

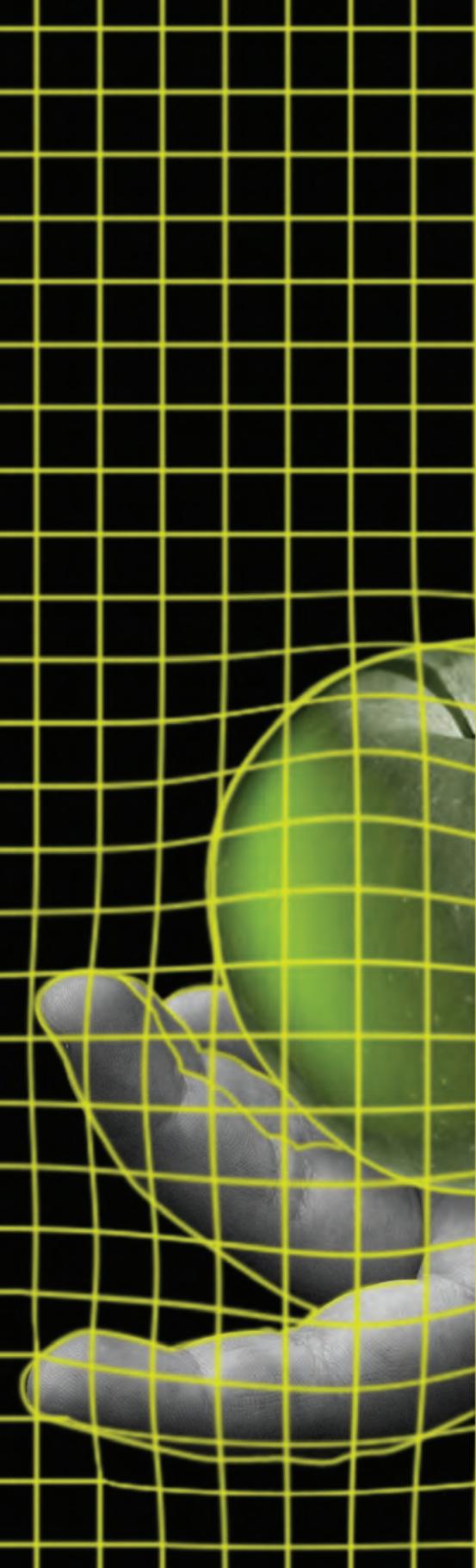


Regione Toscana

corecom

comitato regionale  
per le comunicazioni

# Internet @**minori** **adulti**







*Regione Toscana*

**corecom**

*comitato regionale  
per le comunicazioni*

Vademecum  
**Internet**  
**@** **minori**  
**adulti**

Il Vademecum informativo Internet@minori@adulti è uno strumento di comunicazione del Corecom Toscana, Comitato Regionale per le Comunicazioni.

Il Vademecum è stato realizzato da docenti del Dipartimento di Scienze Politiche e Internazionali dell'Università degli Studi di Siena (referenti scientifici progetto: prof.ssa Donatella Cherubini - docente di Storia del giornalismo; prof.ssa Michela Manetti - docente di Diritto dell'informazione).

Si ringrazia per la prefazione il prof. Alfredo Montagna, sostituto procuratore generale presso la Corte di Cassazione - Roma.

**WORK IN PROGRESS**

**Versione provvisoria - maggio 2013**

**Versione e stampa definitiva - settembre 2013**

## PREMESSA

Con la predisposizione del presente vademecum “Internet@minori@adulti” il Corecom Toscana intende fornire uno strumento informativo sulla tematica del rapporto Internet, minori e genitori, da diffondere all’interno nelle scuole medie inferiori della propria regione.

Il presente vademecum, senza allarmismi di sorta, evidenzia i rischi e i pericoli di Internet, ma anche le potenzialità creative e di sviluppo delle capacità comunicative e relazionali che la rete può offrire al minore.

L’iniziativa, prevista nel programma del Comitato, approvato dal Consiglio Regionale, si inserisce nell’ambito della delega per la tutela dei minori, relativamente alle trasmissioni e ai palinsesti delle emittenti locali, affidata al sistema dei Corecom dall’Autorità per la Garanzia delle Comunicazioni (Agcom).

“Internet@minori@adulti”, realizzato dall’Università degli Studi di Siena, che ringrazio a nome dell’intero Comitato, è finalizzato sia alla tutela dei cosiddetti nativi digitali, per proteggerli dalle insidie della rete (cyber-bullismo, pedopornografia on-line, *grooming*) che per informare gli adulti (i genitori) e gli anziani (i nonni) su come vigilare e aiutare figli e nipoti ad utilizzare lo strumento informatico con intelligenza e senza rischi.

Nelle nostre intenzioni c’è l’auspicio che la diffusione del vademecum nelle scuole medie inferiori sia, soprattutto, un’occasione di riflessione intergenerazionale sul rapporto Internet e minori non solo per gli studenti ma anche per i loro genitori e i loro nonni, con l’importante condivisione degli insegnanti.

Il percorso informativo inizierà, in via sperimentale, nelle scuole medie inferiori della Toscana meridionale per proseguire in quelle della zona nord-costiera e coprire, poi, le altre aree territoriali della regione.

I contenuti del vademecum saranno illustrati e spiegati da docenti universitari, da esperti della rete, dai rappresentanti e dai tecnici delle autorità che effettuano i controlli sul corretto utilizzo di Internet, come a titolo d’esempio la Polizia Postale. L’importanza dei risvolti legali è, infatti, ben evidenziata nella prefazione del sostituto procuratore generale presso la Corte Suprema di Cassazione che, sentitamente, ringrazio.

Sandro Vannini  
Presidente Corecom Toscana



## INDICE

PREFAZIONE (Alfredo Montagna)

<b>I. Comunicazione e informazione nell'era di Internet</b>	<b>3</b>
I.1. Il confronto generazionale tra adulti e minori	3
I.2. Dal Web 1.0 al Web 3.0	4
I.3. Nativi digitali e immigrati digitali	5
<b>II. L'uso di Internet da parte dei minori</b>	<b>7</b>
II.1. Le statistiche nazionali	7
II.2. I riscontri a livello europeo	9
<b>III. Perché Internet è fonte di rischi per i minori</b>	<b>11</b>
III.1. Il "regno della libertà"	11
III. 2. Dieci cose da sapere sulla Rete	12
III. 3. I rischi generali connessi alla navigazione	22
III. 4. I rischi connessi alla socializzazione in Rete	25
III. 5. I rischi connessi alla ricerca di informazioni in Rete	28
III. 6. Il rischio che i minori commettano illeciti	29
<b>IV. I suggerimenti dell'esperto informatico ai minori e ai genitori</b>	<b>33</b>
IV.1. La nota regola delle tre S: Sesso, Sangue, Soldi	33
IV. 2. Autostima, riconoscimento sociale e sindrome dell'avatar	35
IV. 3. Breviario per naviganti giovani o di lungo corso	37
IV. 4. La solitudine	39
IV. 5. Alcune dritte per una tecnologia consapevole	40
<b>V. Dal giornale di carta alle notizie sul Web: <i>Vanishing paper</i> e informazione online</b>	<b>43</b>
V.1. La sfida alla carta stampata	43
V. 2. Dall'informazione alla totale interattività	44
V. 3. L'evoluzione del quotidiano: versione cartacea, online, mobile e su tablet	45
V. 4. Avviso ai naviganti in cerca di "vere" notizie	47
<b>Glossario</b>	<b>49</b>
Help Desk: Link Web, Denunce e Segnalazioni, Recapiti Utili	49



## PREFAZIONE

La analisi del contenuto del presente lavoro, elaborato da un gruppo di esperti per conto del Comitato Regionale per le Comunicazioni della Toscana, induce a una serie di riflessioni.

La prima è certamente quella dell'apprezzamento della analisi "a tutto campo" sul nuovo mondo rappresentato dal sistema di collegamento attraverso Internet, i cui vantaggi viviamo quotidianamente, ma dei cui svantaggi sembriamo non volere prendere pienamente coscienza, specialmente quando questi si traducono in un necessario impegno nel controllo di ciò che da Internet ci è messo a disposizione. Ed è su questo fronte che, nel salutare con favore sia il lavoro in sé che le modalità con le quali si è programmata la sua divulgazione, vorrei aggiungere le mie personali osservazioni, quale operatore del diritto che dal proprio osservatorio privilegiato (per quanto possa definirsi privilegiato il punto di osservazione di chi è costretto a misurarsi giornalmente con la capacità dell'uomo di trovare in ogni nuovo segmento della vita l'occasione per dare sfogo alle proprie peggiori pulsioni) può richiamare quanti hanno rapporti con i minori ad alzare il livello di attenzione, per sapere cogliere i tanti segnali che i giovani ci mandano allorché vengono a trovarsi in situazioni di disagio.

La famiglia, gli educatori, tutti coloro che a vario titolo interagiscono con un minore, hanno oggi l'obbligo, ognuno secondo il proprio ruolo, di fare quanto è in loro potere per neutralizzare gli inevitabili elementi negativi che l'accesso a Internet porta con sé; infatti l'esperienza giudiziaria dimostra come alla fattiva e concreta attività di controllo e regolamentazione da parte degli organismi pubblici non si accompagna una altrettanto adeguata collaborazione dei cittadini, quasi che proprio coloro che sono più vicini al minore ignorino i rischi presenti nei *social network*, nei blog, nei forum, nelle chat in genere.

Il richiamo alla necessità di uno sguardo, anche se discreto, sulle attività online dei nostri figli viene avvertito sovente come una "lezione pedante" a chi ritiene di avere già tutto sotto controllo; ma l'esperienza dimostra il contrario.

Il dato oggettivo secondo il quale i giovani sono i massimi utilizzatori di questo nuovo modo di comunicare è a conoscenza anche di coloro che non sono animati dal semplice desiderio di interagire, ma che in questo "nuovo mondo" vedono l'occasione di "agganciare" il minore per fini distorti, se non delinquenziali.

Nella nostra legislazione è stato introdotto, con la legge 3 agosto 1998 n. 269, il

reato di pornografia minorile, attraverso il quale si sanziona chiunque coinvolge un minore, in vario modo, in attività pornografiche, e ciò anche per via telematica (si tratta di un reato che prevede diverse ipotesi delittuose punite con pene detentive elevate, sino a 12 anni).

La realtà supera anche in questo campo la fantasia, per cui non esiste migliore lezione di quanto realmente accaduto; anche di recente la corte di cassazione (in una udienza tenutasi nell'aprile di quest'anno) è stata chiamata a giudicare il caso nel quale un soggetto qualificatosi come pilota di aereo era riuscito a contattare, utilizzando una serie di differenti identità, nell'arco di meno di due anni, ben 246 utenti di chat, tutte di sesso femminile e di minore età, che era riuscito a indurre a compiere su se stesse atti sessuali online (il cui contenuto si risparmia al lettore), memorizzando poi i filmati nel proprio computer (per un uso personale e/o di divulgazione in Internet). Non occorre evidenziare che l'approccio è progressivo, per cui una volta che il minore ha acconsentito a visualizzare attraverso la web cam gesti ritenuti di scarso impatto erotico, il ragazzo viene costretto a "procedere oltre" con la minaccia che in caso contrario verrebbe data pubblicità alle prime e meno invasive condotte (ma pur sempre tali da generare il timore di una scoperta di quanto fatto in precedenza).

Ma questo è soltanto il primo e pur grave stadio delle possibili conseguenze cui può portare il distorto rapporto che si viene a creare tra un soggetto debole (il minore) e un adulto (spesso presentatosi online come più giovane della propria reale età); anche in questo caso ci soccorre l'esperienza giudiziaria chiamata a giudicare un soggetto che, dopo gli iniziali contatti telematici, era giunto a convincere una minore ad avere un incontro reale, prevedendo anche la prenotazione di una camera d'albergo, e non riuscendo a raggiungere il proprio scopo solo per l'intervento del fato (un contrattempo durante il viaggio per raggiungere la ragazza).

L'insegnamento che si ricava dall'esperienza quotidiana ci porta così a salutare con estremo favore iniziative come quella del Comitato Regionale per le Comunicazioni della Toscana, che, senza innescare inutili allarmismi, raccontano a noi tutti che in un contesto sociale e di comunicazione diverso da quello cui eravamo abituati sono richieste consapevolezza nuova e strumenti di leggibilità aggiornati.

*Alfredo Montagna  
Sostituto Procuratore Generale  
presso la Corte Suprema di Cassazione - Roma*

## I. COMUNICAZIONE E INFORMAZIONE NELL'ERA DI INTERNET

### I.1. Il confronto generazionale tra adulti e minori

**Comunicare significa trasmettere messaggi**, instaurando un rapporto diretto tra individui che interagiscono **sulla base di codici comuni**. Si tratta perciò di un'attività universale e necessaria, presente in tutte le società e a lungo espressa soprattutto con la voce<sup>1</sup>.

Possiamo dire che la storia dell'umanità sia anche il succedersi di forme diverse della comunicazione, dalla voce alla **stampa**, agli altri **mezzi di comunicazione di massa (mass-media)** come la **radio**, la **televisione**, il **cinema**.

Se quindi tutte le società sono necessariamente "della comunicazione e dell'informazione", la nostra lo è diventata in modo generalizzato e pressoché totale con il diffondersi di uno strumento **dalle enormi potenzialità** quale è **Internet**. Si tratta di uno strumento non

definibile semplicemente come nuovo mezzo di comunicazione di massa: attraverso la **Rete Web** racchiude in sé tutti gli altri (**multimedialità**), offrendo opportunità talmente ampie da rendere impossibile il paragone con le precedenti forme della comunicazione.

In questa parte introduttiva è necessario richiamare sinteticamente l'evoluzione del Web e soprattutto le **differenze tra adulti e minori nell'approccio a Internet e nel suo utilizzo**. Si potranno così individuare le possibilità di confronto e scambio tra le risorse culturali di chi ha iniziato a navigare "da grande" e l'abilità pratica di chi si è trovato a farlo fin da bambino.



<sup>1</sup> A. BRIGGS, P. BURKE, Storia sociale dei media. Da Gutenberg a Internet, Bologna, il Mulino, 2007 [A Social History of the Media. From Gutenberg to the Internet, Cambridge, Polity Press, 2005], p. 13.

