in collaborazione con

Polizia di Stato

CORECOM

Comitato Regionale per le Comunicazioni

# INTERNET @ MINORI | NAVIGAZIONE SICURA

## CONSIGLI E LINK UTILI PER FAMIGLIE, BAMBINI E RAGAZZI

I ragazzi e la rete. Un binomio inscindibile: per chi è nato nell'era di internet e appartiene a pieno titolo alla **"web generation"**. Ma anche per i 'nativi digitali' la rete resta una realtà in chiaroscuro, **un mondo di risorse e opportunità immense e, al tempo stesso, un potenziale fattore di rischio e di pericolo**. E' trascorso un decennio, da quando il CORECOM del Veneto è stato tra i primi in Italia ad interrogarsi sull'accesso dei minori alla rete e su opportunità e rischi della navigazione. E primo tra i Corecom d'Italia ha prodotto un manuale per navigare sicuri nella rete. Ora che la rete è diventata lo strumento privilegiato di comunicazione delle giovani generazioni (e anche quelle meno giovani), il CORECOM del Veneto edita una versione integrata e aggiornata della guida. Uno strumento che vuol essere qualcosa di più di una guida alla navigazione 'sicura' per difendere i ragazzi dai rischi: **"Internet e minori" è una finestra aperta sul valore e le novità della comunicazione digitale, una bussola per educatori e agenzie per mettere a fuoco le potenzialità e i pericoli del web**, per approfondire le norme esistenti e per suggerire a famiglie, scuole ed associazioni percorsi e interventi che orientino a una navigazione sicura, responsabile e consapevole. Ringrazio il CORECOM del Veneto e gli esperti che hanno collaborato a questa iniziativa, per aver approfondito i complessi aspetti della comunicazione multimediale e averne privilegiato la dimensione educativa. **Il web è una straordinaria risorsa per tutti, ma va maneggiata con cura.**

***Clodovaldo Ruffato***
*Presidente del Consiglio Regionale del Veneto*

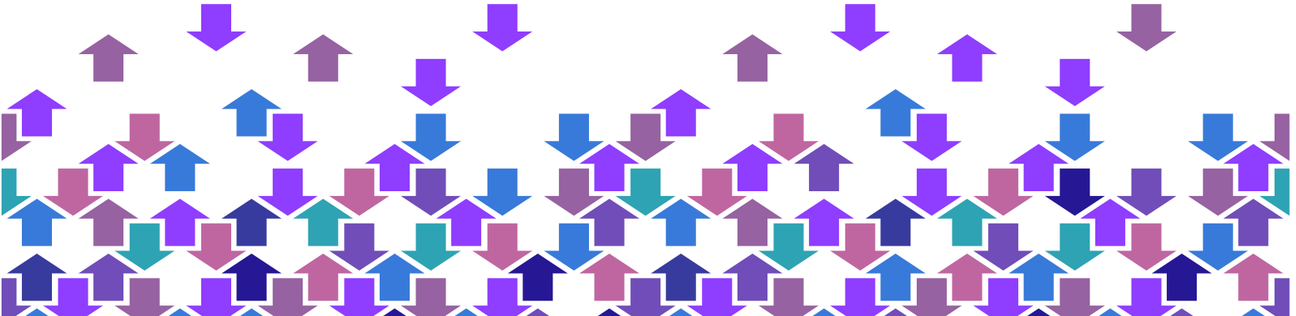
In quanto organo di garanzia, tutela e controllo in ambito comunicativo, il CORECOM del Veneto è particolarmente attento al rapporto tra minori e nuovi media. Negli anni, il rapido susseguirsi di cambiamenti e rivoluzioni nelle tecnologie dell'informazione e della comunicazione rende necessario un **continuo impegno nell'opera di educazione e sensibilizzazione di minori e adulti ad un uso corretto e consapevole di Internet**. Siamo fermamente convinti che la terza edizione, opportunamente ampliata ed aggiornata, dell'opuscolo "***Internet @ minori: navigazione sicura***", rappresenti un utile strumento per mantenersi al passo con un mondo in continuo movimento. L'obiettivo della presente guida è quello di proteggere bambini e adolescenti dalle insidie della rete e di supportare adulti ed educatori nel vigilare e aiutare le giovani generazioni a utilizzare lo strumento informatico con intelligenza e senza rischi. E' indubbio che essere **informati e coscienti** delle proprie azioni rappresenti il punto di partenza imprescindible per compiere scelte consapevoli e consolidare buone pratiche di uso dei nuovi mezzi di comunicazione. Internet presenta potenzialità positive e rischi, e alcune semplici regole possono aiutare i nostri bambini e ragazzi ad evitarne le minacce e coglierne invece le infinite opportunità di informazione, apprendimento e divertimento.

***Alberto Cartia***
*Presidente del CORECOM del Veneto*

È con questa nuova pubblicazione **“Internet @ minori: navigazione sicura”** che il CORECOM del Veneto riconferma il proprio **impegno nell’azione di divulgazione delle buone prassi di navigazione in rete dei e per i minori, riportando all’attenzione di tutti un tema, tanto complesso quanto “sensibile” considerando le sue molteplici implicazioni sociali, educative, etiche**. La guida si propone così, come uno strumento informativo e utile per conoscere e “imparare a riconoscere” rischi e pericoli della navigazione in rete, per scegliere al meglio le tecnologie di protezione e tutela dei minori ma anche - attraverso brevi contributi di esperti - suggerire punti di osservazione e riflessione intorno alle tante criticità ma anche immense opportunità di internet. Come per le passate edizioni, all’interno della guida è stata creata una **parte ludica estraibile dedicata ai più piccoli**, così che fin dai primi passi in rete possano, divertendosi, conoscere stando accanto ai loro genitori le buone regole della navigazione, ma anche i **nonni troveranno uno spazio dedicato con piccole sollecitazioni** utili per avvicinarsi a internet e scoprirne tutti i vantaggi.

A dieci anni dalla prima edizione del nostro progetto Pilota “Internet @ minori: navigazione sicura”, molti paradigmi della comunicazione e dei rapporti media - minori si sono modificati e come è facile immaginare **molti ancora si trasformeranno portandoci in un mondo sempre più “digital oriented”**. Per questa ragione consideriamo importante mantenere vivo il contatto tra generazioni per non “perdersi” nella rete.

***Patrizia Adamoli***
*Direzione Scientifica Progetto Pilota*
*Internet @ minori:navigazione sicura*



# IL VALORE DI INTERNET PER I MINORI

Il rapporto tra ragazzi e Internet è al centro di un dibattito al quale è difficile sottrarsi, in particolar modo se si condividono responsabilità formative in quanto genitori, insegnanti o educatori. Si tratta di un dibattito che, tuttavia, presenta un’ambivalenza che è bene ricordare e sottolineare:

- da una parte, il “panico morale”, che caratterizza **una buona fetta del discorso di senso comune sulla relazione tra minori e media digitali**, prefigura l’aumento delle attività criminali, dei pericoli di natura sessuale, commerciale e ideologica e **fa apparire Internet come una minaccia all’integrità dei minori**. “Paure” che diventano titoli e slogan che agitano il dibattito pubblico e che sono facilmente fatte proprie dagli adulti e dagli stessi ragazzi.
- dall’altra, nonostante questo senso di smarrimento di fronte ai pericoli della rete, siamo più o meno consapevolmente partecipi di una **“febbre tecnologica”** che vede individui e istituzioni avviarsi sempre più velocemente, ma altrettanto spesso disordinatamente, verso quella società in rete (la **“network society”**) che ha proprio in Internet la sua irrinunciabile ragion d’essere. In questo senso, le politiche governative, le strategie delle imprese, la scuola e la famiglia stessa impongono un uso sempre più frequente e diffuso delle nuove tecnologie, per lavorare, studiare o gestire il proprio tempo libero.

Internet è un valore per bambini e ragazzi, uno strumento col quale esplorare e sperimentare territori identitari

Nel mezzo di quest’ambivalenza, tra lo sviluppo incessante delle tecnologie per la comunicazione e le paure sui possibili effetti di questo sviluppo, i bambini e i ragazzi, ma non solo, provano a orientarsi e ad adattarsi al cambiamento che stiamo vivendo, partendo da una consapevolezza: **i media, e Internet in particolare, costituiscono una parte rilevante di quell’ambiente in cui si gioca sia l’avventura del crescere, sia la responsabilità di accompagnare tale avventura.**

Il senso comune sul rapporto tra Internet e minori tende troppo spesso a ignorare le esperienze che, quotidianamente, a casa e a scuola, con amici, insegnanti o genitori, i bambini e i ragazzi fanno della rete, e solo di rado sembra rendersi conto che essi vivono in un mondo molto diverso da quello che ha caratterizzato la gio-

ventù di chi oggi è adulto. Se, tutto sommato, è drammaticamente facile costruire un elenco di quali sono i rischi in cui può incorrere un minore di età nell'uso della rete, meno intuitivo ma altrettanto importante è ricordare quali sono le opportunità che Internet offre a bambini e ragazzi: **dall'informazione all'intrattenimento, dal social networking agli "usergeneratedcontent", dal "fandom" alla possibilità di ampliare le proprie competenze e abilità tecnologiche, dall'acquisire consigli sulla propria salute e vita sessuale all'uso "scolastico" e formativo, al supporto delle attività degli adulti.**

Riconoscere le opportunità educative, partecipative ed espressive derivanti dall'uso della rete significa, in particolare per i genitori, sapersi porre in una condizione di dialogo con ragazzi che, come condizione necessaria per l'autorealizzazione e al fine di crescere intellettualmente, emotivamente e socialmente, "devono", senza eccedere, assumersi dei rischi, sperimentare il "limite", mettersi alla prova per accrescere le proprie capacità. Usare Internet significa poter andare incontro a qualche incognita ma, in cambio, diventare più abili nell'uso stesso della rete, saperne riconoscere i benefici e sfruttare le opportunità.

