Privacy e gestione dei dati online.
Una introduzione sulle basi giuridiche per gli educatori

Chiara Vescovi [1]

Introduzione

Nell'ambito dell'educazione digitale, un posto di rilievo è occupato dal tema della privacy e della gestione delle informazioni proprie e degli altri. Si tratta di un tema complesso, che ha dimensioni prettamente giuridiche e dimensioni di opportunità, legate alla costruzione di buone relazioni interpersonali e di un'identità digitale coerente e positiva online.

La rilevanza di questo ambito è data dal fatto che, sempre più, l'economia di Internet si basa sulla raccolta e l'utilizzo di dati personali. Le piattaforme spingono per raccogliere tali dati, con cui possono indirizzare pubblicità sempre più mirate, ma che possono anche vendere a terzi. Inoltre, la facilità di interazione e scambio di immagini, testi e audio/video spinge gli utenti a pubblicare in rete sempre più materiale che riguarda sé stessi e gli altri. In questo campo, l'Unione Europea è all'avanguardia a livello mondiale per la normativa a protezione degli utenti.

Queste brevi pagine si pongono l'obiettivo di renderci più consapevoli sui problemi della privacy e della gestione dei dati online dal punto di vista giuridico. In questo campo la terminologia è spesso molto tecnica! E' importante, perciò, acquisire degli elementi di consapevolezza di base con cui porre i nostri dati e quelli dei nostri studenti/figli al sicuro. Il documento si divide in due parti, entrambe fondamentali per essere in grado di gestire adeguatamente i problemi legati alla privacy: la prima ha a che fare con la cessione dei nostri dati alle piattaforme digitali (in particolare sulla normativa relativa al famoso GDPR, *General Data Protection Regulation,* così come spiegato nel prossimo capitolo); la seconda con le relazioni interpersonali online e i problemi di riservatezza che le riguardano.

Questo documento è stato redatto dalla dott.ssa Chiara Vescovi, in collaborazione con il progetto "Benessere Digitale Scuole", il progetto V-Data (finanziato dalla Fondazione Cariplo e condotto da Università di Pavia, Università degli studi di Milano Bicocca, Università Cattolica del Sacro Cuore e Careof) e lo spinoff universitario Red Open (Università degli studi di Milano-Bicocca).

[1] Dottoranda in apprendistato nel Dipartimento di Giurisprudenza dell'Università di Milano-Bicocca e nello spin–off universitario ReD Open.

PARTE PRIMA - IL REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI (GDPR): ISTRUZIONI PER L'USO

I dati personali

I dati personali sono informazioni riferite a persone fisiche, che consentono (anche solo potenzialmente) il loro riconoscimento. Tutti i dati personali sono meritevoli di tutela. Questa varia, però, in base al grado di sensibilità del dato.

Il GDPR (*General Data Protection Regulation*, il nome inglese del Regolamento europeo per la protezione dei dati personali) è lo strumento di riferimento quando si parla di tutela delle informazioni personali. Al suo interno, vengono identificate tre grandi categorie di dati personali: i dati comuni, i dati particolari e quelli relativi a condanne penali. Ai nostri scopi interessano, in particolare, i primi due tipi di dati, i dati comuni e i dati particolari.

I dati comuni sono quei dati che, da soli o combinati tra loro, permettono di identificare un soggetto. Sono solitamente dati anagrafici, informazioni relative all'ubicazione di una persona, indirizzi e-mail, o dati relativi all'identità fisica, economica, culturale o sociale (per fare alcuni esempi, il nome e cognome di una persona, il suo indirizzo di casa, l'email personale, il colore dei capelli, l'Università frequentata, o la posizione lavorativa svolta).

I dati particolari (a volte chiamati anche "dati sensibili", usando una terminologia ormai in disuso) sono elencati in maniera puntuale dal Regolamento e sono i dati che possono fornire informazioni circa l'origine, razziale o etnica di un soggetto, le sue opinioni politiche, convinzioni religiose o filosofiche, i suoi dati genetici, quelli relativi alla salute, o all'orientamento sessuale. Uno speciale tipo di dati particolari sono i cosiddetti **dati biometrici**. Questi riguardano elementi fisici e/o fisiologici dell'individuo (per esempio, la sua voce, il volto, l'impronta digitale, la conformazione della mano o della retina), i quali, rispetto ai dati comuni, permettono grazie a trattamenti tecnici e automatizzati, di identificare un soggetto in maniera univoca (per esempio, l'impronta digitale, come dato biometrico, consente facilmente di distinguere un soggetto da altri, fornendo quindi la certezza della sua identità). I dati particolari (e, quindi, anche quelli biometrici) NON dovrebbero essere né raccolti, né utilizzati, salvo che nei casi esplicitamente previsti dal Regolamento e riportati all'articolo 9.2 del GDPR. Tra questi si ricordano, in particolare: il conferimento di un consenso da parte del soggetto a cui le informazioni si riferiscono, specifiche motivazioni legate ad adempimenti di legge nel luogo di lavoro o alla sicurezza sociale; in caso di interesse vitale di una persona, per ragioni mediche o di pubblico interesse per la ricerca scientifica.

Il "trattamento" dei dati personali

Fino a questo momento abbiamo parlato di "uso" dei dati personali, ma il termine corretto e tecnico in questo ambito è "trattamento". Cosa si intende per "trattamento" dei dati personali? Si definisce "trattamento" qualsiasi genere di operazione svolta sui dati personali di un individuo in un contesto in cui la persona a cui i dati personali si riferiscono (il cosiddetto "interessato") non abbia il controllo diretto di ciò che accade ai suoi dati.

La definizione è molto ampia; per semplificare, potremmo dire che si parla di trattamento di dati personali in ogni situazione in cui un soggetto diverso dall'interessato entra in contatto con i dati di questo e li utilizza per compiere azioni. Esempi di trattamento di dati personali sono: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la

consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione dei dati.

L'ambito di applicazione del GDPR

È importante, a questo punto, identificare i casi in cui possiamo invocare il Regolamento per la protezione dei dati personali e avvalerci dei diritti ad esso connessi. Il GDPR si applica quando un ente (pubblico o privato) tratta dati personali di un soggetto che si trovi fisicamente o virtualmente nel territorio dell'Unione Europea o in un luogo in cui vi siano accordi tali per cui si applica il diritto europeo.
Non si applica, invece, il GDPR: in caso di trattamenti che avvengono in territorio extra europeo e non riguardino persone residenti su territorio dell'Unione (non potrà, quindi, invocare il Regolamento un cittadino statunitense, residente per esempio in Texas, in merito a suoi dati che vengono trattati unicamente su suolo americano e da aziende locali); in caso di attività a carattere esclusivamente personale o domestico (quindi, non applicheremo il Regolamento in caso di scambi di dati tra amici e in un contesto prettamente personale, oppure se si dovesse realizzare un video della propria famiglia, nella propria casa, da far vedere ai parenti), o ancora riguardo alle attività effettuate da autorità competenti in tema di sicurezza pubblica e prevenzione.
È bene notare che in caso di minorenni, saranno i genitori a fare le loro veci fino ai 14 anni. Solo a tale età, essi potranno fornire direttamente il consenso al trattamento dei loro dati. Inoltre, così come previsto con l'entrata in vigore del **D.L. 139/2021**, che ha modificato l'art. 144bis del Codice Privacy, i minori potranno rivolgersi direttamente al Garante per segnalare situazioni di abuso di dati personali, oppure (comunque possibile fino ai 18 anni) rivolgersi all'Autorità garante per l'Infanzia e l'Adolescenza.

Come utilizzare il Regolamento per proteggersi: i diritti degli Interessati e il ruolo del Garante

Compreso, quindi, quando è possibile invocare il Regolamento, si vogliono ora evidenziare quali richieste è possibile avanzare in base a quanto in esso previsto. Perché un confronto in materia di trattamento dei dati personali sia proficuo è necessario innanzitutto individuare i soggetti a cui rivolgersi e comprendere i loro ruoli.

Il **Titolare del trattamento**
Il Titolare è il soggetto su cui ricadono le responsabilità dei trattamenti: si tratta della persona o ente che decide quali dati raccogliere, come e perché. I suoi contatti devono sempre essere indicati in un'apposita sezione dell'informativa privacy. Esempi di Titolari sono: l'ente scolastico, l'associazione sportiva, l'azienda di cui si sottoscrive la newsletter, l'ente organizzatore di un evento, il centro medico.

Il **DPO (Data Protection Officer)**
Il DPO è l'esperto tecnico in materia di protezione dei dati personali. Il Regolamento richiede che venga nominato in casi specifici, per esempio, in ambito scolastico. È la figura che consiglia il Titolare nella gestione dei dati personali ed è probabile che si interfacci anche con gli utenti in caso di domande o richieste. Da notare, però, che il DPO non ha, di fatto, alcuna responsabilità in merito a come vengono gestiti i dati: ogni decisione resta in capo al Titolare del trattamento.

Responsabili del trattamento
I Responsabili del trattamento sono i Fornitori a cui il Titolare si appoggia nelle sue attività. Essi gestiscono i dati personali sulla base delle sue indicazioni e istruzioni, che devono rispettare alla lettera. Un elenco contenente i nomi dei Responsabili del trattamento deve essere disponibile in caso di richiesta da parte degli interessati.

I diritti degli Interessati

Una volta compresa la terminologia base e gli interlocutori a cui rivolgersi è ora fondamentale delineare quali sono i diritti previsti dal Regolamento e il livello di trasparenza richiesto al Titolare quando questo tratta dati personali.

1. **L'utente ha diritto ad un'informativa chiara**
   L'informativa è il documento con cui il Titolare del trattamento comunica agli Interessati quali operazioni effettuerà, come e per quali finalità. L'informativa deve essere solamente "presa in visione", non è richiesta alcuna firma e, anche se si predilige la forma scritta, su richiesta dell'interessato stesso può essere resa oralmente. È richiesto che sia redatta con un linguaggio semplice, comprensibile e che sia esaustiva di tutti i trattamenti eseguiti.
2. **Diritto di accesso**
   È garantita la facoltà di richiedere una copia dei dati personali in possesso del Titolare, insieme a comunicazioni in merito alle finalità per cui questi sono stati raccolti e al loro utilizzo (modalità, tempistiche di cancellazione ed eventuali trasferimenti verso paesi fuori dallo Spazio Economico Europeo).
3. **Diritto di cancellazione/modifica/rettifica**
   È possibile richiedere al Titolare la cancellazione, modifica o rettifica dei dati in suo possesso. In questo senso, qualsiasi rifiuto ad adempiere deve essere opportunamente motivato.
4. **Newsletter e diritto di *opt-out***
   In caso di sottoscrizione di newsletter, è possibile richiedere la cancellazione dal servizio in qualsiasi momento (il cosiddetto *opt-out*) e la modalità di disiscrizione deve essere tanto immediata quanto lo è stata l'iscrizione. Nello specifico, qualora l'iscrizione alla newsletter sia avvenuta con un semplice bottone e l'inserimento del proprio indirizzo e-mail, la disiscrizione non potrà passare tramite un numero di passaggi così elevato da disincentivare l'operazione: per esempio non può essere richiesto all'utente di fornire dati aggiuntivi per poter completare la disiscrizione, oppure di chiamare anche un numero di telefono, o di accedere ad uno o più siti terzi e mandare, per esempio, quattro e-mail per confermare l'operazione.
5. **Portabilità**
   È il diritto, introdotto proprio dal Regolamento, di chiedere al Titolare di trasferire i dati in suo possesso presso un altro Titolare. Per esempio, nel caso in cui si voglia cambiare operatore telefonico, sarà possibile chiedere all'operatore A di inviare al nuovo operatore B tutti i dati in suo possesso, così da non dover fornire nuovamente le stesse informazioni e ripetere procedure già concluse.
6. **Revoca del consenso**
   In prima battuta, il consenso dato deve essere "liberamente prestato", il che significa che la richiesta di consenso deve essere chiara, semplice e comprensibile, cosicché per l'utente sia relativamente facile comprendere esattamente quali trattamenti avverranno sui propri dati. Inoltre, il consenso non può essere soggetto a costrizioni, per questo motivo non si considera valido, per esempio, il consenso prestato in sede di candidatura per un posto di lavoro: le sproporzioni di potere tra chi vuole ottenere un lavoro e chi lo offre non garantirebbero, infatti, la libertà necessaria all'interessato di poter valutare con cura le richieste del Titolare. Infine, in caso di richiesta di consenso per più trattamenti, questi devono prevedere ciascuno il proprio consenso, chiaramente diviso dagli altri. Il consenso così prestato sarà conforme al Regolamento, il quale prevede anche che esso possa essere revocato in qualsiasi momento senza necessità di alcuna spiegazione ulteriore.

Le istanze proposte al Titolare non richiedono particolari formalità, ma se si vuole approfittare di un buon modello il Garante ne ha messo uno a disposizione sul proprio sito. Il Titolare del trattamento è obbligato a rispondere alle richieste degli utenti entro un mese (con una proroga di due ulteriori mesi, in caso di

situazioni particolarmente complicate) e, anche nel caso in cui abbia ragioni giuridiche valide per non dare seguito alle richieste dell'utente è comunque tenuto a fornire una risposta, motivando la propria decisione. È poi comunque sempre possibile rivolgersi al Garante per la Protezione dei Dati Personali e proporre un reclamo per lamentare una violazione della disciplina e richiedere una verifica da parte dell'Autorità stessa. Anche in questo caso il Garante mette a disposizione un modulo apposito. Si noti, però, che seppur la forza sanzionatoria del Garante sia considerevole, non è detto che il reclamo si traduca sempre in una verifica da parte dell'Autorità: il consiglio è quindi quello di rivolgersi prima al Titolare del trattamento e solo in seconda istanza all'Autorità Garante.

Il consenso del minore

In Italia, il Codice Privacy (la normativa nazionale che si affianca al Regolamento) stabilisce che il consenso al trattamento dei propri dati espresso dal minore **abbia valore solo a partire dai 14 anni**. Prima di tale età ogni consenso è considerato invalido, salvo che sia prestato dalla persona con responsabilità genitoriale. Si ricorda anche che esistono vari programmi per impostare blocchi e filtri alla navigazione internet così da rendere l'utilizzo del web più sicuro per i minori. In merito, si rimanda all'apposita pagina sul sito del Garante Privacy.

PARTE SECONDA - IL RISPETTO DELLA PRIVACY NELLE RELAZIONI INTERPERSONALI ONLINE

Compresi, ora, i principali strumenti messi a disposizione del GDPR è bene anche concentrarsi su altri strumenti giuridici complementari alle leggi sulla privacy e altrettanto fondamentali. Al fine, perciò, di fornire una panoramica più completa di quali potrebbero essere le conseguenze della condivisione di alcune informazioni, soprattutto online, si propone ora una breve analisi in merito all'utilizzo delle fotografie su piattaforme digitali, alla diffamazione a mezzo stampa e alcuni dei rischi che si trovano a fronteggiare i minori quando navigano in internet. Infine, si parlerà di come le figure adulte possano aiutarli a prevenire e gestire tali rischi.

Foto e immagini: quali sono le tutele e cosa accade quando le condivido sui social

L'utilizzo di immagini e fotografie tocca ambiti giuridici diversi tra loro, che assumono un significato ancora maggiore quando queste vengono condivise online con il grande pubblico. Il Codice civile italiano protegge il diritto all'immagine inteso come diritto di essere riconosciuti come sé dalla società: all'articolo 10, infatti, afferma il divieto di utilizzo o pubblicazione dell'immagine di una persona all'infuori dei casi in cui sia consentito dalla legge e ne punisce a maggior ragione l'utilizzo quando questa crei un pregiudizio alla reputazione della stessa o dei suoi congiunti.
Il diritto all'immagine, poi, si interseca con altri due diritti: quello alla privacy, così come inteso dal Regolamento e dal Codice Privacy, e la legge sulla protezione del diritto d'autore (L.633/1941). In entrambi in contesti è importante soffermarsi su due aspetti: i diritti di colui che pubblica l'immagine, e, in maniera strettamente collegata, le tutele da adottare nel momento in cui si condividono fotografie altrui (sia di proprietà di altri che raffiguranti soggetti diversi).
In merito al primo aspetto, il diritto d'autore consente, da un lato, di rivendicare una certa opera come propria (il cosiddetto diritto morale d'autore), dall'altro permette di sfruttarla economicamente ed impedire che altri ne facciano copie indebite (il cosiddetto diritto patrimoniale d'autore o quello che oggi viene molto

spesso chiamato *copyright*). Nel contesto del diritto d'autore (all'art. 96 della Legge) **l'immagine di una persona può essere riprodotta e/o pubblicata solo dietro consenso di questa**. Gli unici casi in cui il consenso può non essere richiesto sono, come specificato dall'art.97 della Legge, la notorietà della persona ritratta (per esempio, un famoso attore o influencer) oppure qualora questa ricopra un ufficio pubblico (per esempio, il rappresentante di un partito politico). E allo stesso modo non è necessario richiedere il consenso quando si pubblicano immagini di eventi pubblici (intesi come di pubblico interesse o svolti in pubblico) il cui scopo sia quello di rappresentare l'evento e non una o più persone specifiche ritratte nell'immagine.
E se un privato pubblica, comunque, una foto di altri senza consenso? In questo caso può incorrere in un illecito civile, a cui si collegherà un ordine di rimozione dell'immagine e, in caso di danno al soggetto raffigurato potrà essere richiesto anche un risarcimento. Il diritto d'autore rappresenta certamente una prima tutela di cui avvalersi e un elemento da considerare quando si utilizzano fotografie raffiguranti altre persone; tuttavia, è necessario sottolineare che perché un'immagine sia coperta da diritto d'autore questa deve essere nuova, creativa e originale. In linea di massima, quindi, deve richiedere una certa volontà di tipo "artistico"; pertanto, è, per esempio, difficile invocare il *copyright* quando si scattano fotografie esclusivamente amatoriali (per esempio lo scatto di un tramonto sul cellulare) e senza precise finalità artistiche.
La seconda tutela precedentemente citata è ricollegabile al contesto della protezione dei dati personali, a cui, alle previsioni del GDPR si aggiunge quanto previsto dal Codice della Privacy, che all'art. 167 qualifica come reato il trattamento illecito di dati personali per trarne profitto o arrecare danni all'interessato eseguito tramite internet.

Condivisione di immagini su piattaforme digitali

Il contesto giuridico fin qui citato apre le porte ad una domanda fondamentale, soprattutto quando si parla di piattaforme digitali: considerando la presenza delle leggi fin qui invocate, cosa accade quando condivido immagini sui social network e, di conseguenza, come posso condividere sul mio profilo immagini altrui senza violare alcuna legge?
Qualsiasi piattaforma digitale che abbia la funzione "condividi" permette, di fatto, di riutilizzare immagini di altre persone; tuttavia, condividere sulla propria pagina una foto presa da un terzo non comporta l'acquisizione di diritti sulla stessa. Infatti, nel momento in cui si pubblicano immagini sui social è come se si concedesse alla piattaforma utilizzata (per esempio, a Facebook, Instagram o TikTok) una sorta di licenza grazie alla quale essa è in grado di utilizzare la foto e permetterne la condivisione da parte degli utenti. Queste operazioni sono, però, possibili a patto che l'immagine continui ad essere legata all'account che l'ha per primo caricata. Infatti, nel meccanismo di condivisione restano ben visibili (o comunque facilmente recuperabili) i nomi degli autori originari del video o della foto. Questo fa sì che scaricare un contenuto digitale e spacciarlo come proprio costituisca un illecito, ma che ri-condividere una fotografia postata da un altro utente, lasciando visibile l'autore dell'immagine non lo sia.

Scattare e pubblicare fotografie: consenso e liberatoria

Come è necessario comportarsi nel caso in cui si voglia scattare una fotografia di un'altra persona? Secondo la Cassazione (sentenza n. 9446 del 2018), scattare una fotografia di qualcuno senza il suo consenso è qualificabile come una molestia e quindi punibile secondo il Codice penale all'art. 660, tant'è che si può querelare il colpevole e richiedere alla polizia il sequestro della macchina fotografica o del cellulare su cui sono state scattate le foto.
Se a questo si aggiunge quanto detto in precedenza sul diritto alla privacy e in merito alla protezione del diritto d'autore è allora fondamentale, quando si scattano e pubblicano foto chiedere:

- un primo consenso a poter scattare la foto;
- un secondo consenso a poterla pubblicare.

In entrambi i casi i consensi sono revocabili. Tuttavia, se la foto è già stata scattata purtroppo non vi sono molte azioni immediatamente eseguibili. Invece, per la foto pubblicata è diritto del soggetto cambiare idea e richiedere la rimozione in qualsiasi momento, salvo diversi contratti in essere.
Di conseguenza, in caso di eventi organizzati da scuole, associazioni sportive ed enti vari in cui sia possibile che vengano fatte fotografie, magari da pubblicare su siti internet o da stampare ed esporre in palestra o a scuola, è solitamente necessario richiedere la firma di due diversi documenti:

1. il consenso al trattamento dei dati personali dal punto di vista del GDPR;
2. una Liberatoria, per consentire l'utilizzo di immagini, autorizzandone la riproduzione e pubblicazione (o altre attività a seconda di quanto specificato in liberatoria) per un tempo più o meno lungo e per determinate finalità.

Si noti che, in ogni caso, le immagini pubblicate non dovranno mai essere lesive della reputazione o della dignità del soggetto ritratto.

Diffamazione a mezzo stampa

Continuando il nostro discorso sull'utilizzo delle immagini altrui, a quanto detto fino a questo momento si aggiunge un altro tassello, quello del reato di diffamazione e, in particolare, il reato di diffamazione a mezzo stampa. Per la legge italiana, quando due o più persone parlano di una terza, non presente, in termini denigratori, dando un'immagine distorta di questa o in qualche modo lesiva della sua reputazione, si può incorrere nel reato di diffamazione (previsto dall'art. 595 del Codice penale). La situazione si aggrava quando questa operazione viene messa in atto tramite uno strumento che ne aumenti esponenzialmente la diffusione, un quotidiano, per esempio, oppure uno strumento ad esso equiparabile nel contesto digitale, quindi un social network o un gruppo di messaggistica (come Whatsapp). In questi casi si parlerà di "diffamazione a mezzo stampa" (art. 595.3 del Codice penale), una situazione considerata più rischiosa della semplice diffamazione perché aumenta il numero di persone che potenzialmente potrebbero entrare in contatto con la notizia denigratoria: di conseguenza la pensa si inasprisce, fino ad arrivare, nei casi più gravi, anche alla reclusione.
Per fare un esempio concreto: pubblicare un ciclo di storie sul proprio profilo Instagram o un video in un gruppo Whatsapp in cui si cerca di screditare apertamente un proprio conoscente, raccontando fatti non veri sul suo conto o dandone una connotazione derisoria o negativa potrebbe portare all'accusa di diffamazione a mezzo stampa.

Adescamento di minori online

Una pratica purtroppo presente online e alla quale gli adulti che si occupano di bambini e adolescenti è quella dell'adescamento di minori. Si tratta di tutte quelle azioni messe in atto da criminali che portano un/a bambini/a o ragazzo/a a fidarsi di un malintenzionato tanto da lasciarsi indurre ad inviare immagini, video o persino ad incontrarlo (parliamo, in questo caso, di un fenomeno detto *grooming*). In maniera più o meno tecnologica, chi si avvicina ai ragazzi con intenzioni malevole si assicura la loro fiducia fino a portarli a condividere pensieri intimi e insicurezze, che poi il criminale può utilizzare come strumento di ricatto per richieste dubbie o pericolose, come l'invio di fotografie intime, video o l'insistenza ad incontri dal vivo.
La tendenza alla connessione digitale perenne e alla condivisione delle proprie esistenze rende relativamente semplice raccogliere informazioni su un minore, su dove vive, su quali sono le sue abitudini e le attività che gli/le piacciono. Diversi studi hanno dimostrato come per i minori chiedere aiuto in queste situazioni sia complicato, poiché non hanno le risorse per resistere alla minaccia di pubblicazione online del materiale inviato, o si lasciano intimorire dalla vergogna di riferire ai genitori quanto accade.
Che cosa possono fare, quindi, gli adulti responsabili dei minori? Come prima azione, quando possibile, è bene impostare meccanismi di *parental control*, che consentano una navigazione più sicura. Si potrebbe,

poi, ragionare insieme ai minori sull'opportunità di iscriversi a piattaforme social prima dei 14 anni (età limite per il Codice della Privacy italiano per fornire il proprio consenso al trattamento dati). In aggiunta (e forse soprattutto) si può insegnare ai ragazzi a prestare alcune accortezze quando navigano su piattaforme digitali o giochi online (che magari hanno una chat in cui gli utenti possono scambiarsi opinioni):

- impostare la privacy delle piattaforme digitali sempre su "privato", in modo tale che solo persone conosciute possano vedere i materiali pubblicati e mettersi in contatto con loro;
- non fornire informazioni personali a sconosciuti o sconosciute sui social, anche quando sembrano avere la stessa età del minore: creare un profilo falso è molto rapido e si deve sempre stare attenti a quali informazioni vengono condivise;
- non condividere la posizione di casa propria o dei luoghi in cui si trovano spesso indicandoli come tali (anche la semplice localizzazione nelle foto pubblicate o inserita nelle storie di instagram potrebbe costituire un dato prezioso per i malintenzionati);
- fare attenzione, sia quando si ha un profilo privato che quando se ne ha uno aperto, a quali immagini si condividono di sé stessi: purtroppo, che sia giuridicamente corretto o meno, estrapolare parti di immagini e/o di video da un contesto e inserirli in un altro è relativamente semplice e lo è altrettanto condividere informazioni e foto che erano state inviate privatamente. Per quanto si utilizzino varie accortezze, mettere online i propri dati significa rischiare di perderne il controllo;
- nel caso in cui una richiesta o atteggiamento li metta a disagio o li faccia sentire non sicuri, devono sapere che possono parlarne con un genitore, un insegnante (ad esempio, il docente referente per il cyberbullismo, che ogni scuola ha), un adulto di fiducia o, eventualmente anche contattare il numero del Telefono Azzurro i cui operatori sono addestrati a gestire situazioni di questo genere.

Qualsiasi cosa accada, è fondamentale ricordare che la colpa non risiede mai nelle vittime e che la scuola, gli allenatori, gli insegnanti, in generale gli adulti che si occupano della formazione dei ragazzi sono una rete di supporto fondamentale a cui rivolgersi in caso di domande e/o situazioni poco chiare.

Conclusioni

Al termine di queste pagine la speranza è quella di essere riusciti a fornire una base di conoscenza su un tema certamente complesso, ma sempre più rilevante nella nostra vita e in quella dei nostri figli o studenti. Tra gli strumenti che ora si è in grado di utilizzare vi sono: una corretta terminologia in ambito privacy e l'identificazione di vari tipi di dati personali. Si padroneggia un linguaggio specifico, che permetterà di comunicare in maniera efficace con gli interlocutori che il Regolamento ha preposto. Nel corso di queste comunicazioni, sarà ora possibile comprendersi più facilmente ed esercitare con una maggiore consapevolezza i diritti a nostra disposizione, oltre a richiedere una corretta documentazione e informazione. Sarà così possibile accertarsi che i dati personali siano trattati in maniera sicura, corretta e conforme alle normative privacy e aggiungere un grado ulteriore di protezione nei confronti dei nostri figli e verso noi stessi. Infine, sarà più facile aiutare i nostri figli/studenti ad orientarsi nella condivisione di contenuti online e nella gestione delle relazioni mediate dalla rete.

Per ogni ulteriore dubbio il sito del Garante Privacy prevede infografiche specifiche per le varie tematiche, oppure è possibile rivolgersi agli autori di questo testo, che saranno a vostra disposizione.