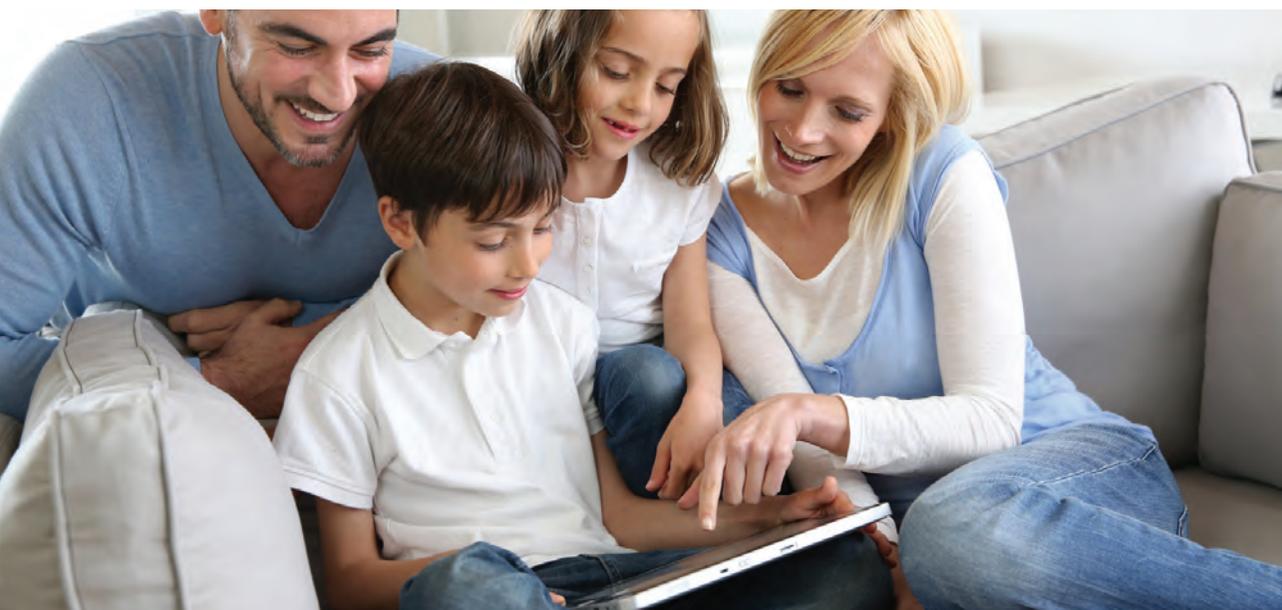
## I.2. Dal Web 1.0 al Web 3.0

**La Rete degli esordi era caratterizzata dalla presenza di siti statici:** in pratica l'utente poteva visitarli, navigare tra le pagine, leggerne i testi e fruirne i contenuti, passare da un sito a un altro tramite i *link* – cioè tramite i collegamenti ipertestuali eventualmente presenti tra un sito e un altro. La ricerca di informazioni veniva effettuata grazie ai motori di ricerca che davano – come risultati – una serie di pagine/siti rispondenti a quanto cercato. **L'utente non poteva in alcun modo interagire con i contenuti dei siti: li doveva fruire così com'erano.**

Con il Web 2.0 diventano centrali, invece, la collaborazione, la condivisione, l'interazione tra utente e sito. **Se il Web 1.0 si poteva definire statico, il Web 2.0 è decisamente dinamico.** L'utente non è più solo un lettore, un consumatore passivo di contenuti, ma li crea direttamente (o contribuisce a crearli) e li condivide.

Ecco alcuni esempi di siti e servizi che sono nati a tutti gli effetti con il Web 2.0:

- **social network** (cioè network sociali come Facebook, Twitter, Flickr, Youtube, Slideshare,...);
- **applicativi basati sul Web** (GoogleDocs,..);
- **blog e podcast;**
- **CMS** (Content Management Systems, cioè sistemi per la gestione di contenuti che sono destinati a cambiare continuamente);
- **sottoscrizione a sistemi di aggiornamento** (feed RSS,...).



Il Web 3.0 è ancora qualcosa di poco definito: le parole chiave di questa ultima versione del Web dovrebbero essere sia la **vastità** dei dati e del loro utilizzo/riutilizzo sia la capacità **semantica**, ossia il riconoscimento del vero significato che i dati stessi hanno, rispetto al contesto in cui sono stati creati.

Infatti, passando dal Web 1.0 al Web 2.0 è rimasto in sospeso un problema: prima c'era scarsità di informazioni e spesso le ricerche non davano i risultati sperati; ora i dati sono tantissimi – a volte troppi – ed è quindi sempre più difficile districarsi tra di loro (il motore di ricerca è un *software*, non una persona!) per ottenere solo quelli veramente significativi.

Proporre risultati che siano strettamente in tema rispetto al contesto fa parte quindi degli obiettivi del Web semantico, cioè del Web 3.0<sup>2</sup>.

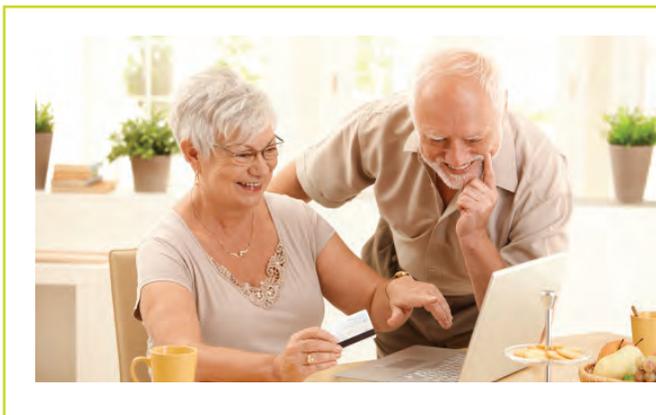
### I.3. Nativi digitali e immigrati digitali

I *Digital natives* sono le generazioni nate a partire dal 1990, anno in cui è cominciato il *boom* delle nuove tecnologie. La maggior parte di questi ragazzi (nei Paesi sviluppati)

è cresciuta avvezza all'uso costante di cellulari, macchine fotografiche e apparecchi musicali digitali, oltre che della Rete, avvicinandosi in modo naturale alla multimedialità.

Tuttavia, più che acquisire vere competenze nell'uso degli strumenti tecnologici, i ragazzi hanno sviluppato una particolare abilità pratica. Infatti operano a

velocità “supersonica” con le tastiere riuscendo anche a svolgere più funzioni contemporaneamente, quali ad esempio chiacchierare con l'amico guardandolo in faccia e contemporaneamente digitare sulla tastiera del cellulare un messaggio di *whatsApp*<sup>3</sup>.



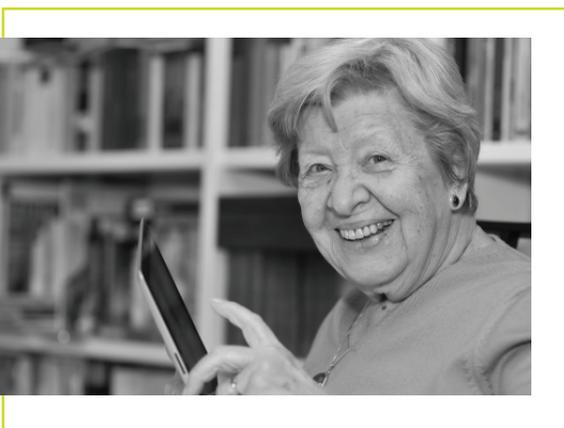
2 Questa versione del Web potrà anche iniziare a sfruttare una vera e propria realtà aumentata, come si propone di illustrare il video rintracciabile in: <http://www.youtube.com/watch?v=kYpxpgyCcns>, predisposto dalla Cisco, una delle aziende leader del settore.

3 WhatsApp è un'app mobile multi-piattaforma che consente di scambiare messaggi di testo con i contatti della propria rubrica, che a loro volta devono avere installato il programma sul loro device. È molto diffusa tra i più giovani: oltre alla messaggistica istantanea di base, permette di creare chat di gruppo, condividere file audio, video e immagini, nonché di geo-taggarli.

È nato anche un linguaggio specifico che potrebbe essere definito da “addetti ai lavori”, dove le vocali sono quasi del tutto abolite (cm, tt, xkè, etc.): classico linguaggio da chat.

E gli **immigrati digitali**? Sono tutti quelli che pur attraversando l’evoluzione delle nuove tecnologie **mantengono forti resistenze rispetto all’uso competente e abile degli strumenti digitali** (telefonino, Internet, e-mail, sms etc.).

Secondo uno studio condotto da *Time Inc*, i “nativi digitali spostano la loro attenzione da una piattaforma all’altra 27 volte in un’ora e sperimentano un minor numero di ‘alti e bassi emotivi’ rispetto alla generazione precedente”<sup>4</sup>. Emerge quindi che mentre “gli immigrati digitali sono intuitivamente lineari – vogliono, cioè, vedere l’inizio, la metà e la fine di una storia – per i nativi le storie hanno ancora bisogno di un inizio, di una metà e di una fine, ma loro li accetteranno in qualsiasi ordine”<sup>4</sup> *ibidem*.



Una terza figura è quella poi del **tardivo digitale**: a differenza dell’immigrato digitale – che pur essendo cresciuto prima delle tecnologie digitali le ha adottate in un secondo tempo –, il “tardivo” è invece una **persona cresciuta senza tecnologia, e che la guarda tutt’oggi con diffidenza**.

Il futuro però porterà a un continuo assottigliarsi di distanza tra queste figure, come ha teorizzato **Marc Prensky (l’ideatore dei termini qui citati)**<sup>5</sup>. Nel contempo, sarà

necessario fare riferimento ad altri concetti per leggere la continua evoluzione del rapporto tra l’uomo e le tecnologie digitali:

“Sono convinto che la tecnologia digitale possa essere usata per renderci non solo più intelligenti, ma anche più saggi. La saggezza digitale è un concetto dal duplice significato: la saggezza che si riferisce all’uso delle tecnologie digitali per accedere al potere della conoscenza in una misura superiore a quanto consentito dalle nostre potenzialità innate; e quella che si riferisce all’uso avveduto della tecnologia per migliorare le nostre capacità”<sup>6</sup>.

Raccogliamo dunque l’invito a sfruttare le nuove tecnologie per potenziare le nostre capacità, e quelle dei minori in particolare, ma anche a farne un **uso avveduto**.

<sup>4</sup> [http://www.timeinc.com/pressroom/detail.php?id=releases/time\\_inc\\_study\\_digital\\_natives.php](http://www.timeinc.com/pressroom/detail.php?id=releases/time_inc_study_digital_natives.php)

<sup>5</sup> <http://prezi.com/axzorflwmte0/nativi-e-immigrati-digitali/>

<sup>6</sup> <http://www.wisdompage.com/Prensky01.html>

## II. L'USO DI INTERNET DA PARTE DEI MINORI



### II.1. Le statistiche nazionali

La concreta rilevanza dei rischi derivanti dalla navigazione in Internet effettuata dai minori può essere meglio compresa analizzando due recenti studi, realizzati separatamente dall'IPSOS<sup>7</sup> e dall'ISTAT<sup>8</sup>, dai quali emergono dati significativi in merito ai seguenti aspetti.

**Per quanto riguarda l'uso di Internet**, l'indagine IPSOS, svolta su un campione di maschi e femmine di età compresa tra i 12 e i 17 anni, evidenzia chiaramente come Internet sia ormai oggetto di utilizzo quotidiano da parte di tutti i ragazzi intervistati: in particolare, il 56% di essi naviga tra le 2 e le 4 ore giornaliere; il 19%, circa un'ora al giorno; il 14%, tra le 5 e le 10 ore; il 6%, meno di un'ora al giorno e il 5% rimane connesso al web per 10 ore o più<sup>9</sup>.

In base a risposte multiple fornite dallo stesso campione, è possibile ricavare anche ulteriori informazioni interessanti con riguardo **ai momenti della giornata** nei quali avvengono le connessioni e **ai luoghi** di connessione<sup>10</sup>.

Per quanto concerne il primo profilo, i dati mostrano come nel 75% dei casi il collegamento alla Rete sia effettuato nel pomeriggio; nel 63% la sera; nel 7% la notte e nel 5% al mattino. In relazione al secondo profilo, le statistiche evidenziano come nel 92% dei casi le connessioni avvengano da casa; nel 27% da qualsiasi altro posto, mediante il free wi-fi o con un abbonamento Internet da cellulare/tablet; nel 20% da casa di amici o conoscenti e nel 14% da scuola.

Con riferimento a classi di età **inferiori agli 11 anni**, l'indagine ISTAT rivela come, in un campione di maschi e femmine di età compresa tra i 6 e i 10 anni, meno della metà (il 40,7%) utilizzi Internet e solo il 4,7% si connetta quotidianamente<sup>11</sup>; per quanto riguarda il luogo di connessione, anche in questo caso la gran parte degli intervistati (90,6%) si connette da casa propria<sup>12</sup>.

7 Cfr. IPSOS, Safer Internet Day Study – il cyberbullismo, 2013. L'indagine è stata svolta per conto della Onlus Save the children Italia e il testo integrale è consultabile al seguente indirizzo Internet: <http://www.ipsos.it/pdf/Cyberbullismo.pdf>.

8 Cfr. ISTAT, Cittadini e nuove tecnologie, 2012. Il testo integrale dell'indagine e le relative Tavole allegate sono consultabili al seguente indirizzo Internet: <http://www.istat.it/it/archivio/78166>.

