghi" di semplice comprensione al fine di preparare gli studenti (ma non solo) a un uso responsabile delle tecnologie in contesti che, in alcuni casi, possono essere per loro problematici.

La prima attenzione è stata dedicata, in particolare, ai loro comportamenti, soprattutto quelli sbagliati.

La griglia di "partenza" del decalogo è stata la seguente[1]:

1. tutto ciò che si fa è pubblico e visibile (qui si è voluto far comprendere come non possa esistere un luogo nascosto, un "mio profilo" o, comunque, qualcosa di intimo e riservato in uno spazio come quello dei social network, votato alla esibizione del dato);
2. tutto ciò che si fa è amplificato (qui si è voluto far comprendere l'incredibile potere che ha la diffusione di contenuti online soprattutto come impatto sulle vittime e come percezione del danno);
3. nulla di ciò che viene pubblicato rimane nella cerchia personale (qui si è voluto far comprendere come anche zone apparentemente private sui social o sulle piattaforme possano in realtà ben essere accessibili da tutti);

[1] Appendice n.1.

4. tutto rimane per sempre (qui si è discusso sulla persistenza delle informazioni, sul fatto che il dato non muoia mai);
5. tutto è virale e inizia a circolare (qui si è discusso sul fatto che la viralità comporti una circolazione immediata, e su larga scala, di tutte le informazioni anche contro la volontà del soggetto che per primo le ha fatte circolare);
6. occorre rispettare la privacy propria e altrui (qui si è discussa l'importanza della riservatezza, della privacy propria e altrui, del sexting e dei suoi pericoli);
7. occorre conoscere gli strumenti ed essere un po' hacker (qui si è discussa l'importanza di conoscere a fondo le tecnologie che si utilizzano, mentre di solito è comune una conoscenza superficiale per avere un'immediata operatività);
8. occorre tenere dei buoni comportamenti anche online (essere un bravo cittadino digitale);
9. non bisogna alzare i toni (e, soprattutto, non bisogna alimentare odio o partecipare a liti online e a *flames*);
10. non bisogna esporre i dati più intimi riferiti alla propria persona (qui si è ribadita la necessità di proteggere i dati sensibili della persona, quei dati che, se circolanti, potrebbero discriminare.

Poi ci si è più concentrati sul raggiungimento della sicurezza attraverso i comportamenti, un aspetto che il gruppo di ricerca ha ritenuto sin da subito fondamentale.

In particolare, si è compreso come la protezione del dato digitale sia una delle esigenze più sentite del momento, visto l'elevato numero di attacchi informatici che colpiscono anche singoli utenti.

Si è allora ragionato su delle "buone pratiche" volte a garantire un livello di protezione accettabile dei propri dati personali.

Vi è infatti un impatto della sicurezza informatica anche nella vita professionale quotidiana, che riguarda sia i dispositivi di uso personale, sia gli strumenti utili per lo svolgimento dell'attività lavorativa.

Il termine "protezione", pur riferendosi a molteplici e differenti aspetti, può trovare un'esaustiva definizione nell'acronimo "Rid" (riservatezza, integrità, disponibilità). In particolare, la riservatezza implica l'esclusi-

va proprietà di un documento che non deve poter essere visionato da altre parti se non per esplicita decisione del proprietario. Per integrità, invece, si intende la protezione delle informazioni dalle alterazioni dei contenuti, siano esse apportate accidentalmente o a opera di terze parti, in particolare durante la loro trasmissione o memorizzazione. Infine, la disponibilità si riferisce alla garanzia per l'utente di accedere ai dati senza alcun problema ogniqualvolta ne abbia la necessità.

Vi è stata l'elaborazione di un decalogo specifico per la protezione dei dati dell'utente, che ha preso la seguente forma:

1. verificare i processi di autenticazione ai dispositivi e ai servizi;
2. verificare l'autorizzazione a vedere certi tipi di dati;
3. verificare sempre la presenza di un antivirus;
4. verificare sempre la presenza di un backup e della ridondanza dei dati;
5. verificare che il sistema sia sempre aggiornato;
6. verificare l'uso di sistemi di crittografia;
7. verificare i propri comportamenti;
8. alzare il livello di diffidenza/paranoia per evitare frodi online;
9. proteggere sempre anche i dati altrui e non solo i propri;
10. non tenere comportamenti nocivi per semplice curiosità o senso di sfida.

Vi è stata altresì, l'elaborazione di un decalogo relativo alle fake news[2]:

1. diversificare i media usati come fonti;
2. controllare le fonti;
3. non alimentare le catene di informazioni inutili;
4. porre attenzione alla quantità esagerata di intrattenimento;
5. chiedersi sempre il perché si sta vedendo una determinata notizia;
6. fare attenzione al contesto;
7. fare affidamento sugli esperti;
8. non fermarsi al titolo, ma approfondire;
9. fare attenzione alla data;
10. fare attenzione ai troppi punti esclamativi (!).