Come molte ricerche europee insegnano, regolare rigidamente e limitare restrittivamente l'uso della rete al fine di ridurre l'esposizione ai pericoli e la probabilità che i minori si sentano turbati dalle esperienze a rischio, conduce i ragazzi a sviluppare un'alfabetizzazione limitata all'uso dei nuovi media; al contrario, **le forme di mediazione attiva, la promozione degli usi responsabili della rete e la condivisione delle pratiche online si dimostrano non solo più efficaci in termini di riduzione del danno possibile ma, soprattutto, più utili ai fini della promozione di un uso più consapevole e responsabile della rete da parte dei minori**.

Internet è un valore per bambini e ragazzi, uno strumento col quale esplorare e sperimentare territori identitari ed esperienze che saranno meno complicate se, accanto, sapranno di avere degli adulti altrettanto curiosi e disposti a conoscere e imparare. Senza paura.

***Claudio Riva,***
*Sociologo, Università degli Studi di Padova*

# INTERNET MOBILE: I MINORI E LO SMARTPHONE

L'uso di Internet è sempre più radicato nella vita quotidiana di bambini e ragazzi che, attraverso il web, possono ricercare informazioni, creare e consumare contenuti ed esprimere la propria identità in modi sempre più personalizzati.
Eppure, la classica immagine che associa Internet al computer di casa, magari in condivisione con genitori e fratelli, sembra destinata a divenire inadatta a descrivere le esperienze che i minori, ogni giorno, fanno della rete. Soprattutto fra i giovani, infatti, la rapida diffusione di supporti tecnologici mobili e convergenti, quali gli smartphone e i tablet, muta profondamente le condizioni di accesso e utilizzo della rete.
**Le connessioni mobili creano un mondo comunicativo da portare in tasca, sempre a disposizione. In particolare, la possibilità di scaricare le applicazioni (le "apps") più disparate apre le porte ad una costellazione amplissima di attività e scopi da modellare sui propri interessi.**
Se i giochi continuano ad essere i più ricercati dagli utenti, conoscono una crescente diffusione anche le apps che forniscono l'accesso a mappe, news, informazioni meteo, nonché quelle che permettono di collegarsi ai social network e a sistemi di messaggistica istantanea o di telefonate tramite Internet.
Tuttavia, la facilità di connessione permessa dai device mobili non conduce necessariamente allo sfruttamento di tutte le potenzialità connesse alla rete. I minori tendono infatti a restringere le loro attività online, mirando soprattutto all'intrattenimento e ad una comunicazione di base limitata alla propria cerchia di amici.
**È con il progressivo accumularsi di esperienze online, esplorazioni, prove ed errori, che cominciano a prendere confidenza con le opportunità creative e partecipative che possono rendere Internet uno strumento di crescita e acquisizione di competenze più complesse.**
D'altro canto, se la connessione mobile è immediata e fa apparire il mondo a portata di mano, ciò può anche aumentare le occasioni di imbattersi in contenuti violenti o inadatti a bambini e ragazzi, o può portare a rendere pubblici con troppa leggerezza particolari della propria vita. **La possibilità di connettersi alla rete utilizzando uno smartphone o un tablet introduce ulteriori elementi di contatto e intreccio tra quotidianità e internet, facilitando** l'accesso ad un mondo in cui rischi e opportunità convivono in modo spesso caotico e disorientante.

Ne consegue anche la necessità di ripensare al ruolo della mediazione del mondo adulto nei confronti delle esperienze digitali dei minori.
**I device mobili, infatti, indeboliscono le possibilità di controllo della navigazione da parte di genitori ed educatori.** Diventa più difficile accedere alle esperienze online dei ragazzi e decisamente illusorio pensare di poterle dirigere completamente dall'esterno. La navigazione sicura in Internet passerà allora attraverso l'acquisizione di consapevolezza e competenze tali da scongiurare un uso ristretto e quindi anche scarsamente avveduto della rete.
Elemento irrinunciabile diviene l'educazione critica dei minori nei confronti di uno strumento che li accompagna giorno dopo giorno, in un legame indissolubile con il loro vissuto.
Supporto che oggi viene spesso a mancare: per una malcelata diffidenza nei confronti delle nuove tecnologie o per la sottovalutazione dei profondi cambiamenti della condizione attuale dei più giovani, il rischio maggiore è proprio quello di lasciarli soli di fronte alla rete, rinunciando a comprendere le loro volontà di esplorazione, espressione e comunicazione.
**La priorità non è soltanto che i genitori siano consapevoli dei pericoli che Internet può riservare ai propri figli, quanto costruire ponti di collegamento e comunicazione tra genitori, educatori e figli, promuovendo il dialogo e la condivisione delle esperienze di rete, al fine di stimolare l'autonomia dei minori e la loro capacità di reagire positivamente alle situazioni rischiose.**

*Ruggero Cefalo*
*Esperto in Comunicazione dell'Infanzia e dell'Adolescenza*

# BLACK LIST E FILTRI A TUTELA DEI MINORI IN RETE

**Vi sono diversi strumenti che evitano che i minori entrino in contatto in rete con contenuti inadatti o addirittura vietati.** Alcuni operano automaticamente quando ricorrono determinate condizioni previste dalla legge: ne sono esempio le black list istituzionali, caratterizzate da criteri rigorosi, particolarmente adatte ai siti ubicati all'estero. Si tratta di casi limitati, la cui gravità fa sì che la protezione sia estesa a tutti, adulti compresi, come i siti pedopornografici stranieri segnalati ai provider internet italiani dalla Polizia delle comunicazioni e i siti di gioco on line non autorizzati dall'AAMS. Tuttavia, occorre considerare che l'aggiramento della black list non è un'operazione particolarmente difficile e la mera visualizzazione di files o siti vietati che ne consegue non è sottoposta ad alcuna sanzione penale o amministrativa. **Una più ampia gamma di tutele sono disponibili invece come parte di un software o di un apparato, con funzionalità non di rado destinate a proteggere anche ad utenti molto piccoli**; la loro impostazione richiede però l'intervento di un adulto, che poi deve successivamente assicurarsi della loro reale efficacia, provvedendo alle necessarie correzioni. In tutti i casi, l'adozione degli strumenti in questione si aggiunge e non sostituisce l'uso delle protezioni consigliate anche agli adulti, **quali firewall e antivirus aggiornati: spesso non ci si avvale di questi fondamentali mezzi di tutela proprio sugli apparati più ricercati dai bambini, come smartphone e tablet**.

Esaminando con maggiore attenzione i meccanismi di tutela dei minori in rete - e ricordando sempre che le scelte e gli indirizzi dei genitori sono, in fondo, sempre determinanti - in riferimento al soggetto maggiormente coinvolto per renderli operativi, distinguiamo quelli che fanno capo:

**1. ai fornitori di contenuti**
**2. ai fornitori di accesso (ISP)**
**3. all'utente.**

Nel primo caso, viene realizzata una etichettatura dei contenuti (con standard come il PICS - Platform for Internet Content Selection utilizzato dall'ICRA, Internet Content Rating Association), in modo che siano selezionati quelli più consoni all'utente dal programma che guida la navigazione. Il sistema ha però il limite di non essere adottato da molti siti ed, inoltre, non si può evitare che il responsabile dello spazio virtuale possa falsare l'uso delle etichette, poiché non vi sono controlli o sanzioni per l'uso improprio.

I sistemi di protezione a monte sono quelli messi in atto dagli ISP e consistono nel bloccare l'accesso al materiale non adatto o illecito a livello di fornitori d'accesso.