9 Cfr. IPSOS, op. cit., p. 10.

10 Cfr. IPSOS, op. cit., p. 12.

11 Cfr. ISTAT, op. cit., Tavola 2.1.

12 Cfr. ISTAT, op. cit., Tavola 2.9.



**Per quanto riguarda le azioni svolte dai ragazzi su Internet**, i dati ISTAT mostrano<sup>13</sup> come le attività online più effettuate dai minori (maschi e femmine) in età compresa **tra i 6 e i 10 anni** siano, in ordine decrescente: 1) giocare o scaricare giochi, immagini, film, musica; 2) guardare video in streaming; 3) guardare programmi televisivi sul web; 4) spedire o ricevere e-mail; 5) postare messaggi su chat, *social network*, blog, forum, usare servizi di messaggia istantanea; 6)

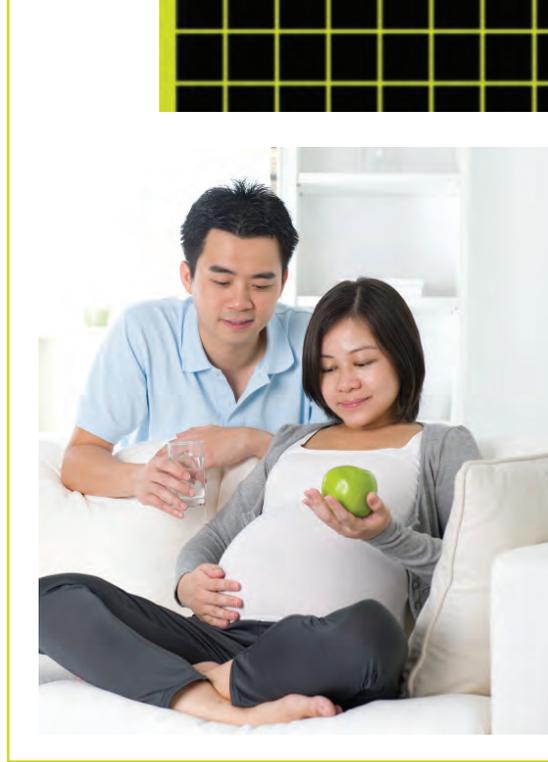
cercare informazioni su merci o servizi; 7) guardare film in streaming; partecipare a giochi in rete con altri utenti; 8) telefonare via Internet/effettuare videochiamate (via webcam); 9) caricare contenuti di propria creazione (testi, fotografie, musica, video, software ecc.) su siti web per condividerli.

Per la classe di età compresa **tra gli 11 e i 14 anni** la graduatoria varia come segue: 1) giocare o scaricare giochi, immagini, film, musica; 2) postare messaggi su chat, *social network*, blog, forum, usare servizi di messaggia istantanea; 3) spedire o ricevere e-mail; 4) guardare video in streaming; 5) guardare programmi televisivi sul web; 6) guardare film in streaming; 7) caricare contenuti di propria creazione (testi, fotografie, musica, video, software ecc.) su siti web per condividerli; 8) telefonare via Internet/effettuare videochiamate (via webcam); 9) partecipare a giochi in rete con altri utenti; 10) cercare informazioni su merci o servizi.

Per la fascia compresa **tra i 15 e i 17 anni**, infine, le stesse attività si presentano nella seguente diversa successione: 1) postare messaggi su chat, *social network*, blog, forum, usare servizi di messaggia istantanea; 2) spedire o ricevere e-mail; 3) giocare o scaricare giochi, immagini, film, musica; 4) guardare video in streaming; 5) caricare contenuti di propria creazione (testi, fotografie, musica, video, software ecc.) su siti web per condividerli; 6) cercare informazioni su merci o servizi; 7) guardare film in streaming; 8) guardare programmi televisivi sul web; 9) telefonare via Internet/effettuare videochiamate (via webcam); 10) partecipare a giochi in rete con altri utenti.

13 Cfr. ISTAT, op. cit., Tavole 3.1, 3.5 e 3.9.

Anche l'indagine IPSOS fornisce informazioni degne di attenzione in quanto individua alcuni **comportamenti che sono diffusi tra i minori** che utilizzano Internet. In particolare, il sondaggio rivela come tra i ragazzi (maschi e femmine) di età compresa tra i 12 e i 17 anni siano comuni le seguenti condotte: inviare dati personali a qualcuno conosciuto in Internet (38%); dare il proprio numero di cellulare a qualcuno conosciuto in Internet (33%); avere rapporti intimi con qualcuno conosciuto in Internet (33%); darsi appuntamento di persona con qualcuno conosciuto in Internet (28%); inviare video/immagini in cui si è raffigurati seminudi o nudi a coetanei conosciuti solo su Internet (22%); inviare o postare immagini nelle quali persone che si conoscono sono raffigurate seminude o nude (22%); inviare video/immagini/attivare la webcam seminudi o nudi per ricevere regali (19%); inviare video/immagini in cui si è raffigurati seminudi o nudi ad adulti conosciuti su Internet (18%)<sup>14</sup>.



## II.2. I riscontri a livello europeo

A completamento di quanto sin qui riportato, è bene rivolgere uno sguardo ai dati emersi a livello europeo dall'ultima indagine EuKidsOnline la quale fornisce un quadro delle principali **preoccupazioni** dei minori che navigano su Internet<sup>15</sup>.

Nello specifico il sondaggio, effettuato su un campione di ragazzi abitanti in 25 Paesi europei (tra i quali anche l'Italia) di età compresa tra i 9 e i 16 anni, rivela come tra le **piattaforme di servizi** che offre la Rete quelle che vengono percepite come rischiose sono, in ordine decrescente, le seguenti: 1) le piattaforme di *video-sharing*; 2) i siti web in generale; 3) i *social network*; 4) i giochi; 5) le chat-room; 6) le e-mail; 7) i servizi di *instant messaging*.

Ognuna di esse, agli occhi dei ragazzi, presenta **specifici pericoli** con riguardo ai contenuti visibili (ad esempio pornografia, violenza), ai contatti intercorsi tramite il web (ad esempio adescamento ovvero *grooming*) e a specifiche condotte tenute in Rete (ad esempio cyber-bullismo; *sexting* ovvero messaggi di natura sessuale; violazione del diritto d'autore o copyright).

<sup>14</sup> Cfr. IPSOS, op. cit., p. 21.

<sup>15</sup> Cfr. EuKidsOnline, In their own words: what bothers children online?, 2013. Il report integrale è consultabile al seguente indirizzo internet: <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>.



### III. PERCHÉ INTERNET È FONTE DI RISCHI PER I MINORI

#### III.1. Il “regno della libertà”

Molti sanno che la navigazione in Rete è fonte di rischi, e non solo per i più giovani, ma non ne hanno piena cognizione. Si tratta di un'ignoranza del tutto comprensibile, dal momento che Internet rappresenta fin dalla sua nascita una sfida alle nostre convinzioni più radicate. **Quando si dice che Internet è il regno della libertà**, e si lotta perché tale rimanga, si dimentica di precisare che si tratta di una libertà molto più ampia di quelle sinora conosciute, non soltanto perché fa uso di una tecnologia molto potente, ma anche perché è in gran parte rimessa all'arbitrio di chi la esercita — e di conseguenza risulta molto più pericolosa per i diritti altrui.

Questo statuto giuridico della comunicazione internettiana è dovuto solo in parte alla natura globale della Rete: il controllo dello Stato sui messaggi ricevibili dai propri cittadini, seppur impegnativo, è tecnicamente possibile, come dimostrano le esperienze dei regimi autoritari. I Paesi occidentali, in via di principio, lo rifiutano, ritenendo vantaggioso — per ragioni non solo culturali, ma anche economiche — consentire **la più ampia disintermediazione sinora conosciuta** nella diffusione dei messaggi.

In altri termini, **da un lato c'è la tecnologia**, che permette la creazione e la diffusione su scala planetaria di messaggi propri dell'utente, aprendo spazi sinora sconosciuti non solo alla comunicazione interpersonale e alla libera manifestazione del pensiero, ma anche alla promozione e alla commercializzazione dei prodotti. **Dall'altra c'è la disciplina giuridica** che, per favorire la più ampia circolazione dei messaggi, li sottrae, di regola, tanto ai controlli delle pubbliche autorità, quanto alla sorveglianza di coloro che rappresentano gli indispensabili intermediari della comunicazione internettiana, vale a dire le aziende, come Google o Yahoo!, che rendono possibile l'uso della Rete.

In sintesi: se in generale noi deleghiamo allo Stato il compito di proteggerci dalle ingiuste minacce ai nostri diritti e ai nostri beni, quando si parla di Internet questo compito è molto più arduo, e deve essere integrato in gran parte da un **uso consapevole e responsabile della nostra libertà, tanto per evitare danni quanto per non causarli ad altri.**

### III. 2. Dieci cose da sapere sulla Rete

#### 1. I messaggi provengono anche da Paesi che non rispettano le nostre regole

Molti messaggi provengono dall'estero, e in particolare da Stati che non rispettano le stesse regole valide in Italia, oppure dai c.d. Stati-canaglia, che non rispettano nessuna regola, neppure quelle imposte dalle convenzioni internazionali sull'uso di Internet.

Può non essere facile capire da dove il messaggio proviene veramente. Un sito che usa la lingua inglese può avere la sua base fisica praticamente ovunque; mentre il fatto che un sito usi la lingua italiana non significa che l'azienda o la persona responsabile trasmetta dall'Italia, e sia pertanto tenuta a rispettare le nostre leggi.

#### 2. I Providers non hanno l'obbligo di controllare i messaggi che trasmettono

In secondo luogo, bisogna sapere che la disciplina accettata da tutti i Paesi civili, ivi compreso il nostro, non consente un'attività di prevenzione e di repressione degli illeciti così efficace come ci si potrebbe aspettare.

Mentre chi pubblica un giornale, o diffonde un film, o trasmette un programma televisivo, è responsabile dei contenuti che trasmette – assieme all'autore dei contenuti stessi – ed è pertanto tenuto a controllarli, lo stesso non vale per l'**Internet Service Provider (ISP)**. Chi fornisce l'accesso ai contenuti della Rete o assicura servizi accessori, ad esempio i motori di ricerca, non è considerato come un "editore", benché svolga la medesima funzione, che consiste nel mettere a disposizione del pubblico dei messaggi.

La libertà della Rete deriva dunque dal fatto che a carico del Provider non esiste un obbligo generale di vigilanza sui contenuti che vengono immessi nella Rete, ma soltanto l'obbligo di segnalare alle autorità i messaggi illeciti *quando e se ne venga a conoscenza*<sup>16</sup>.

Unico responsabile rimane pertanto chi ha immesso in Rete il messaggio lesivo, in qualità di autore dello stesso o in qualità di "editore" di un messaggio creato da altri.

La conseguenza è che le vittime e le stesse Autorità si possono rivolgere solo contro quest'ultimo, ma non anche contro le aziende che forniscono l'accesso ai contenuti: aziende ben note e capaci di risarcire adeguatamente il danno.

Si ricordi che queste compagnie non sono servizi pubblici: pur offrendo molti servizi gratuiti, ricercano profitto dalla propria attività, e la ottengono principalmente tramite l'inserzione di pubblicità.

Di conseguenza non parrebbe illogico imporre loro qualche obbligo di sorveglianza sui contenuti pubblicati.

<sup>16</sup> Così gli artt. 14, 15, 16 e 17 del D. Lgs n. 70 del 2003, con il quale è stata data attuazione alla normativa europea.

Questo tema ha avuto in Italia grande risonanza in occasione della causa promossa dall'Associazione Vividown contro Google, che è stato chiamato a rispondere, assieme agli autori, dei danni causati dalla pubblicazione su Youtube di un video nel quale alcuni ragazzi maltrattavano un loro coetaneo disabile.

Google ha opposto di non essere tenuto a controllare i video, imputandoli alla esclusiva responsabilità di coloro che li caricano su Youtube (nel nostro caso, gli stessi ragazzi autori dei maltrattamenti). I giudici non hanno potuto contestare questa regola, ma hanno notato che Google trae un utile, sia pure indiretto, dai video, dal momento che associa alla visione di questi ultimi la diffusione di pubblicità: un utile tanto più alto quanto più il video è cliccato (come avviene quando esso è scandaloso o scioccante, come era purtroppo nel caso in esame).

Di conseguenza —hanno ritenuto i giudici— Google può avvantaggiarsi del fatto illecito altrui soltanto se prova di avere informato adeguatamente coloro che intendono caricare contenuti su Youtube dei rischi che ciò comporta per la privacy e la dignità di terze persone, e delle conseguenze negative che la legge ne fa discendere a carico dell'uploader.

### **3. ...a meno che non si tratti di messaggi pedopornografici**

Alla regola ora ricordata fa eccezione la legge penale che impone ai fornitori di servizi l'obbligo di individuare tramite appositi sistemi di filtraggio i contenuti pedopornografici e di bloccarli prima della diffusione<sup>17</sup>.

Va peraltro tenuto presente che i filtri non sempre funzionano a dovere: in realtà è molto difficile contrastare adeguatamente tutte le astuzie cui i criminali ricorrono.

Di recente su Facebook Gran Bretagna è stato pubblicato un video dove una bambina veniva abusata da un adulto, video che è stato condiviso da ben 16.000 utenti e ha ricevuto quasi 4.000 "mi piace!" prima che i responsabili del sito riuscissero ad eliminarlo. Questo episodio ha segnato una sconfitta per Facebook, che si impegna programmaticamente a difendere da tali messaggi i propri utenti.

Si noti che l'utente italiano che commentasse "mi piace!" potrebbe violare l'art. 414-bis del Codice penale, che punisce con la reclusione da un anno e sei mesi a cinque anni chi pubblicamente fa apologia di pratiche pedofile o pedopornografiche, ossia le giustifica o le esalta.

### **4. L'identificazione dell'autore del messaggio è talvolta impossibile**

La denuncia presentata alle Autorità dopo che il messaggio illecito sia stato conosciuto consente di far cancellare la pagina web incriminata o di oscurare il sito nel quale è ospitata.

Altro discorso è ottenere una condanna in sede penale o civile del colpevole, quando quest'ultimo ha operato dall'estero, o quando abbia fatto in modo di cancellare le proprie tracce.

Come si sa, nella Rete è assai diffuso il costume di ricorrere a pseudonimi o *nickname*, proprio allo scopo di non essere riconosciuti: a volte per proteggersi da

<sup>17</sup> Artt. 14-ter e 14-quater della legge 3 agosto 1998 n. 269.

minacce ingiuste (come la persecuzione da parte di un regime che limita le libertà democratiche, oppure l'utilizzo indebito dei propri dati personali da parte di altri), a volte invece per poter svolgere indisturbati un'attività criminosa.

C'è da aggiungere che molte persone trovano attraente la possibilità di attribuirsi una identità virtuale diversa da quella reale, presentandosi ai terzi come più giovani o più belli o più interessanti tramite un *avatar* di loro invenzione. Se non ha secondi fini criminosi, si tratta di un divertimento del tutto lecito, che può tuttavia sfuggire di mano: la protezione offerta dall'anonimato induce molti a varcare i limiti che altrimenti rispetterebbero, se è vero che in Rete il *sexting*, ossia la diffusione di messaggi a contenuto erotico, è diventata una vera e propria epidemia.