[2] Appendice n.1.

In ultima analisi, è il comportamento dell'utente stesso a fare la differenza: le regole di condotta non sono molte e si tratta per lo più di indicazioni dettate dal buon senso.

Nel mondo digitale, ogni documento o link proveniente dall'esterno deve essere vagliato e analizzato prima di poter essere considerato sicuro e affidabile.

Nel momento in cui arriviamo a dover prendere noi la decisione sulla "bontà" di qualcosa che ci viene passato da fuori, significa che i sistemi perimetrali e locali non hanno rilevato nulla di anomalo: questo, da un lato, indica che un controllo è già stato eseguito, ma dall'altro potrebbe segnalare che siamo di fronte a un nuovo tipo d'infezione, potenzialmente pericoloso.

Infine, anche con riferimento alle responsabilità (e responsabilizzazione) dei genitori sono state elaborate dieci regole:

1. dare un buon esempio tecnologico ai figli;
2. conoscere le nuove tecnologie a fondo;
3. formarsi e partecipare a seminari e corsi di aggiornamento;
4. proporre soluzioni alternative di gestione del tempo e modelli positivi;
5. ragionare sul tema della fiducia, dei dialoghi o dei silenzi, e confrontarsi sull'uso delle tecnologie;
6. conoscere responsabilità, diritti e doveri del genitore;
7. conoscere la legge e gli strumenti di tutela;
8. cooperare con scuola, insegnanti e dirigenti scolastici per raggiungere un buon equilibrio educativo alle tecnologie;
9. fare rete e conoscere enti e associazioni che possono venire in aiuto in situazioni critiche;
10. elaborare dei set di regole, da condividere a casa e a scuola, per disciplinare il più possibile eventuali imprevisti.

Questi decaloghi, insieme a regole specifiche sul cyberbullismo e sulle fake news, hanno costituito la base delle slide che sono state usate per tutto l'anno scolastico nelle lezioni nelle scuole.

Ovviamente le questioni più tecniche sono state semplificate (soprattutto quando ci si rivolgeva agli studenti più giovani) e sono stati fatti nume-

rosi esempi correlati alle tecnologie usate quotidianamente dalle nuove generazioni.

Le prime dieci regole per gli studenti, in particolare, sono state "esplose" con le seguenti modalità:

1. Tutto ciò che fate online è pubblico (#pubblico #visibile #noprivacy)

- Tutto ciò che viene fatto è pubblico. È visibile dai professori, dai genitori, dagli amici, è ricercabile. Non esistono gruppi chiusi. Non esiste intimità o confidenza.
- La e-mail è come una cartolina. Lo screen shot consente di violare ogni confidenza o intimità. Anche se una gallery di foto viene impostata come privata, il tag fa perdere il controllo della chiusura e, improvvisamente, apre, anche contro la nostra volontà.
- Ci sono alcune limitate possibilità di cancellare messaggi o immagini da WhatsApp o da altre app, ma se uno ha due telefoni – o fa subito lo screen shot – salta la tutela.
- Non esiste il "mio" profilo, la "mia" bacheca, la "mia" chat, il "mio" canale, il "mio" account Instagram, il "mio" spazio web, il "mio" blog.

2. Tutto ciò che fate online è amplificato (#amplificato #megafono)

- "Amplificato" vuol dire che raggiunge tantissime persone e tantissimi luoghi, anche di più della parola. Da una classe, da un piccolo circolo o da un gruppo, può arrivare a tutto il mondo.
- Siamo in presenza dello strumento più potente per la diffusione, oggi, dei messaggi.
- Le visualizzazioni dei video su YouTube sono significative: 200 milioni di visualizzazioni di un video di un cantante, ad esempio. 200 milioni sono due Nazioni!
- Bisogna capire la potenza del mezzo che si ha in mano, un enorme megafono che, soprattutto nei panni di una vittima, ha un impatto tremendo.
- È, poi, un mezzo che può essere ossessivo-compulsivo, ossia i messaggi possono essere ripetuti nel tempo brevissimo, quindi l'amplificazione si potenzia ancora di più; pensiamo per esempio agli influencer.

3. Tutto ciò che fate online rimane per sempre (#persistente #persempre #eterno #permanente)

- Il messaggio rimane per sempre. La rete non rimuove, o rimuove con grandissima difficoltà e non dimentica. La rete ripropone anche dopo tanto tempo.
- Ciò comporta la necessità di pensarci prima, di riflettere prima di mandare il messaggio, la foto o il video, perché si sta ipotecando il futuro.
- Pensiamo al diciottenne che cerca lavoro e ai colloqui lo valutano online, come appare sui social.
- È difficile rimuovere dopo i contenuti.