Si tratta di un sistema particolarmente indicato per i siti ubicati all'estero, dove non ci può essere la rimozione di contenuti illeciti per la mancata collaborazione delle autorità interessate o perché una differente legislazione ne permette l'inserimento e la permanenza in rete; tuttavia, è adatto a selezionare una limitata quantità di contenuti. Il blocco è adottato in Italia, come già accennato imposto coattivamente dal legislatore nell'ambito delle misure predisposte dalle istituzioni per impedire il raggiungimento di contenuti pedopornografici ubicati in risorse straniere della rete. Alcuni ISP, però, di loro iniziativa, offrono accessi alla rete dotati di un **filtro parental control**, per permettere cioè ai genitori di controllare - in genere a posteriori - le attività in rete dei figli; se il filtro effettua una vera e propria selezione di contenuti, si realizza una navigazione differenziata, sistema che però, per la sua complessità, non si è mai sviluppato e diffuso in maniera rilevante. **Per quanto riguarda i sistemi protezione a valle, cioè sul compu-**

**ter dell'utente, vi sono numerose soluzioni, spesso già inserite nei software di più frequente utilizzo. I principali sistemi operativi offrono una funzionalità di controllo per i genitori (parental control) che permette di verificare a posteriori i siti visitati, di stabilire un limite giornaliero di durata per la navigazione, di impedirla in alcune fasce orarie, di impostare un filtro che inibisca alcuni siti.** Anche alcuni pacchetti antivirus offrono soluzioni simili o integrano filtri che, oltre a proteggere il sistema e la privacy dell'utente, possono essere impostati per la tutela dei minori attraverso l'analisi sistematica dei contenuti e il confronto con black list disponibili in rete. **Il ruolo dei BROWSER è altrettanto rilevante, non solo perché la cronologia può essere utilizzata dai genitori per il controllo dei siti visitati, ma anche perché sono spesso disponibili estensioni che impediscono di raggiungere determinati siti; ve ne sono poi alcuni creati apposta per bambini, generalmente basati su liste di siti visitabili (white list). Questi ultimi costituiscono il metodo più sicuro di accesso e permettono di selezionare contenuti non solo sicuri, ma anche di qualità (modello walled garden o "biblioteca di casa"). Vi sono poi SOFTWARE pensati appositamente per la tutela dei minori in rete**, basati su filtri che consultano liste di URL da bloccare, ma quelli più interessanti sono quelli destinati all'uso dei tablet e degli smart-phone: ad esempio, limitano il loro uso ad applicazioni appositamente selezionate, impediscono di scaricare nuove applicazioni, fare telefonate e inviare sms o mms.

**La gamma degli strumenti che adottano funzionalità destinate alla tutela dei bambini aumentano con il passare del tempo ed ora anche i router wireless ne posseggono alcune.**

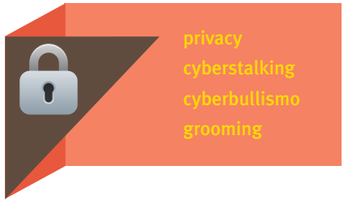
Gli strumenti più sofisticati, cioè quelli che permettono una ampia gamma di attività in rete con un'alta probabilità di evitare contenuti pericolosi od inopportuni, richiedono però una certa abilità da parte degli adulti che li installano o li impostano, anche per evitare che i minori possano aggirarli facilmente; è chiaro che i dispositivi condivisi sono quelli in cui i rischi sono maggiori, perché qualsiasi cautela viene meno se il bambino prende l'apparato quando questo è stato appena utilizzato dal genitore con le impostazioni per adulti.

***Andrea Rossi***
*Primo Dirigente del Compartimento Polizia Postale e delle Comunicazioni per il Lazio*

**I servizi offerti da Internet (posta elettronica, navigazione web, trasferimento file, etc.) costituiscono forse la più grande opportunità di sviluppo che le nuove tecnologie abbiano dato alla nostra società negli ultimi due decenni.** Opportunità di sviluppo e vantaggi di cui beneficiano trasversalmente tutti gli attori della società, dalle istituzioni alle aziende e, naturalmente, i cittadini, sia come destinatari dei servizi posti da istituzione ed aziende attraverso Internet, sia come utilizzatori diretti della Rete.

La sempre maggiore disponibilità di connettività, sia in termini di capacità, che di disponibilità sul territorio, negli ultimi tempi sta amplificando l'impatto di Internet e dei suoi servizi sulle nostre vite, cambiando le abitudini dei cittadini e creando nuovi bisogni. Bisogni connessi alla disponibilità di questi servizi, spesso legati alla **necessità di comunicare con gli altri e di mostrare ad essi, nell'esatto momento in cui si vive una sensazione, cosa si sta provando postando, ad esempio, una foto o un filmato sul proprio social network preferito.**

Ma le opportunità date dal mondo di Internet portano con sé, come rovescio della medaglia una serie di svantaggi, rischi, pericoli, che possono essere contrastati con alcune soluzioni tecnologiche e, soprattutto,




con comportamenti adeguati.

Cerchiamo perciò di identificare alcune categorie di pericoli cogliendone le rispettive peculiarità.

### PERICOLI DOVUTI ALLA TECNOLOGIA

Possiamo definire tali tutti quelli dovuti alla possibile intromissione all'interno del nostro dispositivo (PC, tablet, smartphone, notebook, etc.) di programmi malevoli (**virus, worm, trojan, keylogger, maleware, etc.**) **che, contro la nostra volontà, ci sottraggano dati (la nostra password per la posta elettronica o per il nostro social network o le informazioni per accedere al nostro conto on line) e li diano ad altri per un possibile utilizzo illecito.**

Questo genere di pericoli è spesso sottovalutato dagli utenti, perché si ha la convinzione errata di non essere in possesso di dati interessanti per gli altri e, pertanto, di non essere il bersaglio di attacchi mirati.

Tutto questo spesso si rileva falso. I nostri dati identificativi per l'accesso a servizi sulla rete hanno un valore per chi ha interesse a sfruttarli a proprio vantaggio. Inoltre, molti dei programmi malevoli atti a sottrarre i nostri dati o, comunque, a permettere ad estranei di avere il controllo del nostro PC contro la nostra volontà, possono essere inoculati anche con la semplice navigazione su pagine web ospitate su server che siano stati a loro volta illecitamente compromessi a tale scopo.

## PERICOLI DOVUTI AI COMPORTAMENTI DELLE PERSONE

***Con chi sto chattando? Con chi sto realmente condividendo informazioni? Chi c'è al di là dello schermo?*** Semplici domande che dovremmo sempre farci quando utilizziamo servizi di comunicazione. Quando comunichiamo attraverso tecnologie siamo più predisposti a scambiare informazioni, anche con sconosciuti e questo può essere pericoloso, sia per i minori, ma anche per gli adulti.

Gli adulti possono rilasciare informazioni, anche inconsapevolmente, sui propri gusti, orientamenti politici, religiosi, sessuali. Possono cedere proprie immagini che, se decontestualizzate, potrebbero dare adito ad un'interpretazione diversa dal contesto in cui sono state prese, con risvolti dannosi per il soggetto rappresentato. Possono essere spinti a cedere informazioni sui propri account di posta elettronica o social network.

Tutte queste informazioni, acquisite e trattate in palese violazione della normativa sulla privacy, possono essere utilizzate, in maniera spesso illecita, per sceglierci, ad esempio, come target di aggressive campagne pubblicitarie su prodotti che potrebbero riscuotere il nostro interesse. In alcuni casi, però, tali informazioni diventano preziose per molestatori che utilizzano la rete per perpetrare una vera e propria serie di comportamenti persecutori attraverso quello che oramai viene definito **cyber stalking**.

**Ma è soprattutto quella dei minori la fascia più debole rispetto questo tipo di pericoli. In loro la naturale predisposizione alla comunicazione, unita all'essere nativi digitali,** (perché cresciuti nella società dell'informazione, considerando le tecnologie come un elemento naturale e che non provano alcun disagio nell'interagire con esse) **costituisce un pericoloso cocktail che li espone ancora più degli adulti ai danni di comportamenti persecutori, alcuni dei quali peculiari di questa fascia della popolazione.**Se l'adulto è vittima di cyber stalking, i ragazzi possono essere vittima di comportamenti persecutori che, seppur tipici della loro età, quando vengono associati alle nuove tecnologie, come nel caso del **cyberbullismo**, costituiscono vere e proprie condotte di reato, con gravi conseguenze assolutamente non valutate dagli autori di quella che voleva essere, magari, soltanto la solita ragazzata. Ma **quando la ragazzata viene postata su Internet assume una portata completamente diversa. Perché la documentazione dell'episodio di umiliazione diviene un'informazione destinata a tutti, la cui rimozione definitiva, è soltanto illusoria, ed il danno diventa enormemente più grave, trasformando un pessimo scherzo tra compagni di scuola in un reato.**

Ma il pericolo più grave che corrono i nostri figli nell'utilizzo indiscriminato di Internet è quello di cadere vittima di adescamenti di criminali che cercano di indurre minori ad avere con loro relazioni di natura sessuale.