Ora, è vero che i Providers dispongono dei dati personali che normalmente ottengono al momento dell'utilizzo dei propri servizi, e che sono ovviamente tenuti a riferirli alle Autorità in vista della ricerca del colpevole. È anche vero però che i dati forniti spontaneamente possono essere falsi, sicché l'unico riferimento sicuro rimane l'indirizzo IP del computer dal quale è partito il messaggio: indirizzo che a sua volta può essere disattivato dall'autore che non vuole lasciare tracce.

Insorgono poi complicazioni quando un computer è usato da più persone, ad esempio da colleghi di lavoro o da compagni di scuola. Per questo è indispensabile installare sui computer condivisi un proprio account, protetto da una password personale segreta; per questo, quando ci si rivolge a un *Internet point* è bene controllare che il gestore, secondo gli obblighi di legge, identifichi personalmente il cliente e tenga traccia dell'orario in quale ha utilizzato il computer.



### **5. Tutto ciò che facciamo in Internet lascia tracce pericolose per la nostra privacy; tutto ciò che pubblichiamo volontariamente vi rimane**

L'internauta che non ha nulla da nascondere in compenso viene tracciato dai fornitori dei servizi, che utilizzando le informazioni volontariamente o involontariamente dichiarate da ciascuno di noi sono in grado di risalire non solo alle nostre preferenze di consumo, ma anche allo stato di salute, alla razza, alle opinioni politiche, alla fede religiosa, nonché a fatti che vorremmo restassero privati: ad esempio numerosi servizi di chat, inclusi quelli offerti dai *social network*, permettono di registrare le conversazioni avute con altri utenti.

Questo fatto è oggettivamente pericoloso non solo per

la nostra privacy ma per la nostra libertà in generale: la massa di informazioni che ci riguarda, una volta archiviata, può essere usata da chi la detiene (o da altri che gliela abbiano sottratta) a nostro svantaggio.

**Per questo la legge disciplina l'acquisizione, la conservazione e l'utilizzazione dei nostri dati personali, con particolare riguardo ai dati c.d. sensibili** – quali appunto la razza, la fede, lo stato di salute – che possono dare luogo a più grave pregiudizio sul lavoro o nella vita sociale, imponendo altresì alle imprese l'adozione di adeguate misure di sicurezza per impedire che soggetti esterni possano raccogliere o scaricare in massa (attraverso software spia) i dati che si ritrovano in Rete.

Bisogna, quindi, prestare fiducia soltanto ai siti che dichiarano esplicitamente di rispettare le condizioni imposte dalla legge, in Italia dal D.Lgs. n. 196 del 2003, intitolato Codice per la protezione dei dati personali.

Tra il marzo e l'ottobre 2012 il Gruppo che riunisce le Autorità della privacy dei 27 Paesi dell'Ue ha analizzato la privacy policy di Google che consente, tra l'altro, alla società californiana di incrociare in via generalizzata i dati degli utenti che utilizzano i servizi offerti (da Gmail a YouTube a Google Maps solo per citarne alcuni).

Alla luce dei risultati di questa analisi, i Garanti europei hanno chiesto a Google Inc. di adottare, entro 4 mesi, una serie di modifiche ritenute necessarie per assicurare la conformità dei trattamenti alle disposizioni vigenti sulla protezione dei dati personali.

Bisogna inoltre considerare che **tale tutela non si applica, per definizione, quando siamo noi stessi a decidere di rendere noti i nostri dati, e in generale i nostri messaggi (scritti, fotografie, filmati)**. Questi anzi sono destinati a rimanere visibili a tutti per un tempo indefinito, perché l'uso della Rete è di non cancellare nulla di quanto vi è stato immesso.

Si tratta di una differenza fondamentale rispetto ai mezzi di comunicazione tradizionali. Gli articoli di giornale o i programmi televisivi sono infatti reperibili a distanza di anni, ma ciò richiede di recarsi agli archivi e di svolgere ricerche spesso lunghe e impegnative. D'altra parte, non tutto viene conservato a tempo indeterminato, considerati i costi che l'archiviazione comporta.

Al contrario, la Rete conserva tutto ciò che viene pubblicato (anche se l'autore cancella il documento dal sito nel quale lo ha immesso, ve ne possono essere copie presso terzi) e lo rende reperibile —anche molto tempo dopo— mediante una semplice ricerca per parole.

In altri termini, in Internet non sono ammessi pentimenti: una parola di troppo o un'immagine della quale potremmo non andare fieri in futuro, una volta pubblicata, sfugge alla nostra disponibilità.

È necessario, pertanto, **distinguere accuratamente tra quanto vogliamo comunicare riservatamente a destinatari da noi prescelti e quanto invece vogliamo pubblicare**, ossia rendere accessibile a tutti: l'unico mezzo appropriato a escludere del tutto la pubblicità è la e-mail, che equivale a una lettera in busta chiusa e gode, in base alla Costituzione, di segretezza.

Equivalente è in via di principio il caricamento di un messaggio nella parte “riservata agli amici” del proprio profilo su *social network*. Ma l'autore non può in effetti escludere che questi a loro volta (ad esempio taggando la foto) lo condividano con altri, sconosciuti al mittente originario.

Il problema si sposta allora sulle misure di protezione dei dati che il *social network* mette a disposizione, che bisogna vagliare con attenzione, **scegliendo le impostazioni di privacy più garantistiche**.

A maggior ragione, chi rende un contenuto visibile “a tutti” può ben essere convinto che esso interessi soltanto alla cerchia di persone con le quali normalmente dialoga, ma ciò non toglie che esso diventi conoscibile praticamente a migliaia di persone; anche soggetti estranei al *social network* possono talvolta averne notizia, tramite l'uso di un motore di ricerca.

Come vedremo, evitare la pubblicazione serve non solo a proteggerci da interferenze altrui, ma anche a evitare di commettere involontariamente illeciti.

## **6. Internet è un luogo concepito per gli adulti**

Come è noto, i giornali pornografici e i film registrati su supporti non possono essere venduti se non ad adulti, e non possono essere esposti o reclamizzati in luoghi esposti alla vista dei minori; le pellicole da proiettarsi nelle sale cinematografiche sono soggette alla censura preventiva; la programmazione radiotelevisiva è vincolata al rispetto di determinati orari a tutela dei minori, e le emittenti debbono comunque segnalare se quanto stanno per trasmettere è inadatto alla visione di un pubblico non adulto.

Per tutti i servizi di media audiovisivi (ossia che trasmettono immagini in movimento, anche a richiesta dell'utente) vige inoltre una disciplina piuttosto severa sulle forme e i contenuti della pubblicità, che ha anche lo scopo specifico di proteggere i minori rispetto alla loro “naturale credulità”.

Nessuna cautela specifica è prevista, invece, per i contenuti destinati alla sola diffusione in Rete, la quale si caratterizza pertanto come un luogo destinato agli adulti, e dove gli stessi adulti possono imbattersi senza volerlo in immagini fastidiose o scioccanti (basta cliccare su un annuncio apparentemente innocente o digitare per sbaglio il nome di un sito pornografico).



In effetti, nel 1996 il Governo statunitense si preoccupò di limitare l'esposizione dei minori a messaggi inadatti alla loro età, vietando la diffusione in Internet di contenuti (non solo osceni ma anche) "indecenti".

La legge fu, tuttavia, dichiarata illegittima dalla Corte suprema che ritenne eccessivo imporre a tutti "un linguaggio da educande" quando è invece tecnicamente possibile impedire ai minori l'accesso a siti pericolosi tramite opportuni sistemi di filtraggio, da modulare a discrezione dei genitori<sup>18</sup>.

Sul punto l'Unione europea non ha una posizione diversa da quella degli Stati Uniti; tuttavia ritiene doveroso promuovere tanto forme di *autoregolamentazione* da parte delle imprese che agiscono nel settore (ad esempio per predisporre forme di classificazione dei contenuti, le c.d. *White List e Black List*), quanto iniziative di sensibilizzazione delle famiglie riguardo al problema della sicurezza in Rete.

Da ultimo la Commissione europea ha in sostanza riconosciuto che questa strategia rimarrà poco efficace, e che in generale Internet non servirà davvero a sviluppare le potenzialità delle nuove generazioni digitali, sino a quando la Rete non cesserà – almeno in parte – di essere un luogo destinato agli adulti.

In altre parole, le imprese dovranno essere stimolate non solo a predisporre sistemi di filtraggio, ma anche a rendere disponibili in linea contenuti di qualità destinati ai giovani<sup>19</sup>.

Ci sono aziende che debbono ritenersi già giuridicamente obbligate ad assicurare questo risultato: si tratta delle società concessionarie del servizio pubblico radiotelevisivo, che in base alla loro missione di "educare" oltre che di "intrattenere" il pubblico più giovane sono chiamate a diffondere anche online programmi e servizi di qualità.

<sup>18</sup> Corte Suprema degli Stati Uniti, *J. Reno versus A.C.L.U* (1997).

<sup>19</sup> Vedi la Comunicazione della Commissione europea del 2 maggio 2012 intitolata "Strategia europea per un Internet migliore per i ragazzi".



## 7. La protezione dei minori ricade principalmente sulla famiglia

In sostanza, concedere ai figli o ai nipoti di navigare in Rete equivale a metterli in viaggio verso luoghi sconosciuti<sup>20</sup>, dove ancor più che nel mondo reale mancano soggetti disposti a proteggerli ed aiutarli.

Nessun genitore acconsentirebbe a un viaggio del genere senza prendere le opportune precauzioni, e senza dotare i propri figli dei necessari suggerimenti.

A ciascuna famiglia spetta di scegliere la strategia più adatta, anche in considerazione dell'età dei ragazzi.

Vietare l'accesso alla Rete è una soluzione che rischia di essere facilmente aggirata: basti pensare che in molte città è possibile disporre di aree Wi-Fi nelle quali l'accesso alla Rete è gratuito. La prima cautela consiste nella predisposizione di account diversi per ciascun utente: quelle degli adulti vanno protette con password segrete.

Vengono poi i sistemi di filtraggio resi possibili da appositi software o le forme di navigazione sicura offerti da appositi siti. Infine, sono da preferire i *social network* sicuri, in quanto appositamente dedicati ai ragazzi, e i forum nei quali sia presente un moderatore, che può espellere i partecipanti aggressivi o volgari.

Perché queste cautele funzionino è comunque indispensabile, in via preventiva, che il computer dal quale si naviga sia collocato in un luogo della casa condiviso da tutta la famiglia, e in via successiva che gli adulti consultino regolarmente la cronologia del computer, nella quale rimangono registrati tutti i siti ai quali i ragazzi si sono sia pure involontariamente connessi.

In altre parole, è **indispensabile una gestione condivisa della navigazione**, che richiede da parte degli adulti l'acquisizione di alcune competenze tecniche, la disponibilità a consigliare e la costanza nel vigilare sui comportamenti dei ragazzi.

Un buon modo per creare un'atmosfera di fiducia è chiedere a questi ultimi di mostrare come si usa Internet, e in cambio spiegare loro le avvertenze che ciascun sito indica per l'uso dei propri servizi: avvertenze in genere lunghe e noiose, che però rivelano "l'altra faccia della medaglia".

È possibile anche proporre ai minori un patto nel quale si stabiliscono le regole indefettibili per l'uso di Internet e si fissano le sanzioni in caso di violazione: la più adatta è ovviamente quella che comporta la sospensione dall'uso di Internet per un periodo più o meno lungo<sup>21</sup>.

20 Come fa notare il decalogo pubblicato dal sito [http://www.citta-invisibile.it/int\\_prec\\_ragazzi01.html#regola01](http://www.citta-invisibile.it/int_prec_ragazzi01.html#regola01).

21 Vedi ad esempio il sito [www.e-communication.it/internet-e-minori.it](http://www.e-communication.it/internet-e-minori.it).

## 8. I rischi aumentano con l'uso di dispositivi mobili

La difficoltà di individuare le fonti di pericolo è aumentata da quando la connessione a Internet non è più limitata al computer di casa (o di scuola), ma si ottiene anche con l'uso di strumenti quali il *tablet* e lo *smartphone* (il telefonino chiamato "intelligente" proprio perché offre la possibilità di scaricare contenuti dal Web, di chattare, di leggere e-mail). Le moderne *playstation* consentono inoltre di collegarsi in rete per giocare con sconosciuti, e di condurre parallelamente una conversazione in *chat*.

In tal modo l'accesso alla Rete può svolgersi anche in luoghi dove la sorveglianza dei genitori non è possibile, ovvero dove il minore non è in grado di chiedere consiglio sull'atteggiamento da tenere verso offerte di acquisto o di contatto che gli vengono sottoposte.

Prima di regalare ai ragazzi un dispositivo mobile è bene, pertanto, valutare se questi siano in grado di gestirlo in modo responsabile; anche perché non esistono attualmente sistemi di filtraggio o di controllo parentale per i contenuti cui si accede via telefonino o *tablet* utilizzando un'applicazione anziché un *browser*.

## 9. L'uso della Rete induce l'acquisizione di nuovi modelli di comportamento

A conclusione di questa premessa va ricordato che l'accesso a Internet cambia il nostro modo di vedere le cose. Tutti i sentimenti e i bisogni che proviamo quotidianamente trovano nella Rete una possibilità in più per essere esternati se non soddisfatti, tramite la miriade di servizi offerti<sup>22</sup>.

**La disponibilità di questi nuovi strumenti non è facilmente gestibile**, come dimostrano gli esempi di persone che preferiscono vivere nella realtà virtuale, e in casi limite tagliano completamente i ponti con le persone in carne ed ossa.

Al di là delle ipotesi patologiche, va comunque tenuto presente che l'uso di Internet può spingere a rimuovere le timidezze ma anche gli scrupoli. Nel mondo virtuale chi è riservato può imparare ad aprirsi, ma chi è estroverso può diventare esibizionista o aggressivo, danneggiando sé e gli altri.

Più in generale, si può tendere ad **abusare del mezzo**, quando invece Internet – come una automobile molto potente – va usato con grande cautela. Ad esempio, il fatto che sia possibile raccogliere in Internet gli indirizzi di una quantità di persone sconosciute e inviare loro senza sforzo una quantità di e-mail, anche innocenti, non significa che questo comportamento sia lecito: può infatti sfociare in una forma di molestia. È bene, insomma, attenersi a un uso corretto e rispettare le regole di buona educazione che vigono pure in Internet (dove vanno sotto il nome di *netiquette*).

<sup>22</sup> Vedi il Glossario del *Vademecum*.

Per altro verso, si può nutrire un **falso senso di sicurezza**. Trascurando che il semplice “linkare” o connettersi a un sito sconosciuto, o peggio scaricare contenuti da quest’ultimo, non è sempre un fatto senza conseguenze.

**Per questo bisogna sempre controllare su quale sito ci si trova, e chiedersi di che cosa precisamente si tratta.**

**Neppure è consigliabile abbassare la guardia quando ci si trova all’interno di un social network:** ciò accade talvolta ai più giovani, che di solito usano questi siti per comunicare in modo continuativo con le stesse persone che frequentano nella vita reale, e che pertanto sviluppano la convinzione di trovarsi in un ambiente amico.

Questa idea della “comunità” è eccessivamente ottimistica, almeno nei riguardi di siti che all’origine magari erano limitati agli studenti dello stesso istituto, ma che oggi raccolgono centinaia di migliaia di iscritti. Per quanto i *social network* si impegnino a selezionare e a proteggere i propri iscritti, essi non sono in grado di vagliare l’identità delle persone che si registrano, e di regola possono intervenire soltanto quando il danno è già fatto.

## 10. Gli strumenti che vengono offerti dai soggetti pubblici e privati

Per quanto insufficienti, di per sé soli, a risolvere il problema, esistono validi strumenti che possono aiutare gli adulti ad affrontarlo.

Vi sono innanzitutto sistemi tecnologici che assicurano, in modo più o meno efficace, un controllo della navigazione online per la difesa dei minori. Si tratta dei c.d. **filtri famiglia** che sono in grado di selezionare i contenuti delle pagine Internet in base a specifici criteri<sup>23</sup>. Tale soluzione può essere utilizzata sul pc (mediante l’impostazione dei filtri nativi presenti nel sistema operativo<sup>24</sup> o attraverso l’installazione di uno specifico programma<sup>25</sup>) oppure sul router di accesso a Internet<sup>26</sup> o, ancora, direttamente sulla Rete usufruendo delle estensioni di controllo parentale disponibili per i browser

23 Si fa riferimento a criteri statici, come l’impostazione di Blacklist dei siti il cui accesso viene espressamente inibito, oppure dinamici, come la definizione di Whitelist che indirizzano la navigazione esclusivamente verso siti preselezionati o anche l’impostazione delle c.d. metatag PICS (Platform for Internet Content Selection) le quali consentono di accettare o respingere le pagine web i cui contenuti sono stati classificati (da chi li ha immessi sulla Rete) secondo tale standard (in quest’ultimo caso, il sistema rileva i valori delle metatag PICS associati alle pagine web e, in base al livello di filtraggio impostato, ne inibisce o meno l’accesso ai relativi contenuti).

24 Tali filtri sono integrati, ad esempio, sui sistemi Windows 7, Mac OS e su alcune distribuzioni Linux.

25 Si fa presente che è possibile usufruire di programmi gratuiti scaricabili da Internet (ad esempio Norton Family) o a pagamento (ad esempio Cyber Patrol).

26 Molti modelli di router hanno, infatti, la funzione di filtro famiglia incorporata. In ogni caso, è sempre possibile impostare router che non abbiano tale funzionalità nativa mediante l’installazione di appositi software, quali ad esempio DansGuardian. I vantaggi di utilizzare un filtro sul router sono principalmente due: quello di proteggere l’intera rete dei supporti (pc, notebook etc.) con i quali i minori si connettono a Internet, senza la necessità di impostare filtri su ognuno di essi, e quello di beneficiare di una maggiore sicurezza rispetto alla possibilità che il minore riesca a disattivare il filtro stesso.

Internet (ad esempio Firefox)<sup>27</sup>, delle specifiche funzionalità dei motori di ricerca (ad esempio Google SafeSearch) o di particolari siti web (ad esempio www.davide.it).

Alla fine del 2003 è stato inoltre approvato, su iniziativa del Governo e con la sottoscrizione di diverse associazioni di fornitori di servizi in rete, il Codice “Internet e Minori” che ha lo scopo di rendere la Rete “un luogo sicuro per i minori”<sup>28</sup>.

Si tratta di un impegno di natura esclusivamente volontaria, che potrebbe rappresentare il primo passo verso la trasformazione del Codice in legge vincolante per tutti gli operatori, come è avvenuto in passato per il “Codice Tv e minori”.

In quest’ottica il Comitato che presiedeva all’applicazione del Codice Internet e Minori è stato accorpato nel Comitato Media e Minori, operante presso il Dipartimento delle Comunicazione del Ministero dello Sviluppo Economico, che dovrà predisporre un codice unificato “Media e minori”.

Fatto sta che l’*appeal* di iniziative del genere è rimasto scarso presso le imprese del settore, come ha rilevato di recente la Commissione europea, che si è fatta perciò promotrice di un programma per rendere Internet “un luogo più sicuro per i minori”<sup>29</sup>. Nell’ambito di tale programma è stata realizzata una ricerca sull’uso di Internet da parte dei minori<sup>30</sup> ed è stata stipulata il 1° dicembre 2011 tra le aziende leader del settore una dichiarazione d’intenti<sup>31</sup> con la quale esse si impegnano ad assicurare:

- **strumenti di segnalazione semplici ed efficaci** sui contenuti e sui contatti ritenuti dannosi per i ragazzi;
- **impostazioni sulla privacy adeguate all’età**, per determinare il grado di pubblicità delle informazioni su un utente, o per stabilire se i recapiti e le foto siano visibili solo ai contatti più stretti o se siano pubblici;
- **maggiore utilizzo della classificazione dei contenuti**, per fornire ai genitori fasce d’età chiare;
- **maggiore disponibilità e uso di sistemi di controllo parentale**;
- **effettiva rimozione di materiale pedopornografico**, tramite una migliore collaborazione con le autorità investigative e giudiziarie e le *hotline*<sup>32</sup>.

27 Esiste anche la possibilità di installare gratuitamente sul proprio pc appositi browser dedicati alla navigazione sicura per bambini (ad esempio Il Veliero) e creati con un’interfaccia che ben si adatta alla loro età.

28 Vedilo, con ampio commento, in [www.osservatoriominoi.org/files/codice\\_internet\\_minori.pdf](http://www.osservatoriominoi.org/files/codice_internet_minori.pdf).

29 Vedilo in [www.saferinternet.it](http://www.saferinternet.it)

30 Si tratta di “Eukids online”, commentata nel capitolo III del Vademecum.

31 Promotori della Coalition on Safety sono: Apple, BSKyB, BT, Dailymotion, Deutsche Telekom, Facebook, France Telecom-Orange, Google, Hyves, KPN, Liberty Global, LG Electronics, Mediaset, Microsoft, Netlog, Nintendo, Nokia, Opera Software, Research in Motion, RTL Group, Samsung, Sulake, Telefonica, Telia Sonera, Telenor Group, Tuenti, Vivendi, Vodafone.

32 Per le hotline per la denuncia di materiale pedopornografico, come stop-it o sicurinrete vedi la successiva nota 42.

I poteri pubblici svolgono inoltre azioni di sensibilizzazione, ovvero di educazione degli adulti e dei minori all'uso sicuro di Internet.

**Una di queste azioni, promossa dal Comitato Regionale per le Comunicazioni della Toscana, è il Vademecum che state leggendo<sup>33</sup>.**

I Corecom possono infatti intraprendere iniziative nella materia della tutela dei minori, grazie alla delega loro concessa dall'Autorità per le garanzie delle comunicazioni (meglio nota come **Agcom**).



### III. 3. I rischi generali connessi alla navigazione

#### 1. Accedere a contenuti osceni o scioccanti

Non è raro che alcuni siti, pur di essere visitati, si rendano rintracciabili attraverso l'uso, tramite il motore di ricerca, di "parole chiave" del tutto innocue. In tal modo l'ignaro internauta può trovarsi costretto a subire la visione di immagini non richieste, o a leggere messaggi disturbanti, tanto più per i minori.

Basta pensare a quanti siti istigano al suicidio o all'autolesionismo (come l'anoressia),

<sup>33</sup> Vedi le analoghe iniziative già promosse dal CORECOM EMILIA-ROMAGNA, Nord Sud Ovest Web. Laboratori di educazione ai media tra e-book e blog, 2012 [www.assemblea.emr.it/corecom]; dal CORECOM MARCHE, "Adulti più informati, bambini più sicuri". Minori e New Media, tra opportunità e rischi, 2012 [www.ddpesaro.it/site/index.php?option=com\_content&view=article&id=298:8-maggio-internet-e-minori-adulti-piu-informati-bambini-piu-sicuri&catid=45:patto-formativo&Itemid=28] e dal CORECOM VENETO, Internet@Minori: navigazione sicura, 2007 [www.regione.veneto.it/corecom].

all'uso di alcool, di droghe o di armi, alla commissione di delitti; per non parlare dei siti e dei giochi online a contenuto osceno o violento, che insistono nella rappresentazione di crudeltà efferate sia verso esseri umani che verso animali, scegliendo a bella posta vittime che dovrebbero creare compassione: ragazze o bestiole indifese.

La legge italiana vieta la diffusione pubblica di scritti, disegni, immagini e rappresentazioni osceni, qualunque sia il mezzo usato<sup>34</sup>.

Dai messaggi di natura violenta o raccapricciante deve invece difendersi in prima persona il minore, al quale bisogna spiegare che si tratta di "porcherie" fatte apposta per suscitare disgusto o malessere.

## 2. Subire forme illecite di pubblicità

La pubblicità ci accompagna in tutti i siti che visitiamo, attraverso i banner o le finestre pop-up. Al riguardo bisogna considerare che i fornitori di servizi sono in grado di registrare i nostri gusti ed interessi, monitorando le attività che svolgiamo in Internet: si tratta del c.d. *profiling*, che serve a indirizzare a ciascun internauta una pubblicità mirata.

È facile pertanto che i ragazzi divengano destinatari di messaggi promozionali diretti specificamente a loro, messaggi che possono avere un contenuto ingannevole. Basta pensare ai molti prodotti e servizi che vengono offerti come gratuiti o addirittura presentati come premi (benché il vincitore non abbia partecipato a nessun concorso). Questa pubblicità può essere segnalata online all'Autorità garante della concorrenza del mercato<sup>35</sup>.

## 3. Compiere acquisti incauti

È bene diffidare delle offerte gratuite o dei premi, perché (se non conducono a violare il diritto d'autore)<sup>36</sup> spesso comportano l'adesione a un servizio in abbonamento che dovrà essere pagato, quando non mirano semplicemente a estorcere denaro.

Oltre tutto molti servizi offerti in Rete ai ragazzi possono essere pagati tramite telefonino, il che rende più facile l'acquisto d'impulso, senza la previa consultazione dei genitori.

La regola pertanto è che gli acquisti in Internet vanno fatti assieme ai genitori, che sono poi i responsabili degli impegni di spesa assunti dal minore, a meno che quest'ultimo non abbia occultato con raggiri la sua vera età<sup>37</sup>.

Pertanto, quando il sito, correttamente, limita la facoltà di acquisto ai maggiorenni, è assolutamente vietato spacciarsi per tali.

34 Art. 528 del Codice penale.

35 All'indirizzo <http://www.agcm.it/invia-segnalazione-online.html#wrapper>.

36 V. il par. 6 di questo capitolo, numero 4.

37 Art. 1426 del Codice civile.

Per evitare le trappole peggiori, come i giochi d'azzardo online, le carte di credito degli adulti non vanno lasciate a portata di mano dei ragazzi.

#### 4. Subire il “furto” dei propri dati personali o di quelli dei propri familiari

Diffuso nella Rete non è solo il tentativo di estorcere denaro, ma ancor più quello di ottenere i dati personali altrui.

Come è noto, la criminalità informatica si è specializzata nell'opera di carpire i nostri dati personali e le nostre password con appositi software, che senza saperlo scarichiamo aprendo e-mail o cliccando su determinate finestre. Queste informazioni rendono



possibile il **furto d'identità**, grazie al quale qualcuno potrebbe ad esempio stipulare un contratto telefonico o aprire un conto bancario a nostro nome e a nostre spese.

Esistono tuttavia anche sistemi apparentemente leciti per ottenere il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale. Ad esempio, in Internet capita spesso di poter ottenere servizi gratuiti, a condizione di comunicare i propri dati. Una volta verificato che questo non

comporti implicitamente un acquisto (caso trattato sopra), bisogna appurare se il sito contempla, sia pure a parte e scritta in piccolo, una descrizione dei tempi e dei modi della conservazione e dell'uso dei dati, nel rispetto delle condizioni imposte dalla legge<sup>38</sup>.

È necessario pertanto che la registrazione **nei siti avvenga con l'aiuto di un adulto**. Assolutamente da evitare è poi la comunicazione di dati propri o dei propri familiari quando questa è richiesta via e-mail: si tratta quasi sicuramente di phishing, ossia di ricerca di dati che qualche malintenzionato vuole usare a nostro danno.

La regola generale, del resto, è che non bisogna aprire le e-mail che provengono da indirizzi sconosciuti, né gli allegati che le accompagnano, perché possono contenere virus che una volta installati sul nostro computer lo danneggiano o memorizzano le nostre password.

<sup>38</sup> Si tratta del già ricordato D. Lgs. n. 196 del 2003, Codice per la protezione dei dati personali.

Attenzione: **una e-mail pericolosa può provenire persino dall'indirizzo di persone conosciute**. Anche i nostri amici possono subire un furto d'identità: qualcuno si impossessa della loro password e usa la loro posta elettronica per cercare di truffare tutte le persone contenute nell'indirizzario.

In questo caso è impossibile non aprire la e-mail. Prima di rispondere a richieste di soldi o di informazioni è meglio però verificarne l'autenticità parlando direttamente con l'interessato.

### III. 4. I rischi connessi alla socializzazione in rete

#### 1. Maturare forme di dipendenza patologica dalla Rete

È indispensabile far passare il principio che il tempo dedicato alla navigazione è limitato. Se è il senso di solitudine che spinge a esagerare, la soluzione va ricercata nello svolgimento di attività collettive.

Naturalmente gli adulti debbono dare il buon esempio!

#### 2. Subire l'adescamento da parte di estranei

A nessun bambino o ragazzo è permesso frequentare coetanei, e a maggior ragione adulti, dei quali i genitori non sanno nulla. Il problema è che grazie all'uso dei *nickname* e delle identità virtuali gli stessi ragazzi possono essere indotti in errore sull'età e sull'identità dei loro interlocutori.

Per prevenire la pedofilia e pedopornografia una apposita Convenzione internazionale, recepita dalla legge italiana<sup>39</sup>, ha ritenuto indispensabile punire specificamente il c.d. *grooming*, ossia la manipolazione psicologica attraverso la quale i minori che usano i nuovi media sono indotti a entrare in confidenza con adulti malintenzionati.

La legge italiana ha pertanto introdotto nel 2012 il delitto di adescamento di minorenni<sup>40</sup>, che si realizza mediante qualunque atto (artificio, lusinga o minaccia) volto a carpire la fiducia di un minore degli anni sedici, posto in essere mediante l'utilizzo della Rete internet o di qualsiasi altro mezzo di comunicazione.

Il colpevole non può addurre a propria scusa l'ignoranza dell'età della persona offesa, a meno che questa non fosse inevitabile<sup>41</sup>: **a scanso di equivoci, i minori non debbono mai fingersi maggiorenni.**

Quando si chatta, un ottimo sistema per scoraggiare i malintenzionati è quello di inserire nella conversazione frasi come: "c'è qui mia madre che vuole salutarti, ti va?" oppure "in questo momento sono davanti al computer con mio padre".

<sup>39</sup> Convenzione del Consiglio d'Europa per la protezione dei minori contro l'abuso e lo sfruttamento sessuale.

<sup>40</sup> Art. 609-undecies del Codice penale, introdotto dalla legge 1° ottobre 2012 n. 172.

<sup>41</sup> Art. 602-quater del Codice penale.



In caso di necessità ci si deve rivolgere alla Polizia postale; è bene inoltre segnalare il fatto ad una delle **hotline** che fanno capo all'associazione delle linee di emergenza INHOPE contro l'abuso e lo sfruttamento sessuale dei minori nella Rete, come *Stop-it* o *sicurinrete*.<sup>42</sup> Mai accettare appuntamenti offline da persone conosciute online!

### 3. Ricevere immagini pedopornografiche

La legge punisce altresì severamente chi diffonde a qualsiasi titolo pornografia minorile<sup>43</sup>, stabilendo, come si è detto, un obbligo di censura da parte dei fornitori dei servizi.

Per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

Per colmare le eventuali lacune del sistema è tuttavia essenziale non rispondere **mai a e-mail (o peggio all'invio di immagini) erotiche o volgari**. Nel caso, i ragazzi ne riferiranno immediatamente ai genitori, che debbono denunciare il fatto alla polizia.

### 4. Mettere in circolazione proprie immagini riservate

Un rapporto delle Autorità per la protezione dei dati personali segnala che l'uso di Internet ha apportato in materia una inaspettata difficoltà: i dati personali sono resi pubblici dagli stessi utenti, che lo considerano un comportamento innocuo. Inoltre i nativi digitali risultano avere meno problemi a rendere pubblici dettagli intimi della propria vita privata<sup>44</sup>.

In altre parole, l'uso integrato dei nuovi media (la facilità di parlare, fotografare, filmare e trasmettere il tutto in Rete) incentiva l'esibizionismo – che è caratteristico dei giovani e fa del resto parte della mentalità della nostra epoca – con conseguenze perniciose.

<sup>42</sup> Il sito [www.stop-it.org](http://www.stop-it.org) appartiene a Save the Children; il sito [www.sicurinrete.it](http://www.sicurinrete.it) fa capo a Adiconsum e Save the Children.

<sup>43</sup> Art. 600-ter del Codice penale.

<sup>44</sup> Vedi il Rapporto e linee-guida in materia di privacy nei *social network* (Memorandum di Roma) approvato dalla Conferenza internazionale delle 78 Autorità garanti tenutasi a Strasburgo nel 2008.

Ad esempio alle ragazze può accadere di prendere il sole in topless, al riparo da sguardi indiscreti, e magari di scattarsi qualche foto per ricordo. La cronaca racconta però di una dodicenne canadese che si è suicidata dopo che una foto del genere era finita in mano ad uno sconosciuto, il quale l'ha usata per ricattarla e per rovinarle la reputazione sul *social network* frequentato dai compagni di scuola.

Chi comunica le proprie immagini riservate, o rivela i propri segreti, rischia di attirare su di sé forme di maldicenza o di calunnia.

In alcuni casi, rischia persino un'imputazione per diffusione di immagini pedopornografiche<sup>45</sup>.

**Niente outing o esibizionismi inutili!**

### **5. Subire forme di cyber-bullismo o cyber-stalking da parte di coetanei**

Internet dà occasione a nuove forme di cattiveria, di ripicca e di vendetta, che possono sfociare in una vera e propria persecuzione. Si può trattare, come nella vita reale, di *insulti* o *minacce* che vengono inviati tramite e-mail o vengono pubblicati in un sito web.

Ci sono poi le molestie attuate sui *social network*: la *denigrazione* (come quella subita dalla dodicenne or ora ricordata); l'esclusione deliberata dalla cerchia degli amici; la *sostituzione di persona*, che si ha con l'apertura di un account non da parte del diretto interessato, ma dei suoi conoscenti, che lo usano per sbeffeggiarlo. Al riguardo va ricordato che gli insulti e le minacce costituiscono di per sé reato<sup>46</sup>. Tutti i comportamenti considerati, inoltre – se vengano ripetuti sino ad indurre un perdurante e grave stato di ansia o di paura, se non di timore per la propria incolumità, o sino ad indurre il cambiamento delle proprie abitudini di vita – vengono puniti come atti persecutori o *stalking*<sup>47</sup>.

**Il minore che subisce questi comportamenti senza reagire è destinato ad affrontare una escalation. Non deve pertanto esitare a riferirli alle Autorità o alla persona adulta con la quale è più in confidenza.**

Oltre a registrare con attenzione i possibili sintomi di sofferenza manifestati dai ragazzi, gli adulti dovrebbero controllare periodicamente che cosa gira in Rete sui figli o nipoti.

### **6. Rivelare informazioni che espongono a pericolo se stessi e la propria famiglia**

I dati personali non solo possono essere oggetto di furto, ma assieme ad altre informazioni (ad esempio l'indirizzo della scuola, i propri percorsi abituali) possono consentire a sconosciuti di seguire e incontrare i ragazzi. Inoltre il fatto di sapere che la famiglia è benestante o che possiede oggetti di valore (visibili nelle foto o nei video) e di sapere quando si assenta o va in vacanza è un utile ausilio per i ladri. La prima regola è abituarsi

<sup>45</sup>Vedi il par. 6, numero 3.

<sup>46</sup>Vedi ancora il par. 6, numero 2.

<sup>47</sup> Art. 612-bis del Codice penale.

ad usare un *nickname*, anziché il proprio nome e cognome. La seconda è di evitare di scendere nei dettagli, che sono essenziali quando si parla di emozioni e di sentimenti, ma non in altri campi. La terza è di usare con prudenza i sistemi di geo-localizzazione che sono in grado di rivelare a terzi la nostra posizione in tempo reale.

### **7. Mettere in Rete dettagli della propria vita che possono avere conseguenze negative sul futuro lavorativo**

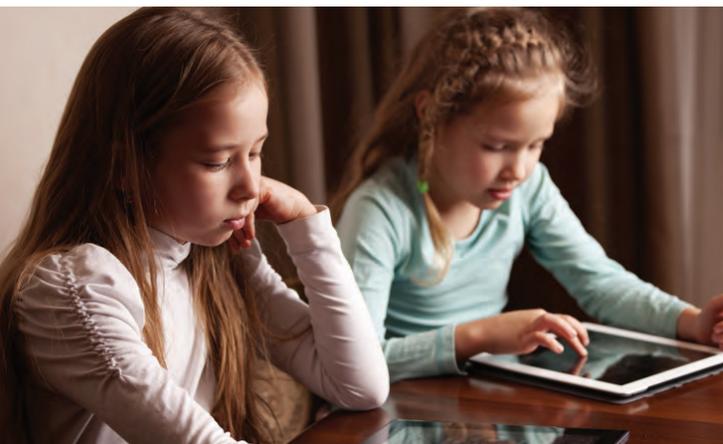
Come si è visto, Internet conserva tutto quanto viene pubblicato. Ed è provato che gran parte dei datori di lavoro dà un'occhiata nella Rete per trovare informazioni su coloro che richiedono un'occupazione.

Questo è un motivo in più per rispettare la propria privacy: niente bravate!

## **III. 5. I rischi connessi alla ricerca di informazioni in Rete**

### **1. Accedere ad informazioni o notizie false, incomplete, non aggiornate**

Al genuino bisogno di notizie e di informazioni la Rete non sempre è in grado di



rispondere adeguatamente.

Non è raro imbattersi in notizie del tutto inventate: nel caso migliore, si tratta delle c.d. leggende metropolitane; nel peggiore, di informazioni artatamente distorte, se non di revisionismi storici più o meno espliciti. Da non dimenticare è che la negazione dell'Olocausto può rappresentare una forma di incitamento all'odio razziale: per il nostro ordinamento è

un reato e il sito che lo pratica deve essere denunciato alle Autorità.

In generale, va censurata la tendenza a ritenere vera e affidabile qualsiasi informazione sia reperibile in Internet. Anche le enciclopedie online devono essere attentamente scrutinate: quelle redatte da istituti di ricerca noti sono più affidabili, ovviamente, di quelle affidate alla compilazione di autori volontari e anonimi.

**Al reperimento delle informazioni in Rete è dedicato il capitolo IV di questo *Vademecum*.**

### III.6. Il rischio che gli stessi minori commettano illeciti<sup>48</sup>

Al riguardo bisogna innanzitutto ricordare che sono **penalmente imputabili** coloro che hanno compiuto i quattordici anni, se al momento del fatto avevano la capacità di intendere e di volere (quest'ultima non attiene alla sanità di mente, ma alla maturità del soggetto)<sup>49</sup>.

La responsabilità civile per i danni causati a terzi si ripercuote invece sui genitori o su coloro che ne fanno le veci (e sui professori per il tempo in cui i minori sono sotto la loro vigilanza), a meno che non dimostrino di aver adottato tutte le cautele necessarie ad evitare il danno<sup>50</sup>.

In secondo luogo va ricordata la distinzione, già menzionata<sup>51</sup>, tra libertà di corrispondenza personale, che si esercita quando ci si rivolge in forma segreta e riservata a uno o più destinatari determinati, e libertà di manifestare il pensiero, con la quale si intende trasmettere un messaggio non a qualcuno in particolare, ma potenzialmente a tutti, ovvero lo si vuole rendere pubblico.

**Scegliendo un mezzo che dà pubblicità al messaggio si rischia infatti di rendere illeciti molti degli stessi contenuti che sarebbero invece leciti, se comunicati riservatamente.**

Certamente la e-mail, che equivale alla lettera sigillata, è lo strumento principe della libertà di corrispondenza, che fa assumere all'autore solo il rischio di offendere i destinatari del messaggio. Per converso, la libertà di manifestare il pensiero tipicamente si esercita utilizzando una pagina web visibile da chiunque sia connesso, o caricando un video su Youtube.

Vi sono tuttavia una quantità di situazioni che possono indurre in errore.

In primo luogo la stessa e-mail cessa di rappresentare una comunicazione riservata quando (come avviene nelle pratiche commerciali) viene usata per pubblicizzare un messaggio verso soggetti scelti poco più che casualmente.

In secondo luogo la discussione in un forum o un blog o in una chat non può considerarsi una forma di comunicazione riservata, dal momento che chiunque può partecipare semplicemente iscrivendosi, e chiunque quindi può venire a conoscenza dei messaggi scambiati. Il fatto che il gestore del forum o del blog possa opporsi all'iscrizione di qualcuno non fa venire meno la pubblicità.

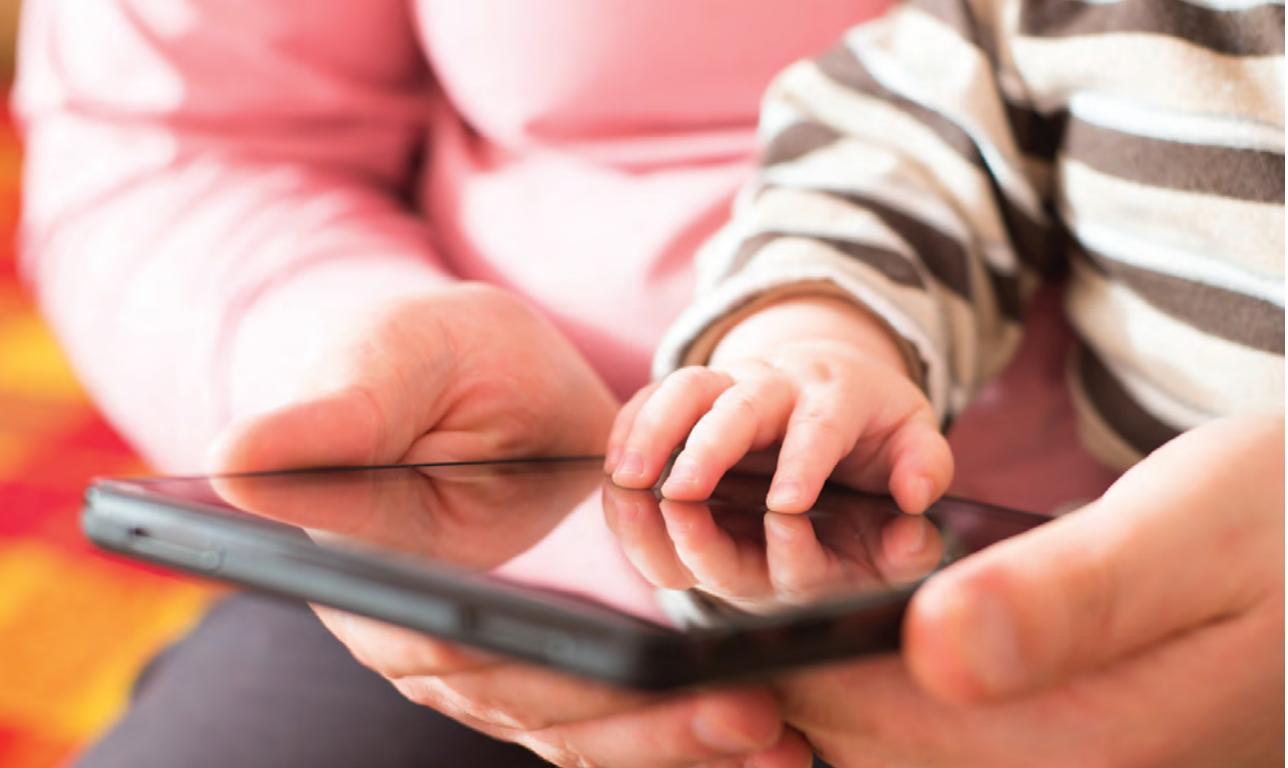
Lo stesso vale, come pure si è già ricordato, per le attività svolte nei *social network*.