4. Tutto ciò che fate online diventa virale (#virale #condiviso #prendevita)

- Il contenuto prende vita. Viene condiviso. Diventa trending topic e, quindi, più visibile in rete. Anche se parte in un contesto intimo, il contenuto poi inizia a circolare e non si può più fermare.
- Oggi la condivisione, i cuori, i like, il numero di commenti, è la nuova valuta. È l'indice di gratificazione di un ragazzo. Più sei virale, più vali.
- Vieni condiviso anche se non vuoi. Vieni condiviso anche parzialmente, spesso perdendo il significato originale dei contenuti.

5. Dovete proteggere la privacy vostra e altrui (#privacy #protezionedeidati #intimità)

- Il rispetto della privacy propria e della privacy altrui. La privacy "propria" significa non condividere dati intimi, che possono mettere in pericolo la sicurezza della persona. I dati si possono anche correlare. Quindi anche un dato singolo, apparentemente inutile, può essere, se unito ad altri, un'informazione importante.
- Rispetto della privacy altrui vuol dire non violare i dati di altri. Se vediamo circolare un dato intimo di una persona, bisogna avvertirla e cancellarlo, non condividerlo, soprattutto su gruppi WhatsApp.
- Ci sono anche forme di bullismo perpetrate da amici o amiche "del cuore" che prima si fanno confidare particolari intimi della vita della vittima e poi li rendono pubblici.

6. Attenzione ai fake e alle false identità/contatti (#fake #identità)

- È facilissimo rubare l'identità, e in rete è complicato validare l'identità altrui.
- Diffidare di qualsiasi contatto che domandi informazioni, che chieda foto. Anche le informazioni sui social network sono spesso false, totalmente o parzialmente.
- Facilissimo è creare un falso profilo, anche in poche ore, che sia credibile, per poi domandare contatti o foto. Nel mondo fisico abbiamo dei parametri: sesso, età presunta, luogo dove abita. Nel digitale salta tutto.

7. La paranoia online è una virtù (#paranoia #diffidenza #cautela #difensiva)

- Nell'ambiente digitale, la paranoia è una virtù.
- Essere sempre diffidenti. Diffidare di richieste di qualsiasi tipo. Informazioni. Foto. Cliccare su link. Aprire allegati. Telefonate di informazioni. Promesse di riservatezza.
- Alzare le cautele. Non mostrare mai il viso. Non mostrare l'ambiente dove si è. Verificare una persona indagando su fonti aperte.

8. Non cambiate carattere online (#carattere #disinibizione #noncambiareonline)

- Non approfittare della mancanza della presenza per aggredire. Non far circolare voci o pettegolezzi malevoli.
- Il mezzo telematico può cambiare il carattere. Ha un effetto disinibitorio. Non c'è contatto fisico. Non è visibile il male che si fa alla vittima. Le persone più calme possono diventare delle furie. Volgari. Bestemmiano. Disinibite. Aggressive.
- Ricordarsi sempre di essere online quello che si è offline. Empatici.
- Non si è anonimi. Essere realmente anonimi è difficilissimo, quindi non c'è uno scudo vero.

9. Siate hacker e curiosi (#esserehacker #conoscere)

- Più si conoscono le tecnologie che si usano, più si è sicuri.
- Investire tempo nel conoscere le tecnologie, le funzioni, dove vengono salvate le informazioni, come bloccare, come proteggersi, come

elevare il livello di privacy, come proteggere le proprie credenziali, gli account, le password.
- Cercate esempi virtuosi. Attenzione che spesso i genitori non sono un buon esempio di uso di smartphone o tecnologie.
- Chi domina la tecnologia? Siete voi a dominarla, o è lei che domina voi?

10. In caso di dubbio, parlatene (#parlare #segnala)

- Fate rete, soprattutto nel bullismo è fondamentale, parlatene in famiglia, a scuola, segnalate anche in maniera anonima, condividete il disagio con i vostri amici.
- Non vergognatevi, non diffidate dell'Autorità (in senso lato), non abbiate paura di ulteriore vittimizzazione: se siete a disagio con l'uso della tecnologia, parlatene con l'interlocutore che preferite. Il disagio si capisce dalla tensione. Tensione quando arrivano messaggi, insonnia, controllo costante del telefono, timore di essere al centro dell'attenzione.
- Il sommerso, purtroppo, è altissimo. Ci si vergogna, soprattutto se l'aggressione tocca le origini etniche, o la sessualità, o le caratteristiche fisiche, oppure si diffida degli insegnanti, dei genitori, o si ha paura di generare altre aggressioni, e allora si preferisce non dire nulla. Ma è sbagliato.