A tal proposito, l'Italia con la ratifica della "Convenzione di Lanzarote", ha introdotto nel codice penale, dall'ottobre del 2012, il cosiddetto **reato di grooming**, previsto dall'art. 609-undicies, che prevede la condanna fino a 3 anni, per il solo fatto di adescare minorenni.

Naturalmente, ove all'adescamento segua anche un abuso sessuale o altri reati, il criminale verrà condannato anche per gli altri illeciti.

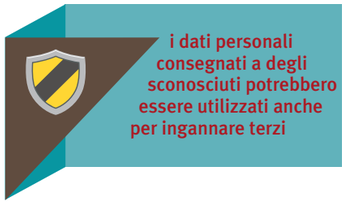
***Tommaso Palumbo***
*Primo Dirigente del Compartimento Polizia Postale e delle Comunicazioni per il Veneto*

# TRUFFE ONLINE

Il diffondersi della rete e la facilità che offre di nascondersi dietro false generalità hanno creato le condizioni per perfezionare truffe già conosciute e per escogitare raggiri del tutto nuovi, che hanno potuto sfruttare l'effetto sorpresa nei confronti delle vittime, tra le quali i minori sono una percentuale considerevole ed in crescita mano a mano che tra essi si diffondono gli smartphone.

Spesso le insidie sono anticipate da attività apparentemente innocue, non direttamente legate ad una spendita di denaro, come la partecipazione a concorsi on line o la compilazione di moduli: **i dati personali consegnati a degli sconosciuti potrebbero essere utilizzati anche per ingannare terzi e rendere credibile un contesto fraudolento.** Massima attenzione deve essere data all'**installazione di applicazioni gratuite o accompagnate da promesse di regali ricevibili solo sottoscrivendo clausole contrattuali che impegnano a versamenti periodici**, spesso difficilmente quantificabili.

Per quanto riguarda i giochi on line, è bene ricordare che è vietato consentire la partecipazione ai giochi pubblici con vincita in denaro ai minori di anni diciotto. Fatta questa premessa, però, è bene ricordare che nonostante le restrizioni introdotte recentemente in Italia, la pubblicità di giochi con vincita in denaro on line sui siti stranieri è massiccia ed invadente ed è perciò indispensabile dare in merito delle precise indicazioni ai minori per evitare spiacevoli sorprese.




La normale attività ludica in rete è comunque sempre più diffusa tra i ragazzi; può anche avere riflessi positivi se non se ne abusa e se i contenuti sono appropriati all'età, ma, ancora una volta, vanno tenute presenti le precauzioni generali per i contatti con gli estranei che ne possono nascere (molte piattaforme permettono lo scambio di messaggi tra i giocatori) e quelle che riguardano le tecniche di marketing sempre più raffinate indirizzate ai minori: **è frequente, per esempio, che un gioco sia presentato come gratuito, ma poi, per poter ottenere poteri o punteggi che lo rendono divertente, si debba acquistarli di volta in volta, a carico dei genitori.**

Talvolta i videogiochi ed i giochi on line non sono altro che pubblicità mascherate, in cui il marchio commerciale interessato diventa protagonista agli occhi del minore per un tempo considerevole.

Se si tratta di prodotti alimentari, come frequentemente accade anche per orientare gli acquisti degli adulti, bisogna evitare che questa sovraesposizione generi la tendenza ad esagerare con il junk food (cibo spazzatura) a scapito di alimenti spesso trascurati quali frutta o verdura fresca.

***Andrea Rossi***
*Primo Dirigente del Compartimento Polizia Postale e delle Comunicazioni per il Lazio*

PER I RAGAZZI E...NON SOLO

# BUONE REGOLE DA RICORDARE SEMPRE PER LA TUA SICUREZZA

1

La Rete è un luogo "virtuale" tutti possono abitarla e per diversi scopi, non tutti però sono leciti quindi, verifica sempre le informazioni che trovi e l'identità dell'autore o di chi ti contatta

2

Non fornire MAI i tuoi dati personali, l'indirizzo di casa o della scuola che frequenti, il tuo numero di cellulare se non per motivi assolutamente indispensabili , ricorda che i dati personali hanno un grande valore "commerciale"

3

Non fornire MAI i dati della carta di credito dei tuoi genitori, se devi fare acquisti in rete utilizza una carta prepagata e solo con la loro autorizzazione e aiuto durante l'operazione

4

Se usi le chat, partecipi a forum, o a giochi di ruolo usa nickname e non dare informazioni personali

5

Ricordati che anche in rete è bene essere educati e ci sono delle regole di *netiquette* che vanno rispettate

6

Prima di postare una tua foto o un filmato pensaci bene... una volta in Rete foto e filmati non sono più controllabili e possono essere utilizzati anche da altre persone e per motivi che possono anche danneggiare te, i tuoi amici o la tua famiglia. Per lo stesso motivo fai attenzione alle tue foto che non siano postate dai tuoi amici senza la tua autorizzazione

7

Se utilizzi i social network fai sempre attenzione alle impostazioni e decidi tu chi far "entrare" nel tuo spazio privato

8

Quando chatti o comunichi via mail fai attenzione alle domande "troppo" personali o alla richiesta di fotografie o filmati.
Se qualcuno ti invia delle sue foto ricorda che potrebbero non corrispondere alla persona con cui sei in contatto

**9**

Se qualcuno con cui chatti o hai contatti via mail ti chiede un appuntamento ricorda sempre che nonostante le conversazioni avute, è e resta uno sconosciuto. Prima di accettare un incontro, avverti i tuoi genitori , organizza le cose in modo da non avere sorprese sgradevoli o trovarti in situazioni pericolose, porta con te un paio di amici o amiche e non solo al primo appuntamento

**10**

Quando ricevi via sms o incontri in rete offerte di ricariche gratis, premi fantastici e vincite allettanti ricorda che spesso sono proprie e vere truffe per farti sottoscrivere costosi abbonamenti o carpire i tuoi dati o la tua fiducia e poi farti fare cose che non sono adatte alla tua età

**11**

Prima di scaricare programmi verificane la provenienza e affidabilità, eviterai virus o spyware

**12**

Anche quando non ti viene richiesto cambia la tua Passaword, e abituati ad averne più di una

**13**

Se qualcosa ti disturba, se diventi oggetto di attenzioni fastidiose, cerca aiuto in un adulto, avvisa subito i tuoi genitori

**14**

Evita ogni comportamento che possa disturbare o infastidire gli altri perchè potresti commettere reati puniti dalla legge

**15**

Ricorda che tutti possono scrivere in rete quindi controlla sempre la fonte delle informazioni che trovi e verifica che sia affidabile

**16**

Ricorda: i tuoi dati sono preziosi, valgono molto per chi li ottiene, quindi prima di fare click, prima di dire OK, pensaci bene!

# BUONE REGOLE PER I GENITORI

Informatevi e imparate almeno l'abc del navigare in rete e tenetevi aggiornati

Spiegate ai vostri figli che cos'è internet , come si usa il computer e il cellulare, fatelo voi prima che imparino da altri o peggio, da soli. Insegnate la netiquette, anche in rete ci vuole educazione e rispetto

Spiegate a cosa può servire navigare, quante cose belle e utili si possono scoprire , e quali sono le regole da seguire soprattutto quando cominciano ad utilizzare chat , forum e social network

Decidete in base all'età dei figli per cosa e per quanto tempo può essere utilizzato il pc di casa

Posizionate il pc in una zona di casa dove c'è passaggio in modo da poter controllare con discrezione

Scegliete delle buone protezioni antivirus e sempre in base all'età il software più adatto per la navigazione protetta che dovrà essere aggiornato e controllato periodicamente

Spiegate ai vostri figli il senso della navigazione sicura e man mano che crescono allargate la disponibilità dei siti e delle operazioni cui possono accedere condividendo le scelte anche in base alle loro preferenze

Impostate la cronologia in modo da avere traccia dei siti che vengono visitati

Quando vi chiederanno di iscriversi ad un social network controllate le impostazioni in modo che l'accesso sia riservato e protetto

Leggete insieme le prime mail e verificate gli allegati, spiegate che anche negli allegati possono viaggiare i virus, non accettare mail dagli sconosciuti e soprattutto non rispondere

Quando i vostri figli cominciano ad utilizzare internet, fate spesso domande su quello che hanno scoperto, cercate una relazione costruttiva e rendetevi disponibili così che si abituino a relazionarsi e soprattutto a chiedere aiuto in caso di necessità

In base all'età spiegare che l'identità delle persone in rete può essere fittizia e non corrispondere alla realtà e che è bene diffidare di chi pone domande - anche in forma giocosa - particolarmente personali e legate alla sfera sessuale. In questi casi e senza vergognarsene è importante informare subito i genitori

Se non potete dedicare un pc all'uso esclusivo dei figli - scelta consigliata - fate regolarmente il backup dei vostri dati

## IN PARTICOLARE DOVETE DIRE AI VOSTRI FIGLI, SEMPRE IN BASE ALL'ETÀ, CHE:

La Rete è un utile strumento per imparare, per studiare, per cercare informazioni e per giocare ed è una vera risorsa se ben utilizzata ma...

