LEZIONE 3
L'IDENTITÀ DIGITALE

Occorre **difendere le proprie identità digitali e i dati** che come utenti Internet quotidianamente diffondiamo, per metterci al sicuro da potenziali rischi di violazione di diritti quali l'**immagine**, l'**onore**, la **reputazione** e la **riservatezza**.

1 Proteggere i propri dati personali

La Rete mette a disposizione dei propri utenti servizi gratuiti (mailing list, newsgroup, *personal web site, wiki*, blog, social network); i gestori delle piattaforme sociali chiedono però in cambio i dati personali al fine di **tracciare le** identità digitali▸ degli stessi utenti. L'obiettivo è la **profilazione degli utenti**, cioè la raccolta ed elaborazione dei dati degli utenti di servizi online al fine di segmentare l'utenza in gruppi di comportamento a vantaggio delle aziende. A gestire i social network sono generalmente aziende che si finanziano vendendo pubblicità mirate; il loro valore di mercato dipende anche dalla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri utenti, per poi rivendere le informazioni a chi ne ha bisogno.

Le interazioni che avvengono all'interno dell'ambiente digitale durante la navigazione lasciano numerose tracce di dati – e quindi informazioni – che si disperdono nella Rete, concorrendo a definire la *digital footprint* di ognuno, ossia la propria impronta digitale. La **dispersione dei dati personali** si manifesta sia nel corso della navigazione in Internet mediante browser (si pensi ai ***cookies***, tecnica utilizzata dalle applicazioni web per archiviare e recuperare informazioni relative agli utenti), sia nell'utilizzo delle piattaforme di social networking. I social network, infatti, sono "**piazze virtuali**", cioè luoghi d'incontro e scambio (fotografie, filmati, pensieri, indirizzi di amici, ecc.) degli utenti della Rete; essi rappresentano uno straordinario **strumento di condivisione e comunicazione**, non privo – tuttavia – di rischi per la sfera personale degli individui. L'impressione di servirsi di uno spazio personale spinge di fatto gli utenti a esporre

Identità digitale È l'insieme dei dati e delle informazioni che individuano un utente che interagisce con un sistema informatico (un sito, un'app, ecc.).

troppo la propria vita privata, rivelando dati e informazioni strettamente personali, azione con effetti da non sottovalutare. Le informazioni che si possono reperire online possono riguardare sia i caratteri personali (le cosiddette informazioni primarie), sia le abitudini sociali e i gusti commerciali (informazioni secondarie). Questi due tipi di informazioni, elaborate tra loro, formano il **profilo-utente**.

La **pubblicità comportamentale**, fondata sul tracciamento delle informazioni rilasciate dagli utenti nel corso della navigazione in Internet, di per sé **non è vietata**, ma quando si inseriscono dati personali su un sito di social network si **perde il controllo** degli stessi; i dati possono essere registrati da tutti i propri contatti e dai componenti dei gruppi cui si è aderito, rielaborati, diffusi, anche a distanza di anni. Spesso, inoltre, gli utenti non hanno a disposizione né gli strumenti necessari per capire quanto possano essere potenti le tracce digitali che lasciano, né quanto danno potrebbero causare, né tantomeno sanno quali dati vengono raccolti e da chi. Inoltre, i dati degli utenti valgono miliardi e c'è poco interesse alla trasparenza proprio perché, attraverso un utilizzo opaco dei dati degli utenti, molte aziende vendono pubblicità sulle proprie piattaforme.

Per comprendere i rischi, occorre aver consapevolezza che tutti i dati presenti nella Rete sono in mano a **due tipologie di entità** e, più precisamente: chi (persona o società) riceve i dati degli utenti (ad esempio Facebook o Google) e chi (persona o società), partendo da dati grezzi, genera informazioni (esempio le compagnie che producono giochi o ap-

VITA QUOTIDIANA

Facebook è un social media a scopo commerciale lanciato nel 2004 che, ad oggi, risulta essere il terzo sito più visitato al mondo dopo Google e YouTube. Ogni volta che un utente accede a Facebook – o a qualunque piattaforma – il sistema recupera e considera, dapprima, tutte le attività svolte (notizie cercate, foto pubblicate, ecc.); successivamente, sulla base di alcuni "segnali" registrati (orario, luogo di accesso, dispositivo, tipologia di contenuto, commenti, reazioni suscitate, ecc.), l'**algoritmo** di Facebook – espressione che fa riferimento a un procedimento di calcolo adoperato per la risoluzione di problemi – fa delle previsioni d'interesse personalizzate per ogni utente dando ad ognuna un punteggio di rilevanza: saranno queste, in base ai punti ottenuti, le notizie mostrate prioritariamente nella "Sezione Notizie" dell'utente (*news feed*) nei collegamenti successivi. Le aziende che utilizzano Facebook useranno poi tutte queste informazioni; così, ad esempio, analizzando con un apposito algoritmo, il "mi piace" di Facebook, è possibile profilare tutti gli utenti del servizio, raffinandone le identità digitali. **Il *like***, infatti, per Facebook **è un'interazione di gradimento da cui dedurre gli interessi dell'utente**. Anche Google memorizza tutto: conosce dove è stato l'utente, quello che ha cercato in Rete, ciò che ha cancellato e – sulla base di queste informazioni – ha un profilo pubblicitario di ognuno. I dati che Google ha su ogni utente sono infatti tantissimi (segnalibri, e-mail, contatti, file di Google Drive, video di YouTube, foto sul telefono, prodotti acquistati, dati del calendario, gruppi di Google cui si è iscritti, siti web creati, pagine condivise, quanti passi vengono fatti in un giorno, ecc.).

plicazioni per i social come Candy Crush). Questi soggetti sono di fatto aziende che cercano di estrarre quante più informazioni possibili dai dati al fine di venderle a terzi, molte volte all'insaputa dell'utente. **Questo meccanismo**, nelle mani sbagliate, **può portare anche a manipolare o polarizzare opinioni**; per questo, nel tempo, si è reso necessario un sistema di protezione dei dati.

Proteggere i dati personali degli utenti da utilizzi illeciti o che vadano a **violare la privacy** degli stessi è fondamentale. Il dato personale rappresenta lo strumento attraverso il quale i legislatori, nazionali e comunitari, tutelano l'insieme dei diritti collegati all'identità personale.

Dato personale **è qualsiasi informazione riguardante una persona fisica identificata o identificabile**, anche indirettamente, mediante informazioni supplementari; in particolare: **dati anagrafici** (nome, indirizzo e-mail, indirizzo di residenza, ecc.); **finanziari** (codice fiscale, conto corrente, ecc.); **identificativi** (video, foto, ecc.); **sensibili** (informazioni su opinioni politiche, religione, ecc.); **giudiziari** (processi, denunce, ecc.).

Il diritto alla protezione dei dati personali è sancito da numerose norme internazionali, dell'Unione europea e dei singoli Stati membri dell'Unione. A livello europeo, dal maggio 2018 è entrato in vigore un Regolamento, noto come **GDPR** (*General Data Protection Regulation*), che chiarisce come debbano essere trattati i dati personali degli utenti, introducendo **regole più chiare su informativa e consenso** e definendo i **limiti al trattamento automatizzato dei dati personali**; esso – inoltre – fissa norme rigorose per i **casi di violazione dei dati**.

In Italia, in materia di **diritto alla riservatezza informatica** legato alla diffusione nel web dei dati personali degli utenti, la Corte costituzionale ha affermato l'esistenza di «un vero e proprio diritto anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria» in considerazione delle disposizioni costituzionali degli articoli 15 (riservatezza e segretezza delle comunicazioni) e 21 (tutela della libertà di pensiero e di

VITA QUOTIDIANA

Nel marzo 2018, un'azienda di consulenza per il marketing online – la **Cambridge Analytica** – è stata al centro di un grosso scandalo per l'uso scorretto di un'enorme quantità di dati prelevati da Facebook durante la campagna presidenziale americana del 2016, che ha visto la vittoria di Donald Trump. L'accusa si è basata sull'uso scorretto delle informazioni raccolte dalla società: elaborate mediante algoritmi in grado di creare **profili psicometrici degli utenti** in termini di abilità, comportamenti e caratteristiche della personalità, oltre ad essere utilizzate per creare pubblicità altamente personalizzate su gusti ed emozioni degli utenti, sono servite anche a manipolare le preferenze degli elettori a favore di Trump, grazie alla diffusione di post e notizie false contro la candidata Hillary Clinton. Un'accusa simile è stata mossa alla stessa società in merito all'uso dei dati degli utenti per favorire l'uscita del Regno Unito dalla UE, in occasione del referendum del 2016.

parola). Secondo la Corte, nella disposizione costituzionale dell'articolo 15 «trovano protezione due distinti interessi: quello inerente alla libertà e alla segretezza delle comunicazioni riconosciuto come connaturale ai **diritti della personalità definiti inviolabili dall'articolo 2 della Carta costituzionale**, e quello connesso all'esigenza di prevenire e reprimere reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale». Tale diritto ha trovato ampia tutela nella legge 675 del 1996, confluita poi nel **Codice privacy**.

FOCUS DIRITTO (E DIRITTI)

Privacy e protezione dei dati personali

La **privacy**, tradizionalmente, è intesa come **diritto alla riservatezza**, cioè come **diritto della persona al controllo delle informazioni che la riguardano**.
In Italia, i fondamenti costituzionali sono ravvisabili negli artt. 14,15 e 21, rispettivamente riguardanti il domicilio, la corrispondenza e la libertà di manifestazione del pensiero; ma si può fare anche riferimento all'art. 2, incorporando la riservatezza nei diritti inviolabili dell'uomo. L'art. 2 è una vera e propria norma di apertura, che consente di attribuire i connotati di diritto fondamentale anche ad altre libertà e valori personali non espressamente tutelati dalla Costituzione, che, per i mutati costumi sociali, richiedono un riconoscimento pari a quello dei diritti espressamente delineati, come ad esempio il **diritto alla riservatezza informatica**.
La **tutela dei dati personali** è un allargamento del concetto di privacy che – basandosi sulla dignità di ogni persona – indica il diritto ad esercitare controllo sui propri dati personali (*data protection*). La dignità della persona umana, infatti, oltre che essere un valore dominante sia nella Convenzione europea dei diritti del 1950 (art. 8), che nel Trattato sul funzionamento dell'UE (art.16), nel costituire un **diritto fondamentale dell'individuo**, è anche un diritto autonomo rispetto al più generale diritto alla riservatezza (privacy).

Differenza tra privacy e diritto alla protezione dei dati personali:

- Il **diritto alla riservatezza** ha un'accezione più che altro negativa: non essendo un diritto a se stante, si pone come **limite alla libertà di espressione e al diritto all'informazione**. In questo senso, è il diritto a far sì che la stampa, o i media, non diffondano informazioni personali senza aver ricevuto preliminarmente il consenso dalla persona interessata (a meno che la notizia ad essa riferita sia di pubblico interesse); il diritto alla riservatezza rappresenta la facoltà di opporsi ad ogni ingerenza degli estranei nella vita privata di un individuo.
- Se la privacy rappresenta una tutela individuale, il **diritto alla protezione dei dati personali**, invece, va oltre la sfera della vita privata per includere, in particolare, le relazioni sociali e assicurare **autonomia decisionale e controllo sulla circolazione dei propri dati**. Il **diritto alla protezione dei dati personali** garantisce perciò la libertà personale, intesa non solo come libertà fisica ma anche come libertà da ogni controllo e intrusione altrui. Raffigura pertanto una tutela degli individui sia dalla diffusione impropria di informazioni da parte di giornali e media, sia – soprattutto – dai rischi di ingerenza nella propria sfera di libertà da parte di Stati autoritari. In base a tale diritto ogni individuo ha la facoltà di esigere che i propri dati personali vengano raccolti e trattati da terzi nel rispetto delle leggi in materia, sia dell'Unione europea che dei singoli Stati nazionali.

2 Proteggersi dalle insidie della Rete

Phishing È una truffa effettuata tramite la Rete Internet, che prevede l'invio di messaggi o e-mail che imitano per aspetto o contenuto le comunicazioni ufficiali di forniture di servizi (rete elettrica, banche, ecc.) per richiedere informazioni riservate (dati finanziari, codici di accesso, ecc.).

Navigare su Internet può essere utile e divertente, ma nella Rete si possono celare delle insidie. In Rete, gli imbrogli possono nascondersi sia nelle e-mail (phishing), sia sulle piattaforme di vendita online e persino sui social network. L'obiettivo di queste **frodi**, raggiri finalizzati al conseguimento di illeciti profitti, è **rubare dati personali** e quindi estorcere dei soldi con l'inganno.

Ad essere esposti ai rischi presenti in Rete sono tutti, ma proprio i cosiddetti **nativi digitali** – espressione che indica la generazione di chi è nato e cresciuto con la diffusione delle nuove tecnologie informatiche – pur mostrando di avere capacità operative circa l'uso del web, tuttavia, risultano essere spesso **carenti di consapevolezza critica** e quindi incapaci di valutare le informazioni della Rete o di prevedere le conseguenze delle pratiche online.

La cyberdipendenza, nota anche come ***Internet addiction disorder*** (in acronimo **IAD**) – espressione coniata dal medico Ivan Goldberg nel 1995 –, descrive il **disturbo legato ad utilizzo intensivo e ossessivo del web**: dalla navigazione sui social, alla visualizzazione di filmati, al gioco online. La "sindrome" di dipendenza dalla Rete presenta segni e sintomi paragonabili alla dipendenza da alcool, droga e gioco d'azzardo patologico. Si parla di **dipendenza** (e non di sola abitudine) quando l'alterazione del comportamento è accompagnata da sintomi quali disturbi del sonno, aggressività, deconcentrazione, difficoltà a relazionarsi, isolamento, depressione, ansia, instabilità emotiva.

La dipendenza da Internet ha varie sfumature. Una è la **nomofobia** – termine formato da un prefisso inglese, abbreviazione di *no-mobile*, e il suffisso *-fobia* – per indicare la paura incontrollata di essere sconnessi dalla Rete di telefonia mobile e non poter, dunque, chattare con amici e parenti. La paura di essere disconnessi può portare a vivere momenti di ansia, malessere, irrequietezza e aggressività.

La nomofobia, così come gli altri disturbi legati alla Rete, tende a minare non poco la vita di relazione; nel corso degli ultimi anni, anche in Italia è

VITA QUOTIDIANA

«**Together for a better Internet**» è il motto del *Safer Internet Day* (SID), evento annuale, organizzato a livello internazionale con il supporto della Commissione europea. Nato nel 2004 per promuovere un uso più sicuro e responsabile del web e delle nuove tecnologie tra i bambini e i giovani di tutto il mondo, l'evento è finalizzato a **far riflettere i ragazzi non solo sull'uso consapevole della Rete, ma sul ruolo attivo e responsabile di ciascuno nella realizzazione di Internet come luogo positivo e sicuro**. L'obiettivo non è contrastare le nuove tecnologie, bensì sfruttare a pieno le grandissime possibilità che le stesse offrono, ma con consapevolezza e considerando anche i rischi. Lo spirito di fondo è quello di credere che insegnare le dinamiche delle app o dei social network non sia molto diverso dall'educazione stradale: apprendere le potenzialità e i pericoli della Rete è semplice e indispensabile come imparare ad attraversare la strada.

esploso il fenomeno dei **ritirati sociali**, espressione che traduce il termine giapponese ***hikikomori*** usato per indicare gli adolescenti che respingono il contatto con gli altri preferendo vivere isolati nelle loro camere. I "ritirati sociali" sono spesso giovani dipendenti dalla **Rete** e **nomofobici**, a volte anche vittime di bullismo. La cyberdipendenza non riguarda solo il mondo dei giovani, ma investe anche gli adulti, tanto che l'Organizzazione Mondiale della Sanità ha consigliato di **non superare le 2 ore giornaliere davanti allo schermo** per non avere conseguenze cerebrali.

Gli adolescenti in Rete, secondo i dati di una ricerca italiana svolta nel 2016 dal MIUR insieme ai principali atenei e il portale Skuola.net

- 7 giovani su 10 hanno un **profilo attivo sui social network**
- solo **1 giovane ogni 16 non accede mai ad Internet**
- 8 giovani su 10 usano abitualmente **WhatsApp** per comunicare coi genitori e persino scambiarsi compiti e appunti coi compagni di scuola
- 4 giovani su 10 dicono di non conoscere di persona almeno la metà dei loro amici su **Facebook**
- 7 giovani su 10, quando vanno a scorrere la lista dei loro follower su Instagram, scoprono numerosi **profili falsi**
- 1 giovane su 4 confessa di non essersi mai preoccupato più di tanto di come vengano diffuse le sue **informazioni personali** sul web
- **9 giovani su 10 usano Internet senza alcun controllo** da parte dei genitori, e circa la metà di loro vi ha libero accesso **fino a tarda notte**

VITA QUOTIDIANA

La nostra vita privata e pubblica è indubbiamente mutata con l'avvento di **Internet**, tanto che il numero delle famiglie italiane che possono accedere alla Rete da casa è in costante aumento (secondo recenti stime l'89% accede al web da casa). L'utilizzo di Internet coincide però soprattutto con quello dei social network da parte dei giovani (Facebook, Instagram, Twitter, YouTube). Secondo una ricerca del 2018 dell'Associazione nazionale sulle dipendenze tecnologiche, **DiTe**, **il 51% dei giovani tra i 15 e i 20 anni controlla mediamente lo smartphone 75 volte al giorno**. Non solo: il 7% lo fa fino a 110 volte. Il **79%** di essi ammette di non riuscire a starne alla larga per almeno 3 ore. Il bisogno di inviare messaggi e chattare si sente anche di notte. Il 13% degli intervistati (23.000 giovani tra gli 11 e i 26 anni) trascorrono online **più di 10 ore al giorno**, con un costo sulla vita di relazione e sulla salute. Sempre più frequentemente la cronaca riporta episodi con ragazzini colpiti da crisi epilettiche per aver trascorso **fino a 20 ore al giorno di fronte a uno schermo**; donne che si innamorano di foto rubate; uomini che hanno rinunciato al proprio benessere per investire tutto nel gioco; bambini a rischio, se affidati alla baby-sitter digitale, di avere delle aree compromesse del cervello deputate allo sviluppo della concentrazione e della memoria.

Offendere un soggetto ritenuto più debole e incapace di difendersi è l'espressione caratterizzante ogni fenomeno di **bullismo** che, se attuato mediante gli strumenti della Rete (e-mail, telefono, blog, chat, ecc.) diventa cyberbullismo. Se nel bullismo tradizionale l'atteggiamento aggressivo ripetitivo implica un rapporto faccia a faccia tra il bullo e la vittima, nel cyberbullismo gli atti di molestia sistematici vengono attuati da un bullo che ha l'occasione di rimanere anonimo sollecitando il coinvolgimento di altri "amici" anonimi, in modo che la vittima spesso non è neanche a conoscenza dell'identità di coloro con i quali sta interagendo. Il cyberbullismo rispetto al bullismo è molto **più infido** in quanto la presa in giro o l'insulto entra all'interno del vasto mondo della Rete dove sono presenti tantissime persone ed è difficile che un messaggio passi inosservato: foto, video e commenti, infatti, possono permanere in Rete anche dopo essere stati eliminati dal diretto interessato. Grazie ad una connessione sempre attiva è possibile attaccare persone più deboli e delicate come possono essere proprio **i giovani adolescenti che non hanno ancora sviluppato una personalità forte e definita** per difendersi nella giusta maniera. Conoscere i pericoli del web e i meccanismi scorretti che si celano dietro la Rete è un primo modo per riuscire a difendersi dal cyberbullismo; allo stesso modo – è importante conoscere i **tratti distintivi del cyberbullismo rispetto al bullismo**.

Cyberbullismo Il cyberbullismo, all'art. 1 comma 2 della legge n. 71 del 2017, è stato definito come «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».

LE PRINCIPALI CATEGORIE DEL CYBERBULLISMO

- **Flaming** (dall'inglese: *flame*, 'fiamma'): caratterizzato da messaggi online violenti e volgari ai danni del soggetto
- **Molestie** (*harassment*): insulti gratuiti ai danni di un soggetto
- **Denigrazione**: sparlare per ledere la reputazione altrui. La denigrazione è la forma di cyberbullismo più comunemente utilizzata dagli studenti contro i loro docenti
- **Esclusione**: escludere deliberatamente una persona da un gruppo online provocando la sua emarginazione volontaria
- **Sostituzione di persona** (*impersonation*): passare per un'altra persona e creare confusione
- **Inganno** (*trickery*): ottenere la fiducia di qualcuno con l'inganno e poi pubblicare del materiale che non ci appartiene
- **Doxing**: diffusione pubblica di dati personali e sensibili, tramite il web
- **Minacce di morte**: la più crudele, perpetrata a danni di soggetti terzi, sempre via web

Il **cyberbullismo è un reato**, cioè un comportamento ritenuto socialmente pericoloso e perciò punito con una sanzione.

La legge n. 71 del 2017 – contenente *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo* – **dispone non solo un sistema di repressione ma anche di prevenzione ed educazione** con il coinvolgimento della scuola. Il provvedimento, infatti, intende contrastare il fenomeno con azioni a carattere preventivo e con una strategia di cura, tutela ed educazione nei confronti dei minori coinvolti, puntando sulla formazione specifica degli insegnanti allo scopo di prevenire e sensibilizzare i minori, nonché incoraggiando un percorso di responsabilizzazione nell'uso dei sistemi informatici e di Rete (**educazione digitale**). Al fine di rispondere alle indicazioni della legge, **in ogni istituto scolastico** viene individuato, tra il corpo docente, **un referente** con il compito di coordinare le varie iniziative, con la **collaborazione anche della Polizia postale e dei servizi** presenti sul territorio; se il dirigente scolastico viene a conoscenza di atti di cyberbullismo deve immediatamente informare i genitori dei minori coinvolti con previsione di **sanzioni disciplinari** commisurate alle gravità degli atti compiuti.

BULLISMO	CYBERBULLISMO
I bulli sono **persone conosciute** dalla vittima (compagni di scuola o di Istituto)	I cyberbulli possono essere **perfetti sconosciuti**
Le azioni sono generalmente raccontate ad altri studenti della scuola e perciò restano **circoscritte nello spazio**	Il materiale cyberbullistico può essere diffuso **in tutto il mondo**
La **disinibizione è media**, incalzata dalle dinamiche del gruppo e dai meccanismi di disimpegno morale	La **disinibizione è alta** e i cyberbulli tendono a fare online ciò che non farebbero nella vita reale; chiunque, anche chi è vittima nella vita reale o ha un basso potere sociale, potrebbe diventare un cyberbullo
Il bisogno di dominare nelle relazioni interpersonali è correlato alla **visibilità** del bullo	Il cyberbullo usa la presunta **invisibilità** per esprimere potere e dominio
Il bullo non presta sufficientemente attenzione ai **feedback tangibili** da parte della vittima	La **mancanza di feedback** frena la comprensione empatica della sofferenza provata dalla vittima
Nel bullismo **c'è sempre deresponsabilizzazione** ("Stiamo scherzando", "Non è colpa mia")	Nel cyberbullismo **è possibile la depersonalizzazione** mediante avatar (alter ego virtuale) appositamente creati
Gli **spettatori sono sempre presenti** e osservano i comportamenti prevaricatori dei bulli nei confronti di una vittima che conoscono	Gli **spettatori possono essere assenti, presenti, conoscere la vittima o ignorare la sua identità**. Quando presenti, possono, assumere una **funzione passiva** (se si limitano a rilevare, nelle proprie e-mail, SMS, chat, atti di cyberbullismo diretti ad altri) o **attiva** (se scaricano il materiale, lo segnalano ad altri amici, lo commentano e lo votano, diffondendolo). Il contributo attivo può essere fornito su sollecitazione del cyberbullo (**reclutamento volontario**) oppure su spinta autonoma, senza, cioè, aver ricevuto specifiche ed espresse richieste (reclutamento involontario)

La legge citata, in caso di azioni di cyberbullismo tra ultraquattordicenni, attribuisce al Questore massima autorità di pubblica sicurezza, l'onere di ammonire, con **avvertimento verbale**, l'autore dei comportamenti affinché non li possa mettere più in atto, nonché accertare e reprimere tutti i comportamenti illeciti commessi al fine di proteggere le vittime. La procedura di ammonimento del minore – alla presenza di uno dei genitori o ad altra persona esercente la responsabilità genitoriale – è possibile solo se non viene presentata una querela o denuncia da parte della vittima. Successivamente all'ammonimento si inizia un **percorso di riabilitazione** presso uno dei Centri per la promozione della mediazione presenti sul territorio italiano al fine di gestire pacificamente i conflitti. L'ammonimento rende la normativa poco "repressiva" e molto "educativa".

Non è sempre facile tracciare una linea di demarcazione tra le molestie in Rete che spesso assumono declinazioni differenti ma con il comune obiettivo di perseguitare il soggetto preso di mira. Tra le molestie in Rete, segnaliamo anche le seguenti.

Il *cyberstalking*: si verifica quando la persecuzione online incessante punta a spaventare la vittima con minacce, anche di violenza fisica. In questo caso, il *cyberstalker*, oltre a minacciare la vittima di aggressioni fisiche, può diffondere materiale riservato in suo possesso (fotografie sessualmente esplicite, videoclip intimi, manoscritti personali) nella Rete. Lo stalker è in genere una persona che agisce sulla spinta di sentimenti ossessivi e per desiderio di controllo e possesso; per questo il fenomeno si presenta tipicamente in **relazioni fortemente conflittuali** tra coetanei o nel caso di **rapporti sentimentali interrotti**. Le persecuzioni possono avvenire attraverso un accesso illegale ai dispositivi elettronici delle vittime, ad esempio con invio di e-mail contenenti codici malevoli o mediante il bluetooth, per installare software *spyware* il cui scopo è raccogliere informazioni al fine di controllare il registro delle chiamate o la lettura dei messaggi, l'agenda degli impegni, ecc. La tecnologia, però, ha anche sviluppato strumenti di contrasto per arginare il fenomeno del *cyberstalking*, con programmi di difesa che permettono di bloccare i software *spyware* progettati per monitorare senza permesso le attività in Rete degli utenti.

Il *revenge porn* – per ripicca e ritorsione nei confronti della persona coinvolta – è la **condivisione pubblica tramite il web di immagini intime esplicite**, senza alcun consenso del protagonista delle stesse. Vera e propria **molestia online**,

VITA QUOTIDIANA

In base ai dati presentati in occasione del ***Safer Internet Day 2018***, ovvero la Giornata mondiale per la sicurezza in Rete, è stato possibile evidenziare l'aumento del numero di denunce da parte dei minori; queste, infatti, dalle 236 del 2016 sono passate a oltre 350 nel 2017. Inoltre, delle 354 denunce trattate dalla Polizia postale, 13 sono denunce di minori per **stalking**, 87 per **diffamazione online** e 79 per **furto d'identità su social network**. I minori denunciati come responsabili di azioni di cyberbullismo sono stati 39, di cui: 13 per **diffusione di materiale pedopornografico**, 12 per **diffamazione online** e 11 per **ingiurie, minacce e molestie**. Tutto ciò significa che se – da un lato – le angherie, le aggressioni, le molestie sui minori sono aumentate, è aumentato anche il numero di coloro che hanno avuto la forza di denunciare.

questo tipo di aggressione ha conseguenze devastanti per le vittime, tanto da aver indotto il legislatore italiano ad introdurre un'apposita norma all'interno della sezione del Codice penale, dedicata a punire questo tipo di reato al pari degli altri delitti contro la libertà morale e di autodeterminazione dell'individuo. La norma – nel tutelare altresì l'onore, il decoro, la reputazione e la privacy di una persona – **inasprisce le sanzioni** nel caso in cui l'autore del reato sia il coniuge, anche separato o divorziato, della persona offesa o soggetto che è o è stato ad essa legato da relazione affettiva, o se i fatti sono commessi mediante strumenti informatici o telematici (cosiddetta **aggravante social**).

FOCUS DIRITTO (E DIRITTI)

Molestie online: i consigli della Internet Society

Le molestie online sono in aumento. La forma di tutela più efficace è sicuramente l'**autotutela**, cioè la gestione attenta dei propri dati personali, ma l'**Internet Society**, un'organizzazione internazionale nata per promuovere lo sviluppo aperto, l'evoluzione e l'uso di Internet per il bene della popolazione di tutto il mondo, ha emanato i seguenti consigli:

1. **Conoscere il mezzo**. Il web è un potente strumento per la comunicazione. È importante imparare come utilizzarlo, tenendo bene gli occhi aperti per sfruttare al meglio ciò che offre.
2. **Mantenere privata la propria vita**. Tenere le informazioni personali separate dal ruolo professionale, usando profili diversi per ruoli diversi.
3. **Proteggere le comunicazioni**. È importante utilizzare la **crittografia** (sistema pensato per rendere incomprensibile un messaggio a chi non possiede la soluzione per decodificarlo) e l'**access control** (meccanismo di autorizzazioni per controllare l'accesso ai dati e prevenire eventuali fughe di informazioni o accessi non autorizzati).
4. **Oscurare la posizione**. È importante rimuovere i dati sulla posizione da immagini e video prima di pubblicare. Disattivare la geolocalizzazione dei post e non rivelare la propria posizione nei post pubblici.
5. **Proteggere i dispositivi**. È importante proteggere i dispositivi da manomissioni fisiche e digitali utilizzando la crittografia, password forti e mailbox sicure.
6. **Tutelarsi da un possibile attacco**. È importante trovare alleati e preparare un piano per affrontare le molestie online, il *doxing* (dossieraggio) e altre forme di abuso.
7. **Non lasciare spazio al cyberbullismo**. È importante mostrare coraggio e non aver paura chiedendo anche un eventuale aiuto agli altri.
8. **Attenzione ai virus, alle e-mail di *phishing* e ai documenti consultati**. È importante controllare prima di connettersi con qualcuno che non si conosce. Se qualcosa sembra troppo bello per essere vero, probabilmente non lo è.
9. **Condividere la propria esperienza con gli altri**. È importante far sapere alla gente la propria disponibilità ad aiutare.
10. **Proteggere gli altri**. È importante, se si ospitano contenuti generati dagli utenti, impedire di pubblicare messaggi offensivi. Rimuovere le informazioni personali che sono state esposte per ferire qualcuno e segnalare i trasgressori.

3 Gestire le informazioni reperibili in Rete

La quantità di dati in Rete (foto, immagini, musica, testi, ecc.) espone l'utente al rischio di un **utilizzo illecito** delle stesse perché erroneamente considerate libere di essere usate senza rispettare i diritti dei legittimi proprietari che, al contrario, godono di una particolare tutela, quella del diritto d'autore.

Nell'ordinamento giuridico italiano **il diritto d'autore** – conosciuto anche con il termine anglosassone **copyright** e abbreviato con il simbolo © – è in generale ammesso per qualunque **opera dell'ingegno** che sia contraddistinta da creatività. Chi crea un'opera intellettuale, pertanto, è titolare sia del diritto di essere riconosciuto autore dell'opera, sia del diritto di utilizzare l'opera in ogni forma e modo e di sfruttarla economicamente. Quest'ultimo diritto ha una natura patrimoniale e dura non solo per tutta la vita dell'autore, ma anche per 70 anni dopo la sua morte a favore degli eredi; dopo tale periodo l'opera può essere utilizzata da chiunque. Si configura la **violazione del diritto d'autore** se l'opera è sottoposta a **plagio** (cioè riprodotta, in tutto o in parte, senza riconoscere la paternità all'autore), o **riprodotta a fini commerciali** (cioè duplicata e venduta senza l'autorizzazione dell'autore), o **modificata senza autorizzazione** (cioè ritoccata senza il permesso dell'autore).

Con l'avvento della Rete, è possibile creare, pubblicare e diffondere in forma digitale un'opera tutelata dal copyright, così che la tutela del diritto d'autore si è estesa e non è più limitata alla sola materialità dell'opera (ad esempio, il divieto di fotocopiare testi). Chiunque componga una canzone, scatti una foto, scriva un testo, pubblicando il frutto della propria attività in Rete, se associa un copyright alla propria opera è quindi tutelato dal diritto di autore; **utilizzare tali opere, senza il permesso dell'autore è una violazione**.

La **pirateria online** è un atto illecito adoperato per identificare una serie di condotte.

Secondo la legge sul **diritto d'autore**, il **download illegale** di un prodotto protetto da copyright è punibile con una sanzione economica; qualora al download di materiale protetto segua la condivisione dello stesso a scopo di lucro, **il pirata online rischia la sanzione penale**. Le norme italiane, infatti, considerano un illecito la condivisione di opere coperte da copyright attraverso attività di ***file sharing*** che, se a scopo di lucro, sono punite con sanzioni pesanti: dalla multa alla detenzione dai 6 mesi ai 3 anni. La ragione sta nel fatto che il download illegale non solo danneggia l'autore dell'opera, ma – se condiviso al fine di trarre profitto – arreca un danno patrimoniale senz'altro maggiore. Non sono i programmi di *file sharing* ad essere illegali, ma l'utilizzo che di essi viene fatto. Sarebbe infatti illegale anche la diffusione di copie di un prodotto acquistato regolarmente.

Lo **streaming** (dall'inglese *to stream*, ovvero 'far fluire') è una **tecnologia per la trasmissione via Internet di dati, in genere segnali audio e video**; grazie a questo sistema i dati possono essere riprodotti progressivamente (su computer, tablet o smartphone) senza necessità di essere scaricati. Lo streaming però non è consentito se non è proveniente da chi è autorizzato a detenere e trasmettere quei dati; bisogna pertanto distinguere tra l'utente che si limita ad usufruire del servizio guardando il contenuto offerto e colui che, al contrario, è titolare del sito streaming. Nel caso in cui il filmato è protetto da copyright e non si hanno le licenze per trasmetterlo, l'internauta che si limita a guardare il video non commette alcun illecito, mentre colui che offre il servizio, al contrario, incorre nelle sanzioni sopra viste per il *file*

sharing, con le differenze di pena dovute dalla presenza o meno del fine di lucro. Lo streaming di opere protette, qualora non autorizzato, costituisce quindi una violazione dei diritti d'autore, al pari del download illecito.

VITA QUOTIDIANA

Negli ultimi anni, la Guardia di Finanza, a seguito di apposite autorizzazioni giudiziarie, è sempre più frequentemente chiamata a intervenire per oscurare i siti illegali che offrono contenuti in streaming e download. In tutte queste operazioni, le forze dell'ordine si sono concentrate prevalentemente nell'individuazione di coloro che offrivano questi servizi e non sull'utente finale. Tentare di perseguire migliaia di utenti sarebbe stato del resto veramente complicato, a meno di non trovarsi di fronte a soggetti che, a loro volta, condividono in Internet i contenuti scaricati illegalmente. Nel 2018 il Parlamento italiano ha emanato una nuova legge che autorizza l'**AGCOM**, cioè l'Autorità per le garanzie nelle telecomunicazioni, a intervenire in modo più tempestivo contro le violazioni del diritto d'autore online, oscurando in modo autonomo i domìni che ospitano portali di streaming illegali.

Il diritto d'autore ha, come già detto, una natura patrimoniale; l'eventuale cessione di questi diritti può avvenire solo tramite un contratto, detto **licenza**, che specifica la modalità e i limiti di utilizzazione. Queste regole valgono anche per i software che, trattati come un qualunque bene, ne vietano l'uso senza il consenso dell'autore. Per poter guadagnare sul programma, infatti, l'autore può cedere a terzi il suo utilizzo sotto particolari condizioni. Per alcuni produttori, invece, il software è da considerarsi un bene pubblico e – in quanto strumento capace di contribuire all'evoluzione culturale e sociale della società – deve essere libero e gratuito; è questo il caso del cosiddetto ***open source***.

VITA QUOTIDIANA

La Corte di Cassazione, nel 2012, ha confermato la sentenza di condanna per un imprenditore che aveva duplicato dei software di cui aveva acquistato regolare licenza. La duplicazione dei programmi utilizzati su vari e differenti personal computer ha, secondo la Corte di Cassazione, violato la norma del diritto d'autore perché l'imprenditore doveva acquistare licenze diverse per ogni singolo computer e non utilizzare la stessa licenza per tutti.

GUIDA ALLO STUDIO

Rispondi oralmente o per iscritto alle domande o individua e sottolinea nel testo la risposta:

- Cos'è l'identità digitale? Perché occorre difenderla?
- Cosa determina il *digital footprint*?
- Quali sono le norme che tutelano i dati personali? Perché?
- Quali sono le principali insidie presenti nella Rete?
- Cosa differenzia e caratterizza il cyberbullismo dal bullismo?
- Come gestire le informazioni presenti in Rete?

Analisi e produzione di un testo argomentativo (tipologia B)

L'essere connessi, ovvero sviluppare e mantenere relazioni positive tra pari, rappresenta un aspetto cruciale per gli adolescenti nel formare la propria identità, contribuendo al loro benessere psicologico. Nel lento e faticoso percorso di costruzione della propria identità, gli adolescenti hanno bisogno di svincolarsi dall'influenza dei genitori e le relazioni con gli amici diventano un 'utero sociale' in cui essere accolti e rassicurati [...]. Ai nostri giorni questo bisogno di essere connessi e in relazione con i pari si declina anche attraverso l'uso delle tecnologie, essere connessi diventa quindi partecipare a social network e a gruppi WhatsApp. [...] Le relazioni, sia quelle reali che quelle virtuali, sono il luogo dove gli adolescenti raccontano e svelano qualcosa di sé (*self-disclosure*) [...]. Raccontare qualcosa di sé è una dimensione positiva e necessaria per sviluppare relazioni più intime e più vere e per mantenere queste relazioni nel tempo. L'utilizzo della rete può in alcuni casi essere positivo, come nel caso di ragazzi che attraverso blog o brevi video su YouTube esprimono i loro desideri e i loro talenti. Tuttavia, se in passato l'adolescente sperimentava gruppi allargati (ad esempio tifoserie, movimenti giovanili), gruppi più piccoli (amici più stretti con rapporti più intimi) e rapporti diadici [...] in cui poter esercitare a livelli diversi la possibilità di aprirsi e di confidarsi, oggi con le tecnologie questi diversi gruppi si sovrappongono e si contaminano e agli adolescenti vengono richieste competenze sociali nuove, che prima non erano necessarie con piccoli gruppi di amici [...]. Raccontare qualcosa di sé agli altri attraverso la rete può diventare molto pericoloso, ad esempio quando gli adolescenti utilizzano le loro bacheche e i loro profili come diari segreti. I segreti intimi, i pensieri ancora non elaborati e le difficoltà possono diventare pubblici per reti amplissime di persone, rendendo vulnerabile l'adolescente. Questo meccanismo viene definito disinibizione on line [...]. Al chiuso della propria stanza gli adolescenti non sono consapevoli di chi leggerà il proprio post, non vedono volti e persone, ma solo uno smartphone o un computer con la percezione di parlare con se stessi. [...] [Un altro aspetto] ci porta a riflettere sul ruolo delle tecnologie e delle informazioni veicolate dai social network nel formare la mente degli adolescenti; sappiamo infatti che in adolescenza la struttura e il funzionamento del cervello vanno incontro a numerosi cambiamenti [...]. L'utilizzo delle tecnologie e della rete ha dei vantaggi importanti per gli adolescenti perché permette loro di cercare informazioni sugli ultimi avvenimenti, svolgere ricerche per la scuola, cercare notizie che riguardano la salute [...]. Accanto a questi vantaggi, emergono tuttavia alcuni rischi. Il primo rischio è quello della non veridicità delle informazioni. Soprattutto in riferimento alla salute, alcune informazioni legate al controllo del peso o legate alla sessualità possono essere sbagliate, inducendo l'adolescente a comportamenti pericolosi [...]. Il secondo rischio è quello dell'omologazione del pensiero. Il pensiero morale dell'adolescente può formarsi a partire da informazioni diffuse attraverso social network, ma anche attraverso video divulgati in rete, creando false credenze, diminuendo la capacità di discernimento e modificando le norme sociali. L'insieme di queste riflessioni indica la necessità che gli adulti si riapproprino della loro funzione educativa nell'accompagnare gli adolescenti nella vita on line, promuovendo al massimo le potenzialità della rete e riducendone i rischi. L'utilizzo della rete e dei social network è parte dell'esperienza di socializzazione dell'adolescente che gli adulti hanno il compito di conoscere e comprendere.

[Testo tratto da *Essere connessi in adolescenza tra nuove possibilità e rischi: il ruolo degli adulti* di Annalisa Guarini, Antonella Brighi, Alessandra Sansavini, in «Studi e Documenti», n. 16, Rivista online dell'Ufficio Scolastico Regionale per l'Emilia-Romagna, marzo 2017]

COMPRENSIONE E ANALISI

1. Nel testo viene sottolineato come le relazioni positive negli adolescenti sono importanti per lo sviluppo della propria identità anche quando queste avvengono attraverso l'uso delle nuove tecnologie. Quali argomenti vengono addotti per sostenere questa tesi?
2. Le autrici, nel corso del saggio, affermano che – per gli adolescenti – raccontare qualcosa di sé è una dimensione positiva e necessaria, ma «raccontare qualcosa di sé agli altri attraverso la rete può diventare molto pericoloso» (riga 17). Perché? Quale condizione viene a mancare in Rete?
3. Seppur complessivamente positivo, il ruolo delle tecnologie e delle informazioni veicolate dai social per gli adolescenti presenta delle criticità. Quali sono? Perché?
4. Nel testo si afferma che l'utilizzo della Rete e dei social network è parte dell'esperienza di socializzazione dell'adolescente. Secondo le autrici, gli adulti hanno il compito di conoscere e comprendere quale compito spetta agli adulti?

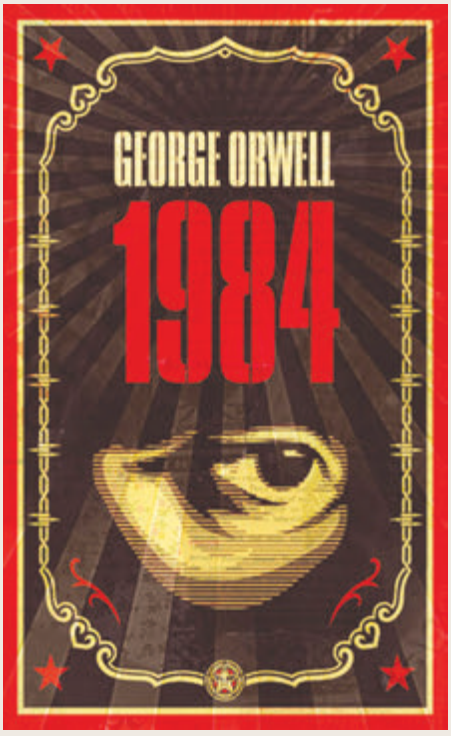
PRODUZIONE

Condividi le considerazioni espresse nel saggio relativamente alla positività dei social nella vita degli adolescenti? In base alle tue esperienze, dirette o indirette, è corretto sostenere che informarsi solo attraverso Internet ha, per un adolescente, il rischio dell'omologazione del pensiero, cioè il rischio di uniformarsi alle tendenze dominanti senza alcuna capacità di critica?

- Argomenta i tuoi giudizi con riferimenti alla tua esperienza e alle tue conoscenze e scrivi un testo in cui tesi e argomenti siano organizzati in un discorso coerente e coeso.

Simulazione di colloquio

Finalità specifica del colloquio dell'Esame di Stato è consentire alla Commissione di verificare l'acquisizione dei contenuti e dei metodi delle discipline, nonché la capacità, critica e personale, di argomentare del candidato. È importante curare la capacità di esposizione e la coerenza delle argomentazioni esposte. L'esercizio da fare è, quindi, costruire una mappa concettuale, preferibilmente interdisciplinare, che consenta di fare collegamenti coerenti con il tema proposto.



ESEMPIO A

Per avviare il colloquio, il materiale scelto dalla Commissione è una delle immagini di copertina del romanzo *1984* di George Orwell, pubblicato nel 1949. Il romanzo descrive – in un futuro dispotico caratterizzato da un permanente stato di guerra – il controllo da parte di un'entità nascosta che non appare mai (il Grande Fratello), ma che controlla azione e pensiero di ogni abitante in qualsiasi momento e in ogni luogo attraverso teleschermi posti in tutto il paese, e l'alterazione della realtà mediante un meccanismo di manipolazione della mente, Il romanzo di Orwell è spesso citato come metafora di ciò che la società di oggi punta a diventare utilizzando metodi sottili e subdoli

con i quali imporre la volontà di poche persone in maniera assolutistica. *1984* è un romanzo spesso accostato al problema del controllo dei mezzi di informazione nella realtà moderna. «La guerra è pace, la libertà è schiavitù, l'ignoranza è la forza», sostiene il regime del Grande Fratello. Oggi, la diffusione delle *fake news*, e della cosiddetta post verità, sono il segno che Orwell aveva previsto tutto.
La scelta della Commissione è uno spunto per consentire al candidato di esporre le sue conoscenze sull'importanza delle **competenze nella società dell'informazione**.

Di seguito la **scaletta dei contenuti**, trattati nel corso della lezione, cui fare riferimento per affrontare il tema:

- L'avvento di Internet e la diffusione e l'utilizzo di informazioni, conoscenze e saperi tecnologicamente avanzati.
- McLuhan, il villaggio globale e la problematica relativa al modo in cui i media possono plasmare la nostra comprensione («il medium è il messaggio»).
- L'importanza della competenza digitale per un approccio critico, etico, sicuro e responsabile nell'utilizzo della Rete come fonte di conoscenze e informazioni.
- I pericoli della Rete e la necessità di proteggersi dalle sue insidie.
- Il problema degli *hate speaches*, dei *trolls* e delle *fake news*.

ESEMPIO B

Per avviare il colloquio, il materiale scelto dalla Commissione è l'immagine di un occhio all'interno dei principali ***widget*** che rappresentano i diversi social. La scelta della Commissione è uno spunto per consentire al candidato di esporre le conoscenze sul tema della **dispersione dei dati personali durante la navigazione in Rete e loro protezione**.

Di seguito la **scaletta dei contenuti**, trattati nel corso della lezione, cui fare riferimento per affrontare il tema:

- Nozione di identità digitale.
- Il valore della profilazione degli utenti per i gestori dei social network.
- Relazione tra *digital footprint* e pubblicità comportamentale.
- Nozione di dato personale e sistemi di protezione della privacy.
- Il Regolamento europeo GDPR.