Privacy e gestione dei dati online
Una introduzione per gli studenti

Chiara Vescovi [1]

Introduzione

Queste pagine si pongono l'obiettivo di aiutare il lettore a comprendere di più delle leggi che ci proteggono nella difesa della nostra privacy e della nostra reputazione online.

Il documento si divide in due parti. La prima spiega come proteggersi dalla raccolta e sfruttamento dei propri dati personali che fanno le piattaforme del web, come i social network o i giochi online. La seconda invece mostra come essere rispettosi di sé e degli altri quando si interagisce nelle chat, sui social o in altri ambienti online.

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).

PRIMA PARTE: La privacy e le sue tutele

La protezione dei dati personali: concetti fondamentali

Prima di poter parlare di privacy e delle tutele ad essa collegate è importante condividere alcune definizioni, cosicché nelle prossime pagine ogni concetto sia chiaro e facilmente comprensibile. Quando si parla di valore delle informazioni, soprattutto nel mondo digitale spesso ci si riferisce ai cosiddetti "**dati personali**". I dati personali sono informazioni riguardanti una persona fisica, che da sole o combinate tra loro, consentono a chi le possiede di identificare con certezza la persona a cui si riferiscono. Per chiarirci sono dati personali, ad esempio, il nome e cognome, il colore dei capelli, il timbro della voce o la via in cui si abita. Alcune informazioni da sole non sono abbastanza per identificare con certezza un soggetto, ma assumono valore perché combinate tra loro possono invece portare ad individuare una persona in maniera specifica.

Si può utilizzare un esempio per spiegare meglio il concetto. Se in una scuola si vuole identificare con precisione un alunno non basterà cercare un ragazzo che si chiami "Luca", perché la maggior parte delle scuole italiana sono piene di moltissimi "Luca". Se però di Luca si sa anche che ha i capelli marroni e gli occhi

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

azzurri, ha 11 anni, frequenta la 1B e di cognome si chiama "Bianchi", allora probabilmente diventerà molto semplice capire di quale alunno stiamo parlando. In questo esempio il nome e cognome (Luca Bianchi), il suo colore di capelli e occhi (capelli marroni e occhi azzurri), l'età (11 anni) e la classe frequentata (1B), sono tutti dati personali, perché permettono di individuare l'alunno di cui si sta parlando.

Quando un'azienda o un ente (per esempio la scuola o gli organizzatori di un centro estivo) svolgono operazioni sui dati (per esempio, la loro raccolta, cancellazione o analisi) queste attività si chiamano "**trattamenti**". Alcuni trattamenti si dicono necessari, perché sono richiesti dalla legge o perché imprescindibili per svolgere determinati servizi: per esempio, chi lavora per un'azienda dovrà necessariamente fornire alcuni suoi dati personali perché previsto per legge o per garantire di poter assegnare la posizione per loro migliore (per esempio, nome, cognome, altri lavori svolti in precedenza, o il conto bancario su cui si vuole ricevere lo stipendio). Oppure, la scuola avrà il diritto di conoscere alcune informazioni sui suoi alunni o sui suoi insegnanti. In altri casi, invece, il trattamento dei dati personali è richiesto comunque per accedere ad un servizio, ma non risponde a degli obblighi imposti dalla legge. L'esempio più immediato in questo senso sono le informazioni richieste in fase di iscrizione ad un social network: senza fornire (almeno) nome, cognome, genere e data di nascita non è possibile creare un profilo su Instagram o su TikTok, ma non è nemmeno possibile creare un indirizzo email su Google o fare acquisiti su Amazon.

È importante comprendere che le aziende (e in particolar modo le piattaforme online, come i social network, Google o Amazon) chiedono dati personali in cambio dell'accesso ad un proprio servizio perché questo gli consente 1) di personalizzare l'esperienza di navigazione mostrando contenuti personalizzati sulla base dei nostri gusti e, soprattutto, 2) di sottoporre agli utenti pubblicità personalizzate sui propri interessi, gusti e abitudini (identificati grazie alle informazioni fornite da noi stessi o al modo in cui utilizziamo la piattaforma). Questa pubblicità mirata consente di guadagnare di più, pertanto le aziende hanno un grandissimo interesse nella raccolta di dati personali! Si capisce, allora, come il trattamento di dati personali assuma una rilevanza così forte da rendere necessario stabilire una serie di regole che ne delimitino l'utilizzo.

Tra queste regole spicca il generale diritto alla protezione dei propri dati personali, quello che spesso viene chiamato diritto alla *privacy*. È stato riconosciuto come uno dei diritti fondamentali degli esseri umani e si esplicita, da un lato, in una serie di garanzie per gli utenti, come ad esempio il fatto che prima di trattare dati personali è necessario informare i soggetti coinvolti (tramite un documento che si chiama Informativa privacy) e, in alcuni casi, richiedere il loro permesso, che in termini privacy si chiama "**consenso**". Dall'altra, si traduce nel diritto alla riservatezza, a creare una propria sfera di libertà privata che sia meritevole di essere protetta e preservata perché necessaria allo sviluppo della persona.

Il minore e il suo consenso: età e libertà

Il diritto alla riservatezza sopra citato è stato più volte riconosciuto, sia in Italia che nel resto del mondo, anche ai minorenni. Tra gli altri, la *Convenzione di New York sui diritti del fanciullo* del 1989, per esempio, sottolinea all'art. 16 come *i ragazzi abbiano diritto ad una propria sfera personale che deve essere protetta dalla legge*. E anche la legge italiana ha confermato più volte come sia fondamentale per i genitori concedere ai figli uno spazio di libertà in cui potersi muovere in autonomia.

E allora ci si chiede, quando il minore viene considerato in grado di esprimere la propria opinione circa i trattamenti svolti sui suoi dati personali? Secondo il *Regolamento per la protezione dei dati personali* (che è un atto di legge europeo, chiamato anche, in inglese, *General Data Protection Regulation*, GDPR) il consenso è valido solo a partire dai 16 anni. In Italia, tuttavia, si è deciso di abbassare questa soglia e il consenso al trattamento dei dati personali può essere espresso dopo il compimento **dei 14 anni**. Prima sarà quindi necessario domandare il permesso ai genitori (si pensi, per esempio, a quando da scuola vengono dati i moduli per acconsentire alle foto di classe), a chi ha la custodia del minore, oppure il genitore dovrà autorizzare espressamente il figlio ad esprimere il consenso.

L'invito è, in ogni caso, quello di non iscriversi da soli a piattaforme social, almeno fino al compimento dei 14 anni e comunque a prendere tutte le cautele necessarie per comprendere che cosa l'ente a cui sto dando i miei dati andrà a fare con essi. Dove si trovano tutte queste informazioni? Nelle già citate informative privacy, quelle che solitamente appaiono prima di poter accedere ai servizi online. Sono documenti complessi e lunghi, ma in questo caso il consiglio è di sottoporli ad un adulto prima di accettare qualsiasi genere di condizioni proposte. Così, per esempio prima di iscriversi ad un gioco online e inserire i propri dati personali è sempre bene consultare un adulto, che legga bene quali trattamenti verranno eseguiti sulle informazioni richieste!

SECONDA PARTE: Le piattaforme digitali tra utilizzo di immagini e relazioni interpersonali

Realizzazione di fotografie e pubblicazioni: consensi necessari

Tra i dati personali, rientrano anche le immagini e le fotografie che raffigurano persone. Se pensiamo al nostro modo di comunicare oggi, ci rendiamo conto di quanto utilizziamo le immagini, soprattutto quando si utilizzano piattaforme digitali come i social network (ad esempio, Instagram, TikTok), oppure quando si partecipa a giochi online, magari con una classifica che condivida alcune informazioni (come un nickname e l'età), o, ancora se si scambiano foto sui gruppi di messaggistica (e. Whatsapp). Le immagini rappresentano una forma molto utilizzata di linguaggio e, in quanto tale, rispondono anche a regole precise, che è necessario seguire, per non rischiare di incappare in spiacevoli conseguenze.

Considerando questo, allora, è bene capire che cosa accade quando si pubblicano immagini online e a che cosa si deve prestare attenzione in caso di condivisione di fotografie raffiguranti altre persone. Per prima cosa esiste un particolare diritto, chiamato diritto d'autore, che consente di rivendicare una certa opera come propria, di sfruttarla economicamente (magari vendendola) e di conseguenza anche di evitare che altri ne facciano copie non autorizzate o la spaccino come propria (lo sfruttamento economico e il divieto di copie illecite rappresentano quel diritto solitamente chiamato *copyright*). Nel contesto del diritto d'autore è vietato riprodurre l'immagine di una persona senza il suo consenso, salvo che non si parli di un personaggio pubblico (per esempio, un famoso attore o influencer), o che ricopra una carica pubblica (per esempio, il rappresentante di un partito politico), o ancora che si parli di un'immagine scattata durante un evento pubblico allo scopo di raffigurare l'evento e non le persone.

Il diritto d'autore può, però, essere utilizzato solo quando un'immagine sia 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. Al diritto d'autore si aggiunge, poi, anche la tutela del GDPR, che punisce chiunque ritragga un'altra persona senza il suo consenso. I giudici italiani sono andati anche oltre, affermando che **scattare una fotografia di qualcuno senza il suo consenso sia paragonabile ad un atto di molestie**, che è un reato punibile secondo il Codice penale all'art. 660, con conseguente sequestro della macchina fotografica o del cellulare su cui sono state scattate le foto, il pagamento di una multa e, nei casi più gravi, anche l'arresto.

Tenendo a mente, quindi, quando detto sul diritto d'autore, sulla privacy e su questo orientamento dei giudici, chi scatta e pubblica foto dovrà:

- Chiedere un primo consenso a poter scattare la foto;
- Chiedere un secondo consento (distinto dal primo) per poterla pubblicare.

Questi ragionamenti valgono sia per chi scatta le foto, sia per coloro che sono ritratti nelle foto: i consensi vanno chiesti o pretesi: senza di essi ci si dovrebbe rifiutare anche solo di prendere parte ad una foto o di scattarla. Si ricorda, poi, che il consenso può comunque essere espresso in Italia solo dopo i 14 anni,. Se, quindi, un fotografo dovesse fermare una ragazza di 12 anni per strada e chiederle di scattarle una foto, la risposta della ragazza non avrebbe valore, perché ancora non ha la possibilità giuridica di esprimere il consenso al trattamento dei suoi dati.

Condivisione di immagini su piattaforme digitali

Considerando quanto detto, quindi, fino a questo momento, viene ora spontaneo chiedersi cosa accada quando una persona decide di condividere immagini sui social network e, di conseguenza, come sia possibile, per esempio, condividere sul proprio profilo immagini altrui senza violare alcuna legge?

Qualsiasi piattaforma digitale che abbia la funzione "condividi" permette, di fatto, di riutilizzare immagini di altre persone: ripubblicare nelle proprie storie di Instagram il post di un proprio amico equivale a riutilizzare un'immagine postata da un'altra persona. Questa operazione, però NON mi consente di acquisire alcun diritto sulla foto che sto condividendo, che resta di colui che l'ha per primo pubblicata. Perché? 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 (una specie di autorizzazione temporanea) ad 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.

Diffamazione a mezzo stampa

Continuando il discorso sull'utilizzo delle immagini altrui, per la legge italiana quando in due o più persone si parla di qualcuno di non presente dicendo cose non vere su di lui o lei, allo scopo di prenderlo in giro o di far cambiare opinione di su lui o lei, questo atteggiamento può essere considerato un reato, in particolare un reato di *diffamazione* (art. 595 del Codice penale). Esso punisce chi riporta informazioni non vere su una persona, rovinando in un qualche modo la sua reputazione. Il reato è poi considerato anche di livello più elevato, e quindi più grave, se queste informazioni vengono diffuse utilizzando uno strumento che consenta di raggiungere in fretta un numero elevato di persone, per esempio quindi un social network o un gruppo 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 lesiva della reputazione della persona. Proprio perché più grave, anche la punizione a cui si va incontro è maggiore, arrivando in alcuni casi anche alla reclusione in carcere.

Le regole per i reati commessi da minorenni, però, sono diverse rispetto a quelle per gli adulti. Il Codice penale italiano indica che prima dei 14 anni non si può essere considerati punibili, anche in caso di azioni molto gravi, come il reato di diffamazione a mezzo stampa.

A maggior ragione però è giusto considerare che dal momento in cui si raggiunge l'età del consenso nel gestire i propri dati personali (14 anni) e, quindi, in cui ci si può legalmente iscrivere ad un social network, allora si diventa anche punibili per le azioni commesse tramite esso. Per fare un esempio concreto: pubblicare un ciclo di storie sul proprio profilo Instagram o TikTok, 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 cercando di leggerli in maniera derisoria o negativa, potrebbe effettivamente portare ad essere accusati di diffamazione a mezzo stampa.

Cyberbullismo

Il cyberbullismo rappresenta una forma di violenza commessa a mezzo internet. È un fenomeno digitale vero e proprio, che ha cambiato il modo di percepire il bullismo.

Il bullo, nella vita reale, è una persona, che si pone in una situazione di prevaricazione (anche fisica) rispetto ai suoi coetanei. Il cyberbullismo invece, si muove in un contesto virtuale, dietro la sensazione di anonimato e impunità che viene dall'utilizzo di uno schermo, allo scopo di isolare un minore o un gruppo di minori. Il cyberbullo potrebbe per esempio sparlare online della vittima, allo scopo di danneggiare la sua reputazione (si parla, in questo caso di *denigration*), oppure inviare messaggi violenti e volgari allo scopo di suscitare una lita su una piattaforma digitale (il cosiddetto *flaming*), oppure ancora l'invio ripetuto di messaggi offensivi, allo scopo di ferire la vittima (detto anche *harrassing*).

Per gli adulti, purtroppo, non è sempre semplice rendersi conto di ciò che accade online tra ragazzi. Nel caso si dovesse essere vittima di forme di cyberbullismo è quindi importante parlarne con persone di fiducia, confidarsi con genitori, insegnanti (ce n'è uno in ogni scuola che si occupa di cyberbullismo), forze dell'ordine o, se per qualsiasi motivo non sia possibile contattare questi soggetti, si può fare affidamento al telefono azzurro: hanno un numero sempre attivo o una chat, entrambi disponibili per ogni emergenza o per parlare e confidarsi.

Sebbene il cyberbullismo non sia in quanto tale un reato a sé stante, i comportamenti messi in atto possono integrare altri reati previsti dal Codice penale, quali la diffamazione (di cui si è parlato poco sopra), le minacce, il trattamento illecito di dati personali o la violenza privata. Infine, anche se non si dovesse giungere al punto di considerare una certa azione come reato, sarebbe sempre possibile oscurare i contenuti pubblicati online dal bullo e persino sottoporle ad un richiamo da parte delle autorità.

Adescamento di minori online

Una pratica purtroppo presente online e dalla quale è fondamentale che anche i ragazzi siano messi in guardia è quella dell'adescamento di minori.

Che cosa si intende per adescamento di minori? Sono tutte quelle azioni messe in atto da criminali che portano un ragazzo o ragazza 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 piacciono. Chiedere aiuto in queste situazioni è spesso complicato, poiché si cede alla paura della minaccia di pubblicazione online del materiale inviato, o ci si lascia intimorire dalla vergogna di riferire quanto accade ai genitori.

Quali accortezze e attenzioni è, quindi, possibile prestare quando si naviga su piattaforme digitali o giochi online (che magari hanno una chat in cui gli utenti possono scambiarsi opinioni):

1. 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 i ragazzi;
2. 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;

3. non condividere la posizione di casa propria o dei luoghi in cui ci si trova (anche la semplice localizzazione nelle foto pubblicate o inserita nelle storie di Instagram potrebbe costituire un dato prezioso per i malintenzionati);
4. fare attenzione, sia quando si ha un profilo privato che quando se ne ha uno aperto, a quali immagini si condividono di se 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;
5. nel caso in cui una richiesta o atteggiamento susciti sensazioni di disagio o di poca sicurezza è fondamentale rivolgersi ad un adulto, che può essere un genitore, un insegnante (ad esempio, il docente referente per il cyberbullismo), un adulto di fiducia o, eventualmente anche il Telefono Azzurro i cui operatori sono addestrati a gestire situazioni di questo genere.

Conclusioni

L'intento di queste pagine è stato quello di aggiungere qualche tassello al vocabolario digitale fino a questo momento conosciuto. È inutile negare che, come in moltissimi altri ambiti, anche la realtà virtuale con le sue peculiarità e regole, presenta dei rischi ma, proprio come nel mondo reale, sapere come proteggersi e affrontare le difficoltà apre la strada all'esplorazione sicura delle tante opportunità offerte dal web.

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. In caso questo non sia possibile, gli operatori del Telefono Azzurro sono a disposizione 24 ore su 24, sia per telefono che per chat. Tramite il loro sito è anche possibile scrivere email o inviare segnalazioni di situazioni che non ci lasciano tranquilli o sulle quali si sente il bisogno di ricevere un parere esperto.

Di seguito i loro recapiti.

Telefono Azzurro telefono: 1.96.96
sito internet: www.azzurro.it