48 Trattiamo qui i comportamenti che non sono già stati esaminati in precedenza dal punto di vista delle vittime (come il cyber-bullismo).

49 Art. 98 del Codice penale.

50 Art. 2048 del Codice civile.

51 Vedi il par. 2, al numero 5.



### **1. Violazioni della privacy altrui**

Secondo la legge, è vietato diffondere pubblicamente l'immagine o altri dati personali altrui senza il consenso dell'interessato (non lo è, invece, comunicare riservatamente tali dati a persone determinate nell'ambito di rapporti personali).

Si noti che il fatto di essere ritratti assieme ad un'altra persona in una foto non toglie che sia necessario informarne costei ed averne l'autorizzazione prima di diffondere la foto. Il trattamento illecito dei dati personali è punito con una sanzione amministrativa irrogata dal Garante per la privacy<sup>52</sup>.

### **2. Offese alla dignità e libertà altrui**

Dirigere insulti a qualcuno via e-mail o all'interno di un blog al quale la vittima partecipa integra il reato di ingiuria. Esprimere pubblicamente opinioni offensive nei confronti di un insegnante, o manifestare il proprio disprezzo verso un compagno di scuola dà luogo invece al più grave reato di diffamazione<sup>53</sup>.

Pure punito è il fatto di minacciare ad altri un danno ingiusto<sup>54</sup>.

### **3. Diffusione di pornografia minorile**

Come si è accennato, il comportamento di minori che riprendano e diffondano volontariamente i propri genitali o le proprie esperienze sessuali può essere

52 Art. 161 del D. Lgs. n. 196 del 2003, dedicato all'omessa o inidonea informativa all'interessato.

53 V. rispettivamente gli artt. 594 e 595 del Codice penale.

54 Art. 612 del Codice penale.

punito<sup>55</sup>. Il fatto che i rapporti sessuali tra ragazzi maggiori dei 14 anni sia lecito non significa, in altri termini, che sia anche lecito trarne immagini, detenerle, o peggio diffonderle.

#### **4. Violazioni del diritto d'autore**

Le difficoltà che gli ordinamenti incontrano, a livello mondiale, nella lotta alla pirateria informatica li induce talvolta a sparare nel mucchio, colpendo anche attività che potrebbero ricondursi ad un “uso corretto” delle opere protette dal diritto d'autore.

Giusto o ingiusto che sia, scaricare gratuitamente da Internet file musicali o video protetti può comportare una responsabilità penale e il pagamento di una sanzione amministrativa, così come può comportarle condividere tali file con gli amici, o mettere in Rete (caricandolo ad esempio su YouTube) un video che comprenda anche parzialmente un'opera protetta (un concerto, un quadro, eccetera)<sup>56</sup>.

Il fatto che talvolta non si sia in grado di stabilire se l'opera in questione è protetta, ovvero se il sito che consente di scaricarla (ad esempio Emule) sia un “sito pirata” rende ovviamente le cose più difficili.

È buona regola pertanto non approfittare di queste opportunità.

55 Art. 660-ter del Codice penale.

56 L'art. 171, lett. a) e a) bis, della legge sul diritto d'autore punisce con la multa da euro 51 a 2065 chi riproduce o diffonde e chi mette a disposizione del pubblico immettendola in un sistema di reti informatiche un'opera protetta o parte di essa. L'art. 174-bis commina poi una sanzione amministrativa pari al doppio del prezzo di mercato delle opere, in misura comunque non inferiore a euro 103.



## IV. I suggerimenti dell'esperto informatico ai minori e ai genitori

### IV. 1. La nota regola delle tre S: Sesso, Sangue, Soldi

La scienza dice che strutturalmente l'organismo umano è rimasto uguale a quello delle origini, quando si dormiva nelle caverne e si usava la clava, e quando il nucleo familiare e la sua consistenza rappresentavano la vera ricchezza.

Pochi individui, che hanno prodotto pensiero e filosofia, hanno contribuito a dare alla nostra razza una parvenza di evoluzione e distanza nei confronti del regno animale. In seguito, la "scoperta" dell'energia elettrica ha permesso quel balzo nella produzione di strumenti e capacità di modificare la nostra biosfera, al fine di renderla sempre più idonea a supportare **l'esigenza di utilizzare la mente in innumerevoli giochi sociali**. Tali "intrattenimenti" servono solo a darci l'impressione di fare qualcosa d'importante, mentre svolgiamo per la natura la medesima funzione che svolge un microorganismo o un albero: **trasformare ossigeno in anidride carbonica**.

Abbiamo poi anche deciso di rendere interconnesso e raggiungibile attraverso la Rete un mondo che ospita frammenti assai eterogenei di civiltà, favorendo il contatto tra elementi storici e culturali incompatibili tra loro, ed esaltando in tal modo l'espressione della differenza e dell'intolleranza, **ove la regola del più forte è anche, naturalmente, la più "giusta"**.

All'interno di questo grande calderone, che ospita ingredienti a dir poco inaccostabili, la nostra sindrome dell'entertainment e del divertimento di massa ha prodotto anche una stampa e un'editoria che funziona secondo **la nota regola delle tre S: sesso, sangue e soldi**. Pochi leggono o "cliccano" su prodotti raffinati della mente umana, e molti invece si gettano sugli scandali altrui, sul torbido, sul truculento, su tutto ciò insomma che alimenta il serbatoio di **quelle emozioni dense e oscure, che abbiamo imparato a scambiare per "vita", poiché ci fanno "sentire vivi"**. Cosa si può pretendere, allora, da una società che sforna prodotti editoriali e mediatici che sfruttano la paura, l'oscuro, il sangue, la violenza e la morte, per formare i nuovi esseri umani e mantenere quelli vecchi soddisfatti?

In questo contesto, si inserisce **quella che è stata definita erroneamente pedofilia**. Erroneamente, perché il termine, da un punto di vista etimologico, indica un sentimento positivo nei confronti dei cuccioli degli esseri umani, una spinta al loro benessere e alla loro protezione. Quello che ci troviamo ad affrontare, invece, è qualcosa di molto diverso, molto più simile all'oscurità e alla truculenta sindrome che s'impadronisce della nostra mente, tutte le volte che guardiamo un telegiornale o sfogliamo un quotidiano.

Quella che definiamo come pedofilia, in realtà potrebbe essere più correttamente nominata “**pedofobia**” o “**pedopatia**”, poiché proprio tra le patologie deve essere annoverata. Questa malattia della mente è la stessa che spinge un essere umano alla prevaricazione su un soggetto più debole, indifeso, ingenuo o innocente; quella che guida i bulli a malmenare e umiliare i compagni più piccoli, timidi e pacifici; la stessa che determina anche l’azione crudele di chi se la prende con gli animali domestici, torturandoli e uccidendoli a volte in modi atroci. Quella **sindrome che spinge alla violenza sessuale e al rapporto basato sulla prevaricazione**.

Naturalmente, questa linea di condotta denota personalità non solo disturbate, ma anche determinate a comportamenti contrari alla sopravvivenza stessa della specie, e quindi antisociali. **Sono persone dominate da uno spaventoso complesso d’inferiorità e dalla paura, che li spinge a riconoscere nella paura e nella sottomissione dell’altro la propria dimensione umana**. Ma non lasciamo che il riconoscimento della loro patologia ci confonda: questi individui sono pericolosi e, in quanto tali, non hanno alcun diritto di mescolarsi a un contesto sociale votato alla vita. Non avrebbero ugualmente alcun diritto di occupare le prime pagine dei quotidiani, o sezioni di spicco dei notiziari in prima serata, piuttosto che le note di ricerca di qualche scienziato interessato alla risoluzione di patologie.

Tuttavia, dato il contesto votato anche alla spettacolarizzazione delle disgrazie altrui, e di questo possiamo incolpare solo noi stessi, **può capitare che il tentativo di denuncia porti invece ad alimentare la sindrome stessa!** Come? Nell’identico modo in cui l’attenzione maniacale puntata dai media sui lanciatori di pietre dai cavalcavia delle autostrade ha portato all’aumento di questo fenomeno.

Tutti coloro che contengono in latenza i semi di una patologia tendono a tradurre la fantasia in azione, quando questa potrebbe dar loro una dimensione di fama e popolarità, e quindi di riconoscimento (il famoso “io esisto se ...”), anche per un solo istante. Il timore delle conseguenze diventa allora secondario, se non vero e proprio stimolo di adrenalina. Potremmo dire infatti che, proprio da quando questa patologia è salita agli onori della cronaca, **il suo diffondersi è aumentato vertiginosamente**, anche con l’aiuto propulsivo della rete, ma soprattutto, come abbiamo detto, con l’aiuto dei media, che sbattono elementi aberranti della razza umana sulle prime pagine, insieme ai grandi della Terra! Come ben sappiamo, infatti, non importa che se ne parli bene o male, ma che se ne parli. Questa sindrome del truculento ha fatto aumentare anche fenomeni collaterali, che dimostrano come il vero medioevo non sia mai terminato.

Spingendoci un poco più in là, diciamo che la spettacolarizzazione della “caccia alle streghe” porta con sé anche eventi tristi, ai quali tutti possiamo assistere ogni giorno. Parlo, ad esempio, dei genitori che seguono con il Gps il figlio quando esce da scuola,

e ne controllano ogni movimento. Non siamo più liberi di sorridere a un bimbo, senza che chi è presente alzi il sopracciglio, o che il genitore non reagisca in modo protettivo, alimentato dalla paura del “mostro” sempre in agguato.

Accadono anche fenomeni più inquietanti, che partono proprio dai bambini stessi, **protetti dal mondo esterno fisico, ma non mediatico**, e che quindi assorbono e interpretano a loro modo le notizie e gli allarmi lanciati dai media. Un giorno sono stato testimone di uno di questi episodi, su un mezzo pubblico. Una zia stava accompagnando la nipote a casa, e quest'ultima, guardando un negozio, le chiedeva di farla scendere, perché voleva vedere la vetrina. La signora disse alla bimba che non potevano fermarsi, perché la mamma le aspettava a casa. A questo punto, la bimba indispettita le disse: “se non mi fai scendere subito, chiamo la polizia e dico che mi fai le brutte cose!”. Ho osservato questa signora, che probabilmente per un miracolo non ha avuto un arresto cardiaco, mentre faceva scendere la bambina alla prima fermata, guardandosi intorno presa dalla vergogna, con decine di sguardi puntati su di lei.

Purtroppo, possono accadere anche queste cose, quando **si scambia una corretta informazione con la cultura della paura**. E mentre “informiamo” tutti, genitori e figli, dei pericoli del mondo, ci scordiamo magari che far rimbambire questi ultimi davanti a un PC, per emergere in un *social network*, o davanti a videogiochi che alimentano la sete di fama e violenza, può avere un solo effetto: gettare benzina sul fuoco.

#### **IV. 2. Autostima, riconoscimento sociale e sindrome dell'avatar**

Un'altra patologia che affligge buona parte della popolazione mondiale, soprattutto nei paesi del cosiddetto “primo mondo”, è quella della **mancanza di autostima, e della conseguente pulsione all'autoriconoscimento e autoaffermazione**, attraverso l'effetto generato sugli altri. Nei casi più estremi, il “male” viene compiuto esclusivamente per poter essere, anche per un solo istante, “visibili” a tutti.

Nel caso, invece, di persone normalissime, che non hanno alcun seme oscuro da coltivare nel loro giardino, ciò che ha prodotto la miscela esplosiva degli ultimi vent'anni è **il libero accesso e utilizzo di ogni tipo di servizio online, in assenza di un sistema educativo adeguato e anche di una struttura regolatoria**, che ponga limiti e penalità a coloro che usufruiscono di tali servizi come fossero dei giocattoli.

Molti esperti di tutto il mondo hanno già tentato di esplorare le mutazioni cognitive e comportamentali derivate dall'esposizione dell'homo sapiens al sistema globalizzante introdotto da Internet e, soprattutto, dalle innumerevoli nuove facoltà che mette a disposizione. Una su tutte, forse la più abusata e pericolosa, è quella che qui battezziamo come “sindrome dell'avatar”, ovvero la progressiva virtualizzazione degli attributi della

personalità, all'interno di un contenitore artificiale, idealizzato e liberato nella rete. In un mondo ideale, pieno di esseri umani illuminati e consapevoli, questo potere che ci conferisce Internet, amplificherebbe smisuratamente le nostre facoltà, rendendoci partecipi contemporaneamente di ogni evento, elemento di conoscenza e azione, ovunque questa accada sul nostro pianeta, annullando i vincoli dello spazio e del tempo. Tuttavia, purtroppo non viviamo in un mondo ideale. Quando esploriamo un nuovo territorio, lo percepiamo solo in base ai bisogni più grossolani ed egoistici, e questo fa sì che diventi uno spazio popolato e dominato dall'espressione dei vizi, desideri e fantasie, che hanno una natura prevalentemente oscura e densa.

**Il primo tra tutti i peccati capitali che proiettiamo nella rete è l'accidia, ovvero l'espressione più estrema dell'inerzia della mente.** Ciò vuol dire che basta scrivere e diffondere qualcosa sulla rete che diventa vera, ripresa e condivisa da altri, il cui unico scopo è affannarsi a diffondere ciò che più riflette un'illusione personalissima. Troviamo in questo modo amplificato il fenomeno del complottismo, del razzismo, della violenza e perfino della violenta antiviolenza. **Tutti i fenomeni di protesta, che un tempo venivano vissuti in prima persona, mettendosi in gioco, ora vengono invece trasferiti nel sistema dei social network,** richiedendo solo un "mi piace" per credersi partecipi e sentire di aver fatto la propria parte.

**Tra i poteri della rete più abusati, c'è quello della notorietà.** Gratuitamente, possiamo costruire profili, nei quali possiamo "dire la nostra", mostrarci ed essere riconosciuti, indipendentemente dallo star system di ogni paese. **Abbiamo finalmente la possibilità di diventare "famosi" per virtù o infamia, poco importa.** Così, di fianco al blogger in zona di guerra, che racconta al mondo la storia del proprio paese, troviamo gruppi di esaltati psicopatici che inneggiano al massacro di animali domestici e che, paradossalmente, ricevono molti più "mi piace" e "commenti", di quanti ne ricevano filosofi e ricercatori, il cui lavoro può cambiare il volto della nostra civiltà. Peggio ancora, vediamo i componenti di intere famiglie, nessuno escluso, che svelano se stessi raccontando la propria intimità fatta di azioni e spostamenti, rendendo pubblici e mettendo quindi a disposizione foto e filmati. Tutto questo, con il solo intento di esistere, almeno nella rete, senza minimamente preoccuparsi che quella vetrina così ordinata è la stessa utilizzata dai cosiddetti orchi, stalkers, molestatori, psicopatici, pedofili, maniaci, ladri d'appartamento, e quant'altro ci si possa immaginare.

Nel mondo reale, però, si può dire a un bambino di non parlare con gli sconosciuti, e di mantenere un comportamento sobrio in pubblico. Nella rete, invece, non è più possibile. Telefonini e macchine fotografiche ad alta definizione, che scaricano direttamente il materiale sulla piattaforma del social network di riferimento, fanno sì che **ogni capriccio del momento venga indelebilmente registrato sul web, e reso disponibile a chiunque.**

**La totale mancanza di controllo sulle identità e i veri attributi di un utente nella rete,** ci dà la possibilità di costruire delle personalità fittizie, attraverso il sistema dell'avatar, grazie al quale pensiamo di esprimere le nostre più intime e profonde tendenze e fantasie in totale sicurezza, avendo la sensazione di essere liberi e non giudicati, ma soprattutto senza alcuna percezione delle conseguenze. Questo stesso potere, tuttavia, viene utilizzato da coloro che vedono in Internet la grande opportunità di soddisfare le proprie tendenze patologiche. Nel mondo reale, infatti, nessun pedofilo o pedopatico potrebbe mai travestirsi da bambino o bambina; nella rete, invece, lo può fare, e può diventare chiunque, con la possibilità di giocare su più tavoli, selezionando le proprie vittime con precisione e, soprattutto, in sicurezza.

### **IV. 3. Breviario per naviganti giovani o di lungo corso**

1. **Accettate contatti solo da persone che si conoscono,** o la cui identità e informazioni anagrafiche sono vere e accertate.

2. Ricordiamoci che **rendere visibili i nostri contatti e/o le nostre amicizie su un social network potrebbe consentire di arrivare a noi,** attraverso uno di loro. È l'anello più debole, infatti, che determina la solidità o meno di un sistema. Le impostazioni di configurazione di un profilo su queste piattaforme consentono solitamente di rendere "non visibili" i nostri contatti.



3. Prima di pubblicare commenti, notizie e quant'altro ci passi per la testa, prendetevi un minuto per pensare all'effetto che quanto state per dire potrebbe avere su chi legge, anche nel futuro. **Mai pubblicare provocazioni, né accettare o rispondere a commenti o "post" provocatori.** Se questi vengono pubblicati da altri sul vostro profilo, cancellateli, invece di rispondere. Una delle regole auree delle arti marziali, quando si è attaccati, è quella di "creare il vuoto", in modo che non esista un bersaglio da colpire.

4. **Non costruite profili pubblici visibili a tutti.** I *social network*, come Facebook, consentono di definire chi sono gli utenti che possono vedere il nostro profilo, e ciò che scriviamo. Utilizzate le impostazioni di configurazione, per limitare solo ai vostri amici virtuali la visione di ciò che scrivete.



5. **Pubbligate solo immagini o altro materiale multimediale di natura sobria**, che non possa attirare attenzioni moleste, o essere penalizzante per voi nel futuro. Ricordate che, una volta pubblicati foto o video, questi diventano di fatto proprietà del *social network*. Utilizzate sempre, quindi, le impostazioni di configurazione per rendere visibili le vostre foto, di qualunque natura esse siano, solo a chi conoscete bene.

6. Una delle piaghe dei *social network* è il cosiddetto “tag”. Anche nel caso voi esercitate ogni precauzione sul vostro profilo, arriva sempre qualcuno che vi tagga in una foto o filmato, rovinando tutto. **Cancellate, dunque, tutti i tag riferiti a voi, e chiedete ai vostri “amici” di non includervi in essi.** Se possibile, inoltre, usate le configurazioni del profilo per inibire questa azione. Ricordate, infine, che una foto è di proprietà del fotografo e non del soggetto, anche se il soggetto siete voi!

7. **Utilizzate i sistemi di instant messaging, come le chat, solo con persone che si conoscono.** L'azione migliore, salvo naturalmente le necessità del momento, è quella di disattivare l'opzione di mostrare ad altri utenti che siete in linea.

8. **Non pubblicate notizie o commenti che potrebbero svelare le vostre intimità a un buon profiler.** Se proprio sentite l'esigenza di rivelare ciò che pensate o provate in

un determinato momento, opinioni personali e quant'altro, fatelo in privato con chi conoscete veramente.

**9. Non comunicate la vostra posizione geografica, o l'intenzione di partire per le vacanze o nel weekend.** I *social network* consentono, a questo proposito, attraverso un'opzione del profilo, di inibire la pubblicazione automatica della localizzazione. Ricordate, però, che la piattaforma di social, e chi ci lavora, sa sempre perfettamente da dove vi collegate.

**10. Non rendete mai pubblica la vostra intenzione di essere in un determinato luogo, a una determinata ora** (e.g. uscire con gli amici, cene, pranzi, aperitivi, eccetera). Soprattutto, non taggate altri in tali esternazioni, e impostate le configurazioni per impedire ai vostri contatti di taggarvi in eventi sociali. Se qualcuno vuole raggiungervi con cattive intenzioni, può farlo anche attraverso chi frequentate.

**11. Non create mai un profilo falso su un *social network*,** illudendovi che vi renda immuni da eventuali conseguenze. Segnalate, anzi, al centro assistenza della piattaforma, tutti i profili che non corrispondono a nomi e cognomi plausibili, bloccandoli attraverso l'apposita funzione.

12. Diffidate, infine, da chi agisce contrariamente a quanto suggerito fin qui.

#### **IV. 4. La solitudine**

Il grande male di sempre, che da sempre esige soluzione, è la solitudine. Sentirsi soli in mezzo agli altri, con la paura del giudizio, della presa in giro, dell'umiliazione, dell'essere "nessuno" in mezzo agli amici. Di non essere ascoltati e, ovviamente, compresi dal gruppo. **Piccoli e grandi complessi, che affliggono ognuno di noi, trovano nella rete una possibilità di riscatto.** Lì, infatti, possiamo mentire e affermare di essere e poter fare tante cose, prendendo in giro tutti e, alla fine, anche noi stessi. Come per la legge del contrappasso, ci dimentichiamo, però, che tutti gli altri, quelli che cercano il contatto con noi, lo fanno più o meno spinti dallo stesso bisogno.

È difficile essere falsi o poco veri, e poi aspettarsi invece cristallina onestà e chiarezza da tutti coloro che sono collegati con noi, e con i quali scambiamo i nostri segreti e le nostre intimità. Il nostro livello di attenzione, allora, cade, e vige il principio secondo cui se tu accetti una cosa che dico di me, io ne accetto una che tu dici di te! Così facendo, **intratteniamo rapporti che si trasformano in pura fiction, scambiandoli per veri,**

poiché questa è la condizione posta all'altrui accettazione delle nostre proiezioni. Quante persone ho sentito lamentarsi della falsità, dell'ipocrisia e della mania di protagonismo in rete, quando poi, dando un breve sguardo al loro profilo, era evidente la medesima sindrome. Qualcuno ha detto che noi siamo la media delle cinque persone con cui abbiamo maggiori contatti. Per chi vive prevalentemente sui *social network*, provate a fermarvi un istante a pensare di chi siete la media!

Naturalmente, quanto sopra è ancora più amplificato dal senso di identità in evoluzione di un bambino o di un adolescente, con la differenza che un bambino e un adolescente hanno un sistema di governo degli impulsi ancora acerbo e sconvolto dalle mutazioni sistemiche e tempeste biochimiche della crescita. Un adulto, che dovrebbe invece avere cognizione di causa e capacità d'intendere e di volere, è invece sconvolto dalla percezione di aridità emotiva in assenza di stimoli forti e densi, e da quella sensazione di vuoto, di mancanza, che non riesce mai veramente a colmare. È difficile, dunque, per l'adulto, non proiettare sul proprio cucciolo il suo personalissimo bisogno, consentendogli e, spesso, anche incoraggiandolo ad avere tutti quei balocchi che possiedono gli amici, senza cui potrebbe entrare in una condizione d'inferiorità. Una volta acquisiti gli strumenti, è ancora più difficile porre dei limiti al loro utilizzo, per destinarli, ad esempio, solo ad attività costruttive o alla necessità di comunicare con la famiglia.

Eppure, se non siamo in grado di fare questo, di trovare cioè un'altra soluzione alle sindromi sopra descritte e, soprattutto, all'invadente presenza della solitudine, stiamo dando ai nostri figli gli strumenti che potrebbero determinare il loro deterioramento psicologico e cognitivo, aiutandoli a sviluppare un senso d'identità falso e deviato, che scandirà il loro futuro. Genereremo adulti che sono solo mezzi uomini e mezze donne, con un sistema immunitario debole o inesistente, tale da renderli appetitosi bocconcini per i predatori della rete, sempre che non lo diventino loro stessi! Chiediamoci una volta in più, se è questo il destino che auguriamo loro...

#### IV. 5. Alcune dritte per una tecnologia consapevole

Alcuni consigli per gli utenti adulti, al fine di interagire in modo consapevole ed efficace con la tecnologia, in presenza dei figli, soprattutto se si tratta di minori.

1. Diamo a noi stessi un tempo, **al massimo due ore al giorno, per l'accesso alla rete e ai *social network*.**

2. **Impediamo ai figli l'accesso al nostro personal computer.** Possiamo naturalmente proteggerlo con una password all'accensione del computer stesso, oppure impostare la nostra



password utente, soluzione che può essere, però, aggirata facilmente da chi sa “smanettare” un po’. Possiamo, inoltre, creare un utente con regole di configurazione per l’accesso al nostro profilo sul pc, e attivare la crittografia su Windows. Ricordatevi, a questo proposito, che i computer hanno sempre un utente “amministratore” già configurato, che normalmente non è detentore di password, e chi sa “smanettare” lo sa. Conviene sempre, quindi, leggere il manuale d’istruzione del sistema operativo, identificando questo utente e impostando una password complessa, per impedire a chiunque di superare le misure di sicurezza.

3. **Acquistate e utilizzate di fronte ai figli solo sistemi multimediali educativi**, anche nel caso di videogiochi. Dovrebbero avere la funzione di stimolare la mente e l’intelligenza, invece di riempire eventuali vuoti di stimoli emotivi, o assecondare e alimentare tendenze deviate.

4. Consentite ai figli **l’uso di Internet, solo per fini educativi o di ricerca**.

5. Consentite ai figli **solo l’utilizzo di sistemi mobili per le funzioni di chiamata ed sms**. Evitate di affidare loro smartphone o tablet, perché poi diventa impossibile controllare l’uso che di tali dispositivi viene fatto.



## V. DAL GIORNALE DI CARTA ALLE NOTIZIE SUL WEB: VANISHING NEWSPAPER E INFORMAZIONE ONLINE<sup>57</sup>\*

### V.1. La sfida alla carta stampata

Nel passaggio tra i due millenni si è verificata una **progressiva diffusione dell'informazione attraverso la Rete Web**, destinata a trasformarsi in una vera e propria sfida ai giornali stampati. Come tanti secoli prima era avvenuto per l'invenzione della stampa, all'inizio non fu ben chiaro che Internet potesse non solo sostituire i libri e i periodici cartacei, ma addirittura ampliare pressoché all'infinito la circolazione delle conoscenze, dei dati, di ogni riferimento agli eventi passati e presenti - e quindi anche delle informazioni.



Col tempo, il rapido aumento di notizie che ci raggiungono in continuazione ha tuttavia causato una pesante diminuzione nelle vendite dei giornali stampati.

Questo fatto non può non destare preoccupazione, perché **scegliere e pagare il proprio giornale rappresenta un gesto di libertà**: questo gesto ha costituito uno degli elementi più importanti del

modo in cui si è formata l'opinione pubblica nei diversi Stati almeno a partire dall'800. Il lettore che sceglie il proprio giornale gli riconosce l'**autorevolezza dovuta alla presenza di giornalisti e commentatori impegnati nel loro lavoro in modo professionale**. Giornalisti cioè che verificano le notizie, danno loro l'adeguata priorità (valorizzando le più importanti della giornata, a fronte delle migliaia che ci arrivano indiscriminatamente dalla Rete), usano in modo appropriato le fonti d'informazione. Nonostante le tante polemiche che pur pesano sul giornalismo - soprattutto in Italia - i giornali stampati, fedeli al loro marchio di origine, sono da sempre impegnati (almeno per principio) a fornire un'informazione vera e attendibile.

Ben diverso, e sostanzialmente **meno libero**, è invece il gesto di *clickare* su un sito, un motore di ricerca, un blog e **cercare informazioni senza che spesso siamo consapevoli da chi provengano, se siano vere, se siano davvero importanti**.

57 Donatella Cherubini "The Vanishing Newspaper". Il giornalismo italiano di fronte alla crisi della carