I rischi della rete

I «Nuovi Media»

Internet e cellulari e più in generale i cosiddetti “Nuovi media” rappresentano un aspetto esistenziale importante nella vita dei giovani della società contemporanea.

I ragazzi e le ragazze di oggi nascono e crescono insieme ad Internet e al cellulare, e i Nuovi Media fanno parte della loro quotidianità.

I Nuovi Media rappresentano un nuovo modo di comunicare con gli altri; aprono ad un mondo di relazioni, di emozioni, di scambio di informazioni e di apprendimento che offre, in particolare ai giovani, opportunità di crescita senza precedenti. Inoltre, mettendo a disposizione diverse opportunità di relazione e di comunicazione, i Nuovi Media attivano nuove strategie e percorsi di identificazione, di rappresentazione del sé e della propria realtà di riferimento, contribuendo ad edificare valori e categorie simboliche, attraverso i quali interpretare la realtà e se stessi.

La sicurezza online

I Nuovi Media, pongono però delle questioni associate al problema della sicurezza: siamo infatti di fronte ad una realtà complessa, apparentemente priva di regole, nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi per lo sviluppo dei più giovani.

I ragazzi e le ragazze, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti.

Per questo motivo, la Commissione Europea ha scelto di finanziare progetti per promuovere un uso sicuro e responsabile dei nuovi media da parte dei giovani.

La privacy ai tempi di internet

La privacy è il diritto alla riservatezza della propria vita privata e al controllo dei propri dati personali.

A dichiararlo è il codice privacy (Decreto Legislativo n. 196/2003, codice in materia di protezione dei dati personali) la cui finalità è garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato (con riferimento alla riservatezza), dell'identità personale e del diritto di protezione dei dati personali.

Il concetto di privacy è dunque correlato a quello di dato personale, che rappresenta ogni informazione che sia relativa all'identità della persona, attraverso la quale è identificata o identificabile.

Cos’è la Privacy

Include:

- **DATI ANAGRAFICI** (nome e cognome, indirizzo mail, indirizzo di residenza e/o domicilio, numero di telefono, ecc.)
- **DATI FINANZIARI** (codice fiscale, conto corrente, numero carta di credito, ecc.)
- **DATI IDENTIFICATIVI** (fotografie, video e qualsiasi cosa permetta l’identificazione diretta dell’interessato);
- **DATI SENSIBILI** (informazioni utili a rivelare nazionalità, opinioni politiche, convinzioni religiose, ecc.)
- **DATI GIUDIZIARI** (processi, denunce, ecc.)

Il codice Privacy

In sintesi, il codice privacy individua e tutela i dati… ...

- **PERSONALI** ossia relativi a persona fisica e/o giuridica, ente o associazione – identificati o identificabili anche indirettamente – mediante riferimento a qualsiasi altra informazione compreso un numero di identificazione personale. ...
- **ANONIMI** vale a dire le informazioni che, in origine o a seguito di indagini, possano essere associate a un interessato identificato o identificabile ...
- **IDENTIFICATIVI** cioè utili all'identificazione diretta dell'interessato. ...
- **SENSIBILI** ossia idonei a rivelare l'etnia, l'orientamento sessuale, filosofico, religioso o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni e organizzazioni di ogni natura, lo stato di salute. ...
- **GIUDIZIARI** vale a dire ogni informazione inerente alla qualità di imputato o di indagato, al casellario giudiziario e all'anagrafico relativo alle sanzioni amministrative dipendenti da reato e di eventuali carichi pendenti. ...
- **STATISTICI** e/o di carattere tematico, per esempio le informazioni contenute nelle banche dati e/o in qualsivoglia complesso organizzato.

Consigli da dare agli studenti

- **EVITATE** DI DIFFONDERE IN RETE INFORMAZIONI PERSONALI, COME L'INDIRIZZO DI CASA O LA SCUOLA CHE FREQUENTATE.
- **PROTEGGETE** I VOSTRI DATI SENSIBILI PER EVITARE SPAM O ALTRI TIPI DI TRUFFE (COME RICERCHE DI MARKETING NON AUTORIZZATE).
- **PARLATE** COI VOSTRI AMICI DI COME GESTITE LE FOTO E DITEGLI DI CHIEDERVI IL PERMESSO PRIMA DI POSTARE IMMAGINI CHE VI RITRAGGONO.
- **CREATE** PASSWORD COMPLESSE, CONTENENTI MAIUSCOLE, MINUSCOLE, NUMERI E SIMBOLI.
- **NON RIVELATE** LE VOSTRE PASSWORD A NESSUNO.
- **CONTROLLATE** LE IMPOSTAZIONI DELLA PRIVACY NEI VOSTRI SOCIAL NETWORK E, SE POSSIBILE, RAFFORZATELE.

Web reputation

A differenza di quanto succedeva prima della diffusione di massa di Internet e dell'accesso sempre più facile a dispositivi ormai tutti connessi online, i più giovani si trovano a dover gestire la propria identità non solo nella vita reale, ma anche online, un po' come una volta succedeva a VIP e a personaggi pubblici: si tratta di una responsabilità che tocca chiunque scelga di avere un profilo su un social network e, di conseguenza, anche la stragrande maggioranza dei più giovani.

Dati, informazioni e azioni non appartengono più (solo) ai legittimi proprietari poiché lasciano una traccia, spesso indelebile, in Rete: è dunque molto importante che gli studenti se ne rendano conto, e che scelgano cosa mettere online con scrupolosità, valutando attentamente le eventuali conseguenze immediate (come si presentano, che immagine di sé danno, che tipo di relazioni strutturano, come vengono percepiti dai loro amici) e future (identità in divenire di bambini e di adolescenti che, in alcuni casi, potrebbero trovarsi a dover fare i conti con “tracce” discutibili del passato, fino ad arrivare al caso estremo in cui anche trovare un lavoro potrebbe essere un problema a causa da ciò che hanno pubblicato o reso noto online anni prima).

Consigli da dare agli studenti

- **INSERITE** PERIODICAMENTE IL VOSTRO NOME SUI PRINCIPALI MOTORI DI RICERCA E GUARDATE I RISULTATI: SE QUALCOSA VI INFASTIDISCE, CERCATE DI ELIMINARLA E, SE NON NE SIETE CAPACI, PARLATENE CON QUALCUNO DI CUI VI FIDATE.
- IN INGLESE SI DEFINISCE **OVERSHARING** E IDENTIFICA L'ABITUDINE DI POSTARE E DI CONDIVIDERE TUTTO CIÒ CHE CAPITA: LIMITARE QUESTO TIPO DI ATTEGGIAMENTO FA CALARE RISCHI E CONSEGUENZE INDESIDERATE.
- **SE NON VOLETE** CHE TUTTI SAPPIANO TUTTO DI VOI, NON POSTATE TUTTO SU INTERNET(NEMMENO NELLE CHAT PRIVATE).
- **CHIUDERE UN ACCOUNT** O ELIMINARE UN PROFILO DA UN SOCIAL NETWORK È UNA PROCEDURA (A VOLTE) COMPLESSA MA FATTIBILE: SE NON NE SIETE CAPACI, PIUTTOSTO CHE RINUNCIARE, CHIEDETE A QUALCUNO DI AIUTARVI.

Ora riflettete….

- Come vorreste essere considerati dalle persone a cui volete bene, soprattutto dai vostri amici?
- Il vostro profilo, le immagini e i post che caricate in Rete vi rappresentano davvero?
- Riflettete su come (e quanto) la vostra comunicazione e immagine potrebbero migliorare…

Il cyberbullismo

Il cyberbullismo (detto anche “bullismo elettronico”) è una forma di prepotenza virtuale attuata attraverso l’uso dei nuovi media, dai cellulari a tutto ciò che abbia una connessione a Internet. Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un’altra percepita come più debole.

Caratteristiche del Cyberbullismo

Le caratteristiche tipiche del bullismo sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno (Olweus, 1996).

Tuttavia, nel cyberbullismo intervengono anche altri elementi, per esempio:

- **L'IMPATTO**: la diffusione tramite Internet è incontrollabile, anche a situazione risolta poiché video e immagini possono restare online.
- **L'ANONIMATO**: chi offende online può nascondersi dietro un nickname o false identità (FAKE).
- **L'ASSENZA DI CONFINI SPAZIALI:** il fenomeno del cyberbullismo può avvenire ovunque e invadere anche gli spazi personali (la vittima può essere raggiunta facilmente tramite supporti connessi a Internet).
- **LA MANCANZA DI LIMITI TEMPORALI**: per i cyberbulli, e di conseguenza per le loro vittime, il giorno e la notte hanno lo stesso valor

Tipologie di Cyberbullismo

Esistono diverse modalità per perpetrare azioni di cyberbullismo.

- **FLAMING**: messaggi online violenti e volgari mirati a suscitare battaglie verbali.
- **HARASSMENT:** spedizione ripetuta di messaggi offensivi mirati a molestare e/o ferire i sentimenti di qualcuno.
- **DENIGRAZIONE**: sparlare di qualcuno (via e-mail, SMS, sui social network, ecc.) per danneggiarne gratuitamente e con cattiveria la reputazione
- **IMPERSONATION:** spacciarsi per un'altra persona per spedire messaggi e/o pubblicare testi reprensibili.
- **EXPOSURE**: rivelare informazioni private e/o imbarazzanti su altre persone.
- **TRICKERY:** ottenere la fiducia di qualcuno con l'inganno per poi condividere con altri le informazioni
- **ESCLUSIONE:** discriminare deliberatamente una persona da un gruppo online per provocarle un sentimento di emarginazione.
- **CYBERSTALKING**: molestie, persecuzioni e denigrazioni ripetute mirate a intimorire altri utenti.

Consigli da dare agli studenti

- **RISPETTATE** GLI AMICI VIRTUALI COME GLI AMICI REALI (ANCHE PERCHÉ, MOLTO SPESSO, SI TRATTA DELLE STESSE PERSONE).
- **SE SIETE VITTIME** DI FENOMENI DI CYBERBULLISMO, RICORDATEVI DI NON CANCELLARE LE PROVE IN VOSTRO POSSESSO.
- **BLOCCATE** CHI VI INFASTIDISCE E, SE POSSIBILE, SEGNALATE IL PROFILO AGLI AMMINISTRATORI DEL SITO O DEL SOCIAL NETWORK.
- **PARLATE DEI VOSTRI PROBLEMI** CON QUALCUNO DI CUI VI FIDATE: TENERSI TUTTO DENTRO NON RISOLVE LE COSE.
- **NON "VENDICATEVI"** REPLICANDO A TONO E METTENDOVI SULLO STESSO PIANO DI CHI VI ATTACCA: FINIRESTE PER PEGGIORARE LA SITUAZIONE.

I videogame

I videogame sono giochi elettronici con dispositivi di comando e controllo (come joystick, mouse, tastiere, telecomandi, ecc.) che permettono al giocatore di rispondere in tempo reale alle situazioni che si ripetono su schermi e/o display.

Alcuni videogiochi moderni sono molto complessi, e contemplano anche la possibilità di giocare con altre persone, perlopiù sconosciuti, attraverso Internet.

La diffusione del gioco online determina nuovi stimoli, ma anche insidie legate alle medesime problematiche di sicurezza che possono insorgere in uno scorretto o poco ragionato uso di Internet (tutela della privacy, contatto con persone potenzialmente pericolose, ecc.).

Gli aspetti “benefici” dei videogiochi

- contribuiscono allo sviluppo di abilità tecniche e strategiche
- migliorano la coordinazione oculo-motoria
- potenziano l’acquisizione del problem solving

Le criticità dei videogiochi

- uso molto spesso eccessivo;
- rischio di violazione della privacy
- richieste di contatti e “amicizie” (videogiochi online)
- esposizione a contenuti non sempre adatti al target

La sessualità in Rete

Internet è ormai parte integrante di ogni aspetto della vita dei teenagers, sfera sessuale inclusa: il bisogno e la crescente curiosità del target rispetto al sesso cercano sempre più spesso risposte in Rete.

Il perché è presto detto: è più semplice e meno imbarazzante chiedere informazioni a un motore di ricerca piuttosto che a un genitore o a un proprio pari “giudicante”.

Purtroppo non è detto che le risposte siano adeguate o veritiere.

La pornografia

Recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti.

Il 14% di ragazzi ambisesso tra i 9 e i 16 anni (il 7% italiani) ha dichiarato di essersi imbattuto più volte in immagini pornografiche nel corso dell'ultimo anno.

Il sexting

Il sexting (parola sincratica che unisce i termini inglesi sex e texting) rappresenta la pratica di inviare o postare messaggi di testo (SMS) e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet.

Rispetto all'adescamento, in cui prevale un comportamento attivo dell'adulto, nel caso del sexting parliamo di un atteggiamento similare ma da parte dei minorenni coinvolti.

Un esempio pratico sono quelle situazioni in cui gli adolescenti producono, condividono e diffondono immagini "sexy" di se stessi o di coetanei, utilizzando le webcam dei PC e/o le fotocamere integrate agli smartphone.

La legge

Per la legislazione, una volta in circolo, si tratta a tutti gli effetti di materiale ritenuto pedopornografico. Con la Legge n. 172 del 1° ottobre 2012, è stata ratificata la Convenzione di Lanzarote riguardante lo sfruttamento e l'abuso sessuale dei minori.

L'articolo 20.2 sui reati relativi alla pornografia infantile asserisce che: L'espressione "pornografia infantile" definisce ogni tipo di materiale che rappresenta visivamente un bambino che si dà a un comportamento sessualmente esplicito, reale o simulato, o qualsiasi rappresentazione degli organi sessuali di un bambino per scopi essenzialmente sessuali.

Produrre questo materiale, e soprattutto diffonderlo, è dunque reato penale.

Non è raro che fare sexting per gli adolescenti equivalga molto spesso a una “dimostrazione d’amore”, oppure a sentirsi strumenti volti all’ottenimento di piccoli vantaggi personali (per esempio ricariche telefoniche).

Consigli da dare agli studenti

- **EVITATE** DI POSTARE IMMAGINI PERSONALI E INTIME, E RICORDATEVI CHE SI PUÒ ESSERE FACILMENTE REGISTRATI O FOTOGRAFATI SE SI USA LA WEBCAM IN MODO INAPPROPRIATO: UN’IMMAGINE IMBARAZZANTE PUÒ ESSERE USATA IN MILLE MODI.
- **LE RELAZIONI SENTIMENTALI** NON GIUSTIFICANO IL SEXTING “SELVAGGIO”: SE LO FATE, SAPPIATE CHE CORRETE IL RISCHIO DI ESSERE “TRADITI” SE E QUANDO LA VOSTRA RELAZIONE FINIRÀ.

L’adescamento: il grooming

Il grooming (dall’inglese to groom che significa prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adescatori utilizzano online.

Grazie alla facilità di accesso alla Rete attraverso dispositivi mobili da parte di giovani e giovanissimi utenti, il rischio di contatti con adescatori (spesso adulti) e malintenzionati è purtroppo molto alto.

L’adescamento avviene attraverso alcuni passaggi “strategici”:

- **CONTATTO**: l’adescatore crea una situazione che attivi la relazione. Banalmente può essere un commento gentile a una foto postata sul profilo.
- **FIDUCIA**: se riceve un riscontro positivo al primo contatto, l’adescatore passa agli step successivi, ossia raccogliere informazioni sulla privacy (“hai il PC in cameretta o in sala?”), tentare di conquistare la fiducia del minore facendo leva su fantomatici interessi comuni (in realtà noti a tutti dai social network), affrontare argomenti di natura intima e, infine, scambiarsi foto non necessariamente di natura sessuale (perlomeno inizialmente).

ESCLUSIVITÀ: ottenuta la fiducia, quando l’adescatore si sente sicuro di sé, inizia la fase dell’esclusività, in cui solitamente avvengono i primi contatti via webcam (spesso a sfondo sessuale) che, successivamente, potrà usare per ricattare la vittima. Dimostrando un interesse di tipo sentimentale e, facendo progressivamente scivolare i contenuti della relazione su argomenti intimi, l’abusante riesce a ottenere il massimo controllo della situazione.

La legge

Spesso il minore ignora che dall'altra parte della chat potrebbe trovarsi un adulto: istintivamente è infatti portato a credere che il suo amico o amica virtuale abbia solo pochi anni più di lui/lei. Altre volte, invece, la differenza di età è nota fin dall'inizio, ma lo schermo facilita le confidenze e la possibilità di proiettare le proprie fantasie e pulsioni.

Il 23 ottobre 2012 nel nostro codice penale il reato di adescamento di minori (art. 609 undecies) è stato esteso a Internet (grooming), per cui le dinamiche che si innescano durante il percorso di adescamento sono ora legalmente perseguibili.

Recenti ricerche hanno indicato che un'alta percentuale delle vittime (ben il 48%6), ha un'età compresa fra i 13 e i 14 anni

Consigli da dare agli studenti

- **NON FIDATEVI CIECAMENTE** DEI SENTIMENTI CHE VI INNESCA UNA PERSONA CONOSCIUTA ONLINE: SE DECIDETE DI LANCIARVI SIATE CONSAPEVOLI CHE LA "COTTA" RISCHIA DI BRUCIARVI
- **SE UNA QUALCHE SITUAZIONE** CREATASI IN RETE VI METTE A DISAGIO O VI IMPONE SCELTE CHE NON VORRESTE FARE, PARLATENE CON PERSONE CHE VI SONO REALMENTE VICINE E DELLE QUALI VI FIDATE
- **SE UN AMICO O UN'AMICA VIRTUALE** VI CHIEDE UN APPUNTAMENTO E VOI VOLETE ANDARCI, EVITATE I POSTI ISOLATI, NON ANDATECI DA SOLI E PARLATENE A QUALCUNO
- **SE VI ACCORGETE** CHE UN VOSTRO AMICO O UN'AMICA SI COMPORTA IN MODO STRANO, CHE SI ISOLA O È PARTICOLARMENTE ATTACCATO/A ALLO SMARTPHONE, CERCATE DI CAPIRE IL PERCHÉ PARLANDOGLI/LE
- **SIATE PRUDENTI IN RETE** COME SIETE PRUDENTI PER LA STRADA: DARESTE IL VOSTRO INDIRIZZO A UNA PERSONA CHE NON CONOSCETE E CHE VI HA FERMATO MENTRE FATE UNA PASSEGGIATA?
- **EVITATE** DI DIVULGARE I VOSTRI DATI PERSONALI (MA ANCHE QUELLI DEI VOSTRI AMICI E/O PARENTI) BADANDO CHE PER DATI PERSONALI NON SI INTENDONO SOLO NOME E INDIRIZZO MA ANCHE I LUOGHI CHE FREQUENTATE ABITUALMENTE E LE VOSTRE FOTO.

Video

- Social network
- https://www.youtube.com/watch?v=BqtnYcfgLbM&ab_channel=Garanteperlaprotezionedeidatipersonali
- App
- https://www.youtube.com/watch?v=MopODAPI5HY&ab_channel=Garanteperlaprotezionedeidatipersonali
- Rischi
- https://www.youtube.com/watch?v=6eF-mwKhrVo&ab_channel=Garanteperlaprotezionedeidatipersonali
- https://www.youtube.com/watch?v=MJxtTIyuqlI&ab_channel=Registroit
-
- Spam
- https://www.youtube.com/watch?v=hDOH09EcFr0&ab_channel=Garanteperlaprotezionedeidatipersonali
- Cookies e Privacy
- https://www.youtube.com/watch?v=Mut-YXSExnw&ab_channel=Garanteperlaprotezionedeidatipersonali