La Rete è "aperta" e attraverso la rete si creano relazioni e dato che non si può sapere chi c'è" dall'altra parte" è necessario essere prudenti e attenti a ciò che si fa,

Mai dare i propri dati personali, indirizzo di casa o di scuola né tantomeno il numero di telefono o della carta di credito dei genitori.

Le fotografie, i filmati sono strettamente personali prima di inviarli o postarli è necessario pensarci bene

Mai accettare inviti senza comunicarlo ai genitori,

Non credere alle offerte di premi e regali perché nascondono truffe e raggiri,

Molti contenuti -musiche, fotografie, filmati - sono soggetti a diritto e "scaricarli" è una violazione delle leggi della proprietà autoriale e intellettuale.

## PER LO SMARTPHONE:

**Valutare l'età e la tipologia di apparecchio da dare in uso ai figli**

**Ricordarsi che gli smartphone hanno tutte le funzioni di un pc, possono fare foto e filmati, "caricare e scaricare" contenuti ma a differenza del pc che può essere "tenuto d'occhio", il cellulare viene utilizzato fuori casa ...**

**Scegliere SIM ricaricabili per poter monitorare la quantità di traffico, dare ai figli il PIN ma non il PUK che permette l'accesso al cellulare anche se il PIN viene modificato,**

**Spiegare che non bisogna richiamare numeri sconosciuti, non bisogna richiamare numeri da cui provengono chiamate mute o squilli perché sono metodi spesso usati da malintenzionati per identificare e adescare i minori**

**Non accettare promesse e offerte di ricariche via sms o mms in cambio di foto, filmati o qualsiasi altra richiesta**

**Non fare fotografie o filmati - e non lasciarseli fare - e postarli "per scherzo" perché una volta immesse in rete la diffusione dei materiali non è più controllabile**

# NET EDUCAZIONE, PER UNA VERA CITTADINANZA DIGITALE

**Bambini e ragazzi, come ben sappiamo, nascono con una predisposizione naturale alla comunicazione e ai nuovi media.**
Per loro, tutto ciò che la tecnologia per la comunicazione crea e offre, è in brevissimo tempo strumento familiare e materia spendibile in attività del quotidiano, utili per mantenere e ampliare rapporti e relazioni, manifestare sé stessi, conoscere e condividere. Tuttavia l'utilizzo che i ragazzi fanno della Rete, della tecnologia e del loro talento digitale è spesso limitato in azioni frutto di autoapprendimento e di scambio tra pari, che però, come è facile intuire, ne limitano gli orizzonti e le reali potenzialità.
In questo contesto, la figura dell'adulto risulta spesso defilata se non addirittura assente, come se **l'educazione digitale non facesse parte a tutti gli effetti del percorso di relazione e di crescita genitori-figli e potesse essere in qualche modo limitata ai divieti**, delegata ad altri o peggio, elusa.
In realtà, l'educazione digitale - e un impegno forte a suo favore - può offrire grandi spazi di opportunità per tutte le generazioni - dai più piccoli ai nonni - proprio perchè adattabile, fluida e compatibile con le diverse esigenze e bisogni.
**Una buona educazione digitale inoltre è imprescindibile per crescere come veri cittadini digitali e poter utilizzare con sapiente proattività tutto ciò che la rete offre e c'è da contarci, continuerà ad offrire.**

*Patrizia Adamoli*
Esperta in Media Education e
Tecnologie Comunicative

### COSA VUOL DIRE NET EDUCAZIONE?

**Educare** ed essere educati all'uso degli strumenti digitali e della Rete, conoscerne le potenzialità, sviluppare capacità critiche e di scelta.

### NET EDUCAZIONE IN QUATTRO PUNTI:

**Conoscere** gli strumenti e i linguaggi utili per navigare,

**Conoscere** le regole e avere rispetto della Rete e degli altri naviganti,

**Sviluppare** competenze d'uso e abilità utili alle proprie esigenze,

**Conoscere** rischi e pericoli così da evitarli o sapere come agire in caso di necessità.

## SE CERCHI@TROVI

**La rete è come una grande enorme immensa incalcolabile biblioteca con contenuti sempre disponibili, in aggiornamento costante e a misura personale.** Basta saper cercare e scegliere tra video, musica, e-book per studiare, approfondire, imparare e conoscere. In rete la formazione è davvero continua.

La rete offre opportunità per tutti, sostegno e strumenti dedicati, programmi specifici anche nei casi di svantaggio fisico o difficoltà dell'apprendimento.

**PER I NONNI:**

Qualsiasi sia la vostra età non è mai troppo tardi!
E con internet si può:

***Leggere il giornale***

***Fare la spesa***

***Scrivere ai figli, ai nipoti, agli amici lontani***

***Scaricare libri e leggerli***

***Comunicare con la pubblica amministrazione***

***Prenotare visite o comunicare con il medico***

***Sapere che tempo farà***

***Tenersi aggiornati, approfondire o coltivare hobbies***

***Giocare a scacchi***

***Fare il solitario e, non sentirsi mai soli!***

Usare internet non è difficile, tutti possono imparare e aiuta a rimanere in forma. Chiedi ai tuoi familiari, magari ai nipotini, naviga con loro e fatti spiegare oppure informati presso il tuo Comune o Associazioni della tua zona, troverai chi può insegnarti come si fa a navigare.



# I "RISCHI PENALI" NELL'USO DEI SOCIAL NETWORK

## I "RISCHI PENALI" CORRELATI ALL'USO DEI SOCIAL NETWORK DA PARTE DI MINORI QUALI "VITTIME" O "AUTORI" DI REATI

Uno degli effetti più incisivi dell'informatizzazione nella vita quotidiana dei giovani in genere e dei minori in specie è costituito dall'espandersi dell'uso dei Social Network. Facebook, Twitter, LinkedIn, Google+, ecc., solo per citare i più famosi, contengono sempre più "profili" di giovani e di giovanissimi, inseriti anche in violazione del limite d'età anagrafica teoricamente previsto (comunemente 16 anni), eludibile facilmente non essendovi un controllo effettivo sull'identità di chi vi si iscrive e partecipa.

**Le "reti di comunicazione sociale" sono perciò accessibili a tutti, anche sotto false identità o comunque con nomi, soprannomi o singole caratteristiche di fantasia, oltre che da ogni luogo ed in ogni momento**, visto che lo consentono gli apparecchi portatili (tablet e smartphone in particolare), di cui anche i più giovani, perfino minori in età prescolare, sempre più frequentemente dispongono.

Certamente la partecipazione a queste reti - come più in generale l'uso di Internet - arricchisce di stimoli la loro crescita e ne facilità la socializzazione, offrendo possibilità di comunicazione ed accesso immediato ad un'enorme quantità e varietà di informazioni e contenuti, sempre aggiornati, in tempi ed in misura neppure immaginabili qualche anno orsono.

**Ma la penetrazione capillare dei Social Network nella vita quotidiana dei giovani porta con sé anche molteplici rischi, come dimostrano tragicamente alcuni fatti di cronaca ascrivibili al c.d. cyberbullismo**, che non sono sempre tempestivamente avvertiti né conosciuti in modo adeguato, stante la diversità di regole di comportamento e di modalità di relazione nel cyberspace rispetto a quelle proprie del mondo "reale". Per cui vi è maggiore difficoltà a comprendere e valutare adeguatamente possibili situazioni pericolose ed a compiere scelte conseguenti per prevenire possibili effetti dannosi.

**In questa sede si illustreranno brevemente i "rischi penali", vale a dire i rischi di subire, da un lato, e di commettere, dall'altro, reati tramite l'utilizzo dei Social Network.** Gli utenti (in particolare anche i minori, che come noto possono essere "imputabili" con il compimento di quattordici anni: art. 98 codice penale) possono di volta in volta essere "autori" oppure "vitti-

me” dei **reati realizzati in rete o tramite la rete, la cui esistenza e gravità è difficile da percepire proprio per la menzionata natura “immateriale” - o come si usa dire “virtuale”** - delle comunicazioni e delle condotte in esame, dato che l’idea stessa di “reato” è tradizionalmente (ed inconsciamente sempre) correlata alla “materialità” di un’offesa fisicamente percepibile: qual è ad esempio la sottrazione di “cose” in un furto o la violenza fisica o verbale in un’estorsione od ancora, nelle violazioni dei diritti d’autore, la riproduzione e cessione vietata di supporti materiali contenenti musica o film (quali cd-rom ovvero audio o video-cassette). Requisiti che ovviamente non esistono nel cyberspace.

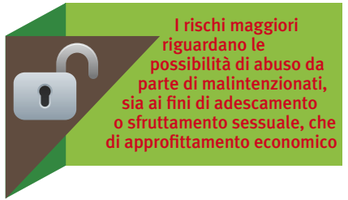
## I REATI CONTRO LA PRIVACY

I reati di cui i minori ed i giovani possono essere autori o vittime quali utenti dei Social Network riguardano in prima battuta la privacy o riservatezza dei dati personali.

Proprio la torrenziale creazione di “profili” personali, l’utilizzo di tag, il moltiplicarsi a catena di “inviti” ad accettare amicizie e a scambiare messaggi, informazioni, testi, video, immagini, con soggetti anche sconosciuti o sotto falso nome, il continuo aggiornamento con ogni genere di notizie relative ad attività svolte ed a luoghi frequentati, disponibili a chiunque partecipi al Social Network, rappresentano un modo penetrante e diffuso di mettere a disposizione e di scambiare dati anche strettamente personali, che vanno da quelli identificativi dell’individuo (data di nascita, sesso, indirizzo, numeri telefonici, immagini, ecc.) a notizie esplicite od indirettamente ricavabili sulle attività, preferenze, orientamenti di vita (dallo svago allo sport, dalla musica ai film, dalle scelte e tendenze in campo sessuale a quelle culturali, religiose, ideologiche o politiche, ecc.).

È un’enorme flusso di dati messi in circolazione ad opera dell’interessato stesso (colui cui i dati si riferiscono), nonché da “amici” e terzi, comprese persone con cui vi sia solo un occasionale o indiretto contatto (si pensi ad un tag identificativo sulla propria immagine prodotta e caricata da altri), che sfugge alle concrete possibilità di controllo, pronta rettifica o cancellazione, aggiornamento, ecc. da parte dell’interessato, se non altro

perchè la sua percezione può non esserci del tutto o avvenire molto tardivamente. Ed anche dopo l’eventuale modifica o cancellazione (compresa quella del proprio profilo) i dati immessi restano in grado di circolare ulteriormente in altri account, siti, reti o settori di rete in cui siano già stati scaricati o comunque acquisiti o riprodotti. **I rischi maggiori riguardano le possibilità di abuso da parte di malintenzionati, sia ai fini di adescamento o sfruttamento sessuale, che di approfittamento economico** (ad esempio nel caso di dati di rilievo economico, quali quelli concernenti condizioni di vita e familiari, numeri di conto corrente, pin, password, codici di accesso di carte di credito o prepagate o conti on-line, ecc.). **La più elevata pericolosità per i più giovani dipende dal fatto che non considerano la successiva circolazione “incontrollabile” od utilizzazione strumentale da parte di terzi, dopo l’iniziale**




**condotta volontaria, dei dati immessi.** Per cui possono essere di volta in volta vittime ed autori (o quantomeno “complici” e partecipi, o comunque “strumento”) di tali violazioni, concorrendo a loro volta alla immissione, circolazione, riproduzione, memorizzazione di questa enorme massa di informazioni personali, anche quando non vi sia o non vi sia più il consenso esplicito ed informato dell’interessato, quale sarebbe richiesto dal Codice della privacy (decreto legislativo 30 giugno 2003, n. 169 e successive modifiche) come condizione perché il “trattamento” (che va dalla raccolta alla memorizzazione alla circolazione ecc.) dei dati sia lecito, configurandosi in mancanza il delitto di cui all’art. 167 dello stesso codice.

**La privacy propria ed altrui è facilmente e spesso superficialmente “sacrificata” all’esigenza sentita come ben più forte ed immediata di partecipare appieno alla comunità degli “amici” della rete**, e di mettere anzi in evidenza le proprie caratteristiche, qualità, preferenze, attività, ecc., nonché di scambiare reciprocamente sempre nuovi materiali e informazioni di ogni genere. Comportamenti i cui effetti negativi si possono percepire solo a distanza di tempo od in situazioni particolari.

## I REATI DI PEDOPORNOGRAFIA ED ABUSO SESSUALE: IN PARTICOLARE IL C.D. ADESCAMENTO IN RETE (GROOMING)

**I più gravi reati cui sono esposti i minori sono quelli di abuso e sfruttamento sessuale.** Realizzare, procurare, far circolare, detenere immagini pedopornografiche (cosiddetta

"pornografia minorile") sono delitti punibili ai sensi degli art. 600-ter e 600-quater codice penale, anche nel caso di immagini meramente "virtuali", create cioè o manipolate realisticamente - in tutto od in parte - al computer con tecniche elettroniche (art. 600-quater.1 codice penale).
Ed è punibile non solo far entrare questo "materiale" in un circuito commerciale lucroso o comunque fornirlo od offrirlo ad un mercato in cui la domanda è in continua crescita, ma anche produrlo con il consenso (giuridicamente invalido) di altri minori che si lascino ritrarre in attività sessuali, lasciandolo poi circolare o cedendolo a terzi (come è avvenuto nel caso di immagini di una ragazza ritratta dal suo ex ragazzo, esposte poi sul profilo in rete a disposizione degli "amici" una volta terminata la relazione o addirittura divulgate ad un pubblico più vasto).
Oltre alle molte e severe incriminazioni introdotte al riguardo nel codice penale in attuazione di convenzioni internazionali e direttive europee (legge n. 269/1998, legge n. 38/2006, da ultimo legge n. 172/2012 di attuazione della Convenzione di Lanzarote), si è creato anche un notevole apparato di forze investigative, mezzi di indagine e strumenti di cooperazione internazionale (in Italia affidati soprattutto alla Polizia Postale), che non di rado si avvalgono proprio dei Social Network per acquisire indizi e prove dei reati, entrandovi con account e profili "di copertura".
**Di grande rilievo è in questa materia il nuovo delitto di "adescamento di minori" in rete (cosiddetto grooming)** introdotto nel 2012 quale art. 609-undecies codice penale, che punisce condotte e atti sostanzialmente "preparatori" finalizzati alla realizzazione dei più gravi reati a danno di minori, che non abbiano compiuto anni 16, quali la produzione e circolazione di materiale pornografico, la prostituzione minorile, la tratta e il traffico di minori, il turismo sessuale, la corruzione di minori, i reati di abuso sessuale in genere.
L'adescamento si realizza con "qualsiasi atto volto a capire la fiducia" del minore attraverso artifici, lusinghe o inganni posti in essere anche mediante l'utilizzo della rete internet o altri mezzi o reti di comunicazione.

## I REATI CONTRO LA REPUTAZIONE E LA "LIBERTÀ MORALE": IL C.D. CYBERBULLISMO

Molti reati in cui la condotta punibile si realizza mediante una "manifestazione o comunicazione del pensiero" possono essere commessi e subiti in rete: quali ingiurie e diffamazioni (artt. 594 e 595 codice penale), minacce (art. 612), molestie (art. 660), atti persecutori (art. 612-bis: c.d. stalking), estorsioni (art. 629), ecc., che offendono rispettivamente l'onore e la reputazione, ovvero la c.d. "libertà morale" della vittima, condizionandone la volontà e la capacità di scelte autonome.

I più gravi reati cui sono esposti i minori sono quelli di abuso e sfruttamento sessuale.

**Inviare e far circolare informazioni ed immagini – vere e false – che mettono in cattiva luce la vittima, specie nella cerchia di "amici" cui appartiene, pressarla psicologicamente con richieste, minacce, denigrazioni, esclusioni da attività o gruppi, ecc. sono comportamenti che ormai si realizzano facilmente e con relativa frequenza in rete**, fra minori o comunque a danno di minori, più fragili e sensibili a tali aggressioni, talvolta coperte sotto falsi nomi o profili identitari. Il fenomeno, chiamato **"cyberbullismo", può assumere dimensioni ed intensità preoccupanti, portando al crollo psicologico della vittima, che può essere indotta a gesti autolesionistici e perfino al suicidio, come la cronaca dimostra.**

le violazioni dei diritti d'autore, vengono con grande frequenza commesse in rete proprio attraverso i Social Network

La notevole difficoltà di accertamento, repressione e prevenzione di tali reati dipende anche dal fatto che le stesse vittime tendono a non denunciare i fatti subiti, per timore o vergogna, o quanto meno a segnalarli a chi di dovere, con la creazione di una sorta di omertà verso l'autorità pubblica che finisce per garantire impunità agli autori.

## LE VIOLAZIONI DEI DIRITTI D'AUTORE

**Infine si devono menzionare le violazioni dei diritti d'autore, che vengono con grande frequenza commesse in rete proprio attraverso i Social Network,** oltre che attraverso chat, comunicazioni peer-to-peer, creazione ed utilizzo di siti per scambi di opere protette, in specie musica, film, giochi, oltre che artistiche e letterarie in genere.
**I Social Network ne facilitano la ricerca e lo scambio, anche mediante informazioni sui siti e modi per procurarsi le opere desiderate**, in conformità alle preferenze, conoscenze, disponibilità dei partecipi. Mentre specie da parte dei più giovani non è percepito il disvalore giuridico e tantomeno la possibile rilevanza penale di tali comportamenti, estremamente diffusi e condivisi, in cui tutto quanto è tecnicamente realizzabile viene percepito come possibile.
Si tratta di un ambito d'intervento estremamente delicato, perché la stessa legislazione (in particolare

quella italiana) appare farraginosa e talora contraddittoria, con punte di severità e di estesa incriminazione, anche per l'utilizzo meramente personale di singole opere protette (cfr. artt. 171 segg. Legge 22 aprile 1941, n. 633 e succ. modifiche), ma senza che poi vi sia un'effettiva corrispondente persecuzione e capacità (e fors'anche volontà) di accertamento e sanzione. Probabilmente in molti casi sarebbero più opportuni strumenti di tutela civile e amministrativa, o di prevenzione anche mediante un'opera di sensibilizzazione sul rispetto dei diritti altrui e sulla preferenza, ove possibile, di condotte conformi alle regole, pur a costo di un qualche sacrificio economico.

## CONCLUSIONI: PREVENZIONE E RESPONSABILIZZAZIONE SULLA COMMISSIONE DI REATI NEI SOCIAL NETWORK

Certamente le sanzioni penali appaiono insufficienti per fronteggiare con efficacia tutti i fatti illeciti che vengono commessi e subiti nei **Social Network**. Molto importanti appaiono, per prevenirli, i codici di autoregolamentazione dei gestori delle reti e gli interventi di filtro e controllo del traffico in rete, che possono essere realizzati dagli **Internet Service Provider**, oltre che dalle autorità competenti. Parimenti rilevanti sono gli interventi di sensibilizzazione degli educatori nonché di monitoraggio, operati da associazioni, centri ed enti pubblici e privati, spesso attivi anche nella segnalazione dei casi più gravi in cui possano essere coinvolti i minori (in specie i casi di prostituzione minorile, di abuso sessuale, di pedopornografia). In questo contesto, appare opportuna l'informazione e sensibilizzazione dei minori stessi sul rilievo penale che possono avere le condotte esaminate, di cui possono essere sia vittime che autori partecipando ai **Social Network**, entrati ormai così pervasivamente nella loro vita quotidiana. Essi possono così apprezzarne più consapevolmente e responsabilmente i rischi e regolare di conseguenza i propri comportamenti nelle relazioni con gli altri. Benché realizzate nel mondo "virtuale" del **cyberspace**, si tratta infatti di condotte che si traducono in **relazioni interpersonali** e sociali "reali", da cui possono scaturire effetti gravi e talora anche irreparabili, per sé e per gli altri.

***Lorenzo Picotti***
*Professore ordinario di diritto penale e diritto penale dell'informatica, Dipartimento di Scienze Giuridiche - Università degli Studi di Verona*

# AFFETTIVITÀ E SESSUALITÀ ATTRAVERSO LA RETE

Lontano dal ritratto allarmistico che i media spesso propongono, così come dai facili entusiasmi che parlano indistintamente di nuove frontiere di democratizzazione e parità, il rapporto tra nuove tecnologie della comunicazione, i minori d'età, la sessualità e l'affettività si definisce come un terreno ricco sia di rischi sia di opportunità.

**Per ciò che concerne l'intimità, internet non diviene solo l'oscura porta di accesso a mondi adulti che dovrebbero stare lontani dagli occhi dei più piccoli, ma anche un modo per trovare alcune risposte che l'imbarazzo o la vergogna spesso rendono inaccessibili nel confronto con i pari o con i genitori.**

La rete non è un mondo a sé stante, vi sono piuttosto dinamiche di reciproca interazione che ribadiscono, una volta ancora, lo stretto contatto tra la vita quotidiana e mezzi di comunicazione.

Solcando gli spazi che la rete mette a disposizione con gli occhi di chi ogni giorno naviga attraverso le pagine web si può infatti capire quanto spesso le paure adulte monopolizzino i discorsi su internet.

**Varie ricerche hanno più volte rilevato le capacità dei più giovani e dei più piccoli di dotare di significato le proprie azioni per utilizzare le risorse che la rete mette loro a disposizione**

**In relazione all'intimità, la rete non è un mondo a sé stante, vi sono dinamiche di reciproca interazione**

**per meglio esplorare la sessualità, così come l'affettività, e cercare dei significati che spesso nelle famiglie o nel gruppo dei pari sono difficili da ritrovare.**

In relazione all'intimità, per bambini e ragazzi la rete significa spesso **ricerca di risposte, confronto con i coetanei, controllo dell'ansia**.

Tutto avviene frequentemente sotto la spinta del desiderio di mostrare la **propria "normalità" e la sicurezza del proprio corpo in continuo mutamento** ai coetanei (fuori e dentro alla rete) e, in primis, a se stessi.

Questo accade non solo tramite la ricerca d'informazioni, ma anche attraverso la costruzione dei propri profili personali nei siti di social networking o, ancora, nelle pratiche di consumo della rete in relazione alla corporeità.

In questo percorso vi sono rischi e pericoli che possono generare situazioni non previste e spiacevoli.

Per questo occorre "aiutare" i ragaz-

zi ma anche genitori e adulti di riferimento, a costruire strumenti di lettura delle situazioni mediate in modo da favorire un'esplorazione quanto più libera, ma al contempo sicura, utile al percorso di crescita di chi, per l'età che sta vivendo, ha la necessità di mettersi in gioco.

**Bisogna aiutare i più piccoli a riconoscere i pericoli che la rete può nascondere, a comprendere l'importanza della propria intimità e quanto essa potrebbe essere potenzialmente violata**, con maggiore semplicità, nel momento in cui donano l'accesso alle proprie informazioni agli altri utenti (più o meno conosciuti). Bisogna supportare la crescita sessuale e affettiva non semplicemente chiudendo un canale comunicativo quale internet, ma accompagnando i ragazzi, da una parte, utilizzando le risorse tecnologiche che sono disponibili al fine di evitare contatti indesiderati (filtri, blacklist, etc.) e, dall'altra, costruendo con loro un **percorso conoscitivo e di sensibilizzazione che non ha a che fare solo con la rete, ma piuttosto riguarda i contenuti che essa, parte della vita di ciascuno, veicola**.

A fianco del modo in cui internet entra nella vita dei minori, bisogna interessarsi anche delle condizioni dell'infanzia e dell'adolescenza, e il modo in cui stanno cambiando, con un'attenzione critica.

Sono queste mutazioni, infatti, che danno forma ai significati che assume l'uso di internet da parte dei più giovani e le conseguenze nella loro quotidianità.

L'assenza totale di un supporto per ciò che concerne le tematiche vicine all'intimità da parte di genitori, educatori e adulti in generale è ciò che più facilmente rende pericolosa la rete che, in situazioni del genere, può diventare l'unica fonte di confronto.

**E' senza gli strumenti utili per una lettura critica della rete che aumentano realmente i pericoli.**

***Cosimo Marco Scarcelli***
*Sociologo, Università degli Studi di Padova*

# ANORESSIA E BULIMIA IN RETE, COME RICONOSCERLE

In ragione della loro crescente diffusione, in particolare nelle fasce più giovani della popolazione, i Disturbi del Comportamento Alimentare (DCA) generano da tempo un'ampia discussione pubblica che sta sempre più interessando anche Internet, per la **presenza di siti, forum e blog pro-Ana e pro-Mia, dove "ana" sta per anoressia e "mia" per bulimia, esempi di comunità online in cui i principali contenuti sono relativi, principalmente, ai comportamenti anoressici e bulimici**. Nati negli Stati Uniti verso la seconda metà degli anni Novanta, questi spazi del web cominciano a diffondersi rapidamente anche in Italia agli inizi degli anni Duemila e hanno, come peculiarità, la velocità con la quale nascono e si moltiplicano, al di là dei tentativi di contenimento e della richiesta di chiusura immediata da parte dei gestori.

**Spesso organizzate in blog o forum, le forme di comunicazione pro-Ana e pro-Mia sono drammaticamente un efficace strumento di "partecipazione" alla malattia, oltre che di diffusione della stessa tra le adolescenti**. Sono luoghi virtuali che fungono da rete di sostegno e che si contrappongono alla famiglia e ai medici: **"comunità di malattia" in cui le partecipanti, giovanissime, si scambiano consigli e stati d'animo,** immagini e contenuti che supportano e rinforzano la loro patologia, consolidando i processi di individuazione e di identificazione, sottolineando la presenza, da una parte, di **"nemici" da cui guardarsi - coloro che vogliono farti ingrassare - e, dall'altra, di riferimenti simbolici e tecnici in grado di aiutare l'adolescente malata a percorrere il suo cammino di malattia**.

**Le forme di comunicazione pro-Ana e pro-Mia sono purtroppo un efficace strumento di diffusione dei DCA**

Ma come è possibile riconoscerle?

Uno dei termini più utilizzati dai soggetti affetti da disturbo alimentare è **"thinspiration"**, eventualmente contratto in "thinspo": non indica solo il voler essere magre, ispirate dalla magrezza, bensì assumere personaggi del mondo dello spettacolo, del cinema, della moda ecc. come modelli di perfezione e di bellezza che concretamente incarnano il paradigma a cui ci si ispira. Digitando in un motore di ricerca questi termini, appaiono non solo centinaia di immagini di modelle e attrici magrissime, ma un numero

ancora più elevato di foto amatoriali di ragazze, soprattutto adolescenti, del tutto identiche nella posa e nel significato che vogliono trasmettere: tra questi, la t-shirt alzata fino al seno per mostrare il busto senza un filo di grasso o i jeans leggermente abbassati affinché si vedano le ossa sporgenti dell'anca. **Le tematiche ricorrenti nei blog sono le diete effettuate e i metodi per dimagrire o per non mangiare**. Anche argomenti che non hanno nulla a che vedere con il peso corporeo (lo shopping con le amiche, i risultati scolastici ecc.) diventano occasioni per parlare di chili e dell'obiettivo di diventare magrissima. Per i blog attivi da qualche tempo, tali resoconti diventano sempre più scarni, lasciando spazio esclusivamente ai diari alimentari, ovvero l'elenco dei pasti della giornata, la cui descrizione, dettagliatissima, è accompagnata dal calcolo delle calorie ingerite. In tutti i blog che si autodefiniscono pro-Ana compaiono lunghe liste che hanno l'intento di sostenere e incentivare il comportamento patologico. Tra i più noti: **l'elenco, in dieci punti, dei "comandamenti della magrezza" e il Credo Ana", considerato il manifesto della pratica anoressica**.

Molto diffusi, inoltre, sono i lunghi elenchi di motivi per non mangiare e di trucchi per distogliere il pensiero dal cibo, incrementare il senso di sazietà o, ancora, per non destare sospetti in famiglia. Il dolore provocato dal digiuno può essere mitigato dal riscontro della sofferenza comune e si rimuove nell'osservare i progressi ottenuti dalle altre, testimoniati dalle fotografie che le ragazze si scambiano o nella compilazione di tabelle in cui inserire le proprie misure (quali il peso o il girovita), in un frame generale in cui non è il riconoscimento della patologia alimentare a guidare la narrazione di sé: le pro-Ana, infatti, rifiutano l'etichetta di "malate" e, quando nelle loro pagine qualche utente interviene per sottolineare le pericolose conseguenze di certi comportamenti, le reazioni sono di irritazione o colleriche. Per tutte, vi è l'impressione di potersi controllare e di poter vivere con poche calorie al giorno senza il rischio di ammalarsi. **Sono narrazioni di malattia, di corporeità, di identità femminile che si costituiscono come un pericoloso modello da inseguire, specialmente da ragazze che sono alla difficoltosa ricerca di un senso da dare alla propria giovane vita**. Condividere con i propri figli l'esperienza della navigazione online "dal punto di vista" dei minori può significare anche riconoscere quei **"segni nella rete"**, nel blog o nella pagina facebook della propria figlia o delle sue amiche, che sono **segnali di una sofferenza**, di una **richiesta d'aiuto**, di un problema da affrontare assieme.

*Claudio Riva*
*Sociologo, Università degli Studi di Padova*



## LA POLIZIA POSTALE E DELLE COMUNICAZIONI

La *mission* della Polizia Postale e delle Comunicazioni è la prevenzione e la repressione di tutti i crimini che aggrediscono i servizi postali e di comunicazione, soprattutto quelli che si basano sulle nuove tecnologie e sulla rete Internet.
Ogni volta che si ritiene esser vittime di crimini commessi attraverso gli strumenti informatici è opportuno rivolgersi alle Forze di polizia in genere ed in particolare al più vicino ufficio della Polizia Postale e delle Comunicazioni presente sul territorio.

### SEZIONI

**Belluno**
tel. 0437931776, 0437932129
fax 0437939886
**Padova**
tel. 049656456, 049666038
fax 0498772004
**Rovigo**
tel. 0425202521, 0425420330
fax 0425460168
**Treviso**
tel. 0422653301-2
fax 0422653244
**Verona**
tel. 0458059386, 0458059309
fax 0458059446
**Vicenza**
tel. 0444507070, 0444338558
fax 0444322554

### CONTATTI

Compartimento della Polizia Postale e delle Comunicazioni per il Veneto.
**Venezia**
Via Cappelletto, 11,
VENEZIA MESTRE, CAP 30174
tel. 04129073111, 0412907349,
fax 0415310438,
email: poltel.ve@poliziadistato.it

### LINK

www.poliziadistato.it
www.commissariatodips.it

note

Il Comitato Regionale per le Comunicazioni Co.Re.Com è un organo istituito presso il Consiglio Regionale del Veneto e **svolge funzioni di consulenza, gestione e controllo in materia di comunicazioni**. Il Comitato è, altresì, organo funzionale dell'Autorità per le garanzie nelle Comunicazioni (Agcom) e ha competenze istruttorie per conto del Ministero dello Sviluppo Economico.

**La legge regionale 10 agosto del 2001, n. 18, ne disciplina l'organizzazione ed il funzionamento.**

Il Comitato è costituito da 7 componenti, compreso il Presidente, scelti fra persone in possesso dei necessari requisiti di competenza ed esperienza nel settore della comunicazione nei suoi aspetti culturali, giuridici, economici e tecnologici.

Il Presidente e i componenti sono eletti dal Consiglio regionale, restano in carica per tutta la durata delle legislatura regionale e non sono immediatamente rieleggibili.

Entro il 31 marzo di ogni anno, il Co.Re.Com. presenta al Consiglio regionale e all'Agcom, il resoconto dell'attività svolta nell'anno precedente.

Entro il 15 settembre di ogni anno, il Co.Re.Com. presenta al Consiglio Regionale il programma di attività per l'anno successivo, specificando la parte relativa alle funzioni proprie e quella relativa alle funzioni delegate.

Per l'esercizio delle sue funzioni il Co.re.Com è assistito dall'Unità Complessa Co.re.Com, una struttura tecnico - amministrativa istituita nell'ambito del Consiglio Regionale del Veneto.

**I compiti attribuiti al Co.Re.Com. sono molteplici. Rientrano tra le funzioni proprie del Co.re.com l'attività di:**

**- consulenza agli organi regionali in materia di comunicazione e informazione locale** anche in forma di pareri preventivi sui provvedimenti della Giunta e del Consiglio regionale nel settore radiotelevisivo e dei media;

**- vigilanza sulla comunicazione politica e sul rispetto della "par condicio" da parte delle radio e televisioni private e della Rai regionale, in particolare durante le campagne elettorali e referendarie;**

**- messa in onda e rimborso dei messaggi politici autogestiti gratuiti (MAG) trasmessi dalle emittenti radiotelevisive venete;**

**- monitoraggio del sistema televisivo locale a garanzia della completa ed equilibrata informazione ai cittadini**

**- (MAG) trasmessi dalle emittenti radiotelevisive venete;**

**- monitoraggio del sistema televisivo locale a garanzia della completa ed equilibrata informazione ai cittadini del Veneto:**

**progettazione e realizzazione di iniziative promozionali, di studio e di ricerca nel campo della comunicazione;**

**- accesso radiofonico e televisivo alle trasmissioni di Rai 3 Veneto;**

**- predisposizione, per conto del Ministero dello Sviluppo Economico, della graduatoria in base alla quale sono assegnati contribuiti ministeriali alle emittenti televisive locali.**

- Il Co.Re.Com, inoltre, a seguito della Convenzione stipulata nel Dicembre 2004 tra l'Agcom e la Regione del Veneto, svolge delle funzioni di vigilanza e garanzia in materia di comunicazioni, in materia di:

- tentativi di conciliazione nelle controversie tra gestori del servizio di telecomunicazione e utenti in ambito locale;

- vigilanza in materia di tutela dei minori con riferimento al settore radiotelevisivo locale;

- esercizio del diritto di rettifica con riferimento al settore radiotelevisivo locale;

- vigilanza sul rispetto dei criteri per la pubblicazione e diffusione dei sondaggi sui media locali.

CORECOM
Comitato Regionale per le Comunicazioni

**COMITATO:**
**Alberto Cartia (Presidente)**
**Roberta Boscolo Anzoletti, Franco Gabrieli, Giovanni Gallo,**
**Mariarosa Pellizzari, Silvio Scanagatta, Luciano Zennaro**

**CORECOM Veneto**
Via Poerio, n.33
Mestre Venezia, CAP 30171
Tel. 041 2701650
Fax 041 2701659
email: uccorecom@consiglioveneto.it
Pec: corecom@consiglioveneto.legalmail.it
http://corecom.consiglioveneto.it

**"Internet @ minori: navigazione sicura"- CORECOM del Veneto**
**Progetto editoriale a cura di Patrizia Adamoli** Settembre 2013

Progetto Grafico: Loredana Banfi
Stampa: