ARTICOLO DI ELEARNINGNEWS

Year 6 - number 191 Wednesday 23 february 2022

La sicurezza dei bambini nell'era digitale

Come proteggere i bambini dai "pericoli" legati all'esposizione al digitale? Ecco i rischi in cui possono incorrere i giovani e le raccomandazioni dell'OCSE per garantire la sicurezza digitale

L'ambiente digitale è diventato una parte fondamentale della vita quotidiana, dell'istruzione e delle interazioni sociali anche tra i **bambini**. Questa tendenza, già in aumento negli anni precedenti, ha ricevuto una forte spinta dalla pandemia di Covid-19, che ha colpito il mondo intero, costringendo le persone a ricorrere ai mezzi digitali per comunicare tra loro attraverso uno schermo e le scuole ad usufruire della didattica a distanza.

Oggi, un numero sempre maggiore di bambini e ragazzi si sta avvicinando al mondo di Internet. Secondo i dati dell'UNICEF, **ogni giorno nel mondo sono 175mila i bambini e i ragazzi che entrano in rete per la prima volta**, in media uno ogni mezzo secondo. E in generale, un utente su tre è minorenne.

Se, da un lato, **Internet** offre una moltitudine di possibilità, come la socializzazione e la ricerca di informazioni di ogni genere, dall'altro espone i propri utenti anche a una serie di **rischi** che, sempre più spesso, interessano anche bambini e ragazzi che, grazie all'uso di dispositivi mobili con connessione Internet, si collegano online più facilmente. I rischi derivati dalla Rete possono incidere sul benessere dei bambini e sono, per la maggior parte, versioni online dei pericoli che i bambini corrono anche offline, come bullismo, razzismo e abusi. Ma i pericoli legati alla navigazione in Rete non escludono la possibilità di usufruire delle enormi opportunità offerte dall'online. Si tratta, piuttosto, di trovare il modo per promuovere l'uso di Internet, senza dimenticare l'importanza della protezione dei bambini che ne fanno, puntando su un'**educazione digitale** sempre più efficace e al passo con i cambiamenti tecnologici.

I rischi online

Secondo il rapporto *Children in the digital environment. Revised typology of risks*, redatto nel 2021 dall'**OCSE**, l'Organizzazione per la cooperazione e lo sviluppo economico, sono quattro, attualmente, le **categorie di rischio** cui si può accorrere in Rete. Bisogna tenere presente che i rischi connessi alla navigazione in Internet sono molto variabili e possono modificarsi col passare del tempo. Per questo, l'OCSE ha deciso di effettuare una revisione rispetto alle tre categorie delineate nel rapporto del 2019, che non tenevano ancora presenti i rischi di condotta, considerando i bambini solamente come fruitori passivi della rete. Alcune delle categorie individuate anni fa risultano ancora attuali, anche se possono essersi evolute nel tempo, mentre altri possibili rischi che precedentemente non esistevano stanno ora emergendo con maggior vigore, come la diffusione di informazioni errate (fake news) o la partecipazione dei bambini che sono diventati protagonisti della Rete, in uno scambio tra pari che li coinvolge in modo attivo.

Le quattro grandi **categorie** aggiornate dell'OCSE riconoscono i rischi di contenuto, i rischi di condotta, i rischi di contatto e i rischi per consumatori. In più, il rapporto identifica anche rischi che vanno oltre queste grandi categorie e possono avere impatti su larga scala anche sul benessere dei bambini, come i rischi per la privacy, quelli legati alle tecnologie avanzate e quelli per la salute.

I rischi di contenuto

I **rischi di contenuto** riguardano i casi in cui il bambino riceve o è esposto a contenuti disponibili anche a tutti gli altri utenti della Rete. Questa categoria comprende il rischio all'esposizione di quattro tipologie di contenuti:

- Contenuti di **incitamento all'odio**, che possono presentarsi sotto forma di immagini, parole, video, simboli, canzoni e giochi. Questi tipi di contenuti possono prendere di mira un certo tipo di religione, genere, orientamento sessuale o disabilità.
- Contenuti **nocivi**, come truffe online, pubblicità pornografiche o immagini violente e spaventose.
- Contenuti **illegali**, che possono esporre i bambini a concetti che violano le leggi e le norme sociali.

- Contenuti di **disinformazione**, che riportano false notizie: i bambini devono essere educati al riconoscimento di un fatto accaduto rispetto a una falsa rappresentazione.

I rischi di condotta

Nel rapporto precedente, l'OCSE aveva escluso le azioni dannose dei bambini in Rete, quando questi creano pericoli. Ma questa posizione attiva dei bambini nell'ambiente digitale sta diventando sempre più evidente. Per questo, nell'ultima analisi è stata inserita la categoria dei **rischi di condotta**, una possibilità che interviene quando i bambini sono attori in uno scambio tra pari e tengono una condotta non corretta o che può renderli vulnerabili. Nel concreto, un rischio di condotta "si verifica quando un bambino si comporta in un modo che contribuisce alla creazione di contenuti o contatti digitali rischiosi". Questo tipo di possibile pericolo riguarda non solo i bambini vittime di questi comportamenti, ma anche coloro che lo hanno tenuto. Rientrano nei rischi di condotta le seguenti tipologie: comportamenti di odio, che implicano l'utilizzo della Rete per aggredire un altro bambino, comportamenti dannosi, illeciti e problematici. Questi ultimi possono consistere nello scambio di messaggi o immagini sessuali, che si possono trasformare in materiale pedopornografico ed essere diffusi rapidamente in Rete.

I rischi di contatto

In questa categoria rientrano i casi in cui un bambino è vittima di una situazione dannosa in Rete. Sono esempi di **rischi da contatto**:

- Cyber bullismo, ovvero l'aggressione intenzionale e ripetuta nel tempo, portata a compimento tramite le moderne tecnologie, che ha come obiettivo una vittima che non è in grado di difendersi;
- Sexting: si riferisce allo scambio di messaggi sessuali, che possono diffondersi rapidamente online;
- Sextortion: è la minaccia della condivisione e dell'esposizione di un'immagine sessuale per costringere la vittima a fare qualcosa.

I rischi per consumatori

I ragazzi che si connettono a Internet possono affrontare anche **rischi per consumatori**. Precedentemente, l'OCSE aveva definito i rischi per consumatori come quelli in cui possono incorrere i bambini quando ricevono messaggi di marketing inappropriati, sono esposti a messaggi commerciali non facilmente identificabili come tali e quando la loro inesperienza viene sfruttata causando rischi economici (frodi online). Questa definizione può essere considerata ancora attuale, anche se una serie di nuove pratiche emergenti possono andare ad arricchire i rischi per consumatori in cui possono incorrere i bambini, come per esempio alcuni meccanismi che potrebbero nascondersi dietro le app per acquisti.

Oltre a queste categorie, l'OCSE ha riconosciuto anche rischi che attraversano quelli da contatto, di condotta, commerciali e di contenuto, arrivando ad influenzare anche significativamente la vita dei bambini. Questi sono:

- Rischi per la privacy;
- Rischi tecnologici avanzati;
- Rischi per la salute e il benessere.

In realtà, per proteggere i propri dati personali, cercando di evitare rischi per la privacy, è possibile mettere in atto alcuni accorgimenti, per mantenere una **sicurezza informatica**.

Le raccomandazioni dell'OCSE

Nel 2012 il Consiglio dell'OCSE adottò una *Raccomandazione per la protezione dei minori online*, che venne poi modificata nel 2021 e ribattezzata *Raccomandazione online sui bambini nell'ambiente digitale*. Il documento intende aiutare gli insegnanti, i genitori e i politici ad affrontare i progressi tecnologici e ad individuare gli strumenti utili a supportare bambini e ragazzi nell'inseguimento delle opportunità offerte dalla Rete e ad affrontarne i rischi. Le prime raccomandazioni riguardano la necessità di garantire un "**ambiente digitale sicuro** e benefico per i bambini" e vengono rivolte alle organizzazioni che forniscono servizi per i bambini nell'ambiente digitale. Questa prima categoria di raccomandazioni viene suddivisa in:

- Valori fondamentali, che consistono nel riconoscimento dell'interesse del bambino e nell'identificazione dei suoi diritti, che vanno protetti e rispettati;

- Potenziamento e resilienza, che prevede il supporto verso genitori, tutori e bambini nella comprensione e consapevolezza dei diritti e dei servizi legali legati all'ambiente digitale;
- Proporzionalità e rispetto dei diritti umani nelle misure adottate per la protezione dei bambini in Rete;
- Inclusione dei bambini nell'ambiente digitale, tenendo conto delle loro esigenze e della loro età;
- Responsabilità e condivisione tra le varie organizzazione per fornire un ambiente digitale e sicuro.

Il secondo gruppo di raccomandazioni riguarda il **quadro politico complessivo** e mira alla creazione di politiche che sviluppino un ambiente digitale sicuro e vantaggioso per i bambini, tramite l'adozione di leggi adeguate, l'alfabetizzazione digitale e la promozione della ricerca e dello sviluppo di tecnologie per la protezione della privacy. Il documento, nella terza sezione, raccomanda la promozione della **cooperazione internazionale**, sottolineando l'importanza della collaborazione tra i vari Paesi, attraverso reti internazionali in grado di difendere l'interesse dei bambini nell'ambiente digitale e grazie allo sviluppo di standard condivisi. Infine, le Raccomandazioni dell'OCSE mettono l'accento sulla necessità di promuovere Linee guida per i fornitori di servizi digitali, così da proteggere i bambini che navigano in Internet.

Cinque consigli per una navigazione consapevole

Per permettere a bambini e ragazzi di accedere all'ambiente digitale in modo sicuro è fondamentale garantire loro un'educazione e fornirgli gli strumenti necessari per affrontare la Rete e le problematiche in cui potrebbero incorrere. Dati i numerosi possibili rischi a cui Internet espone i suoi utenti, l'UNICEF ha fornito ai ragazzi **cinque consigli utili** per proteggersi dai pericoli della rete:

- 1. Evitare il droomscrolling, cioè la ricerca ossessiva di **cattive notizie** sul web. In caso di droomscolling è consigliato imporsi un limite di tempo, dedicando il restante ad attività creative;
  2. Usare **fonti affidabili** dal punto di vista informativo;
  3. Prestare attenzione alla **sicurezza**: è bene controllare le proprie impostazioni sulla privacy, rivolgendosi a un adulto di fiducia in caso di dubbi o segnalando la situazione alla piattaforma;
  4. Mettere la **gentilezza** al primo posto, per evitare di utilizzare l'ambiente digitale per diffondere messaggi aggressivi e offensivi;
  5. Tenere presente il **mondo reale**, senza dimenticare le relazioni personali, che devono essere vissute senza la presenza di uno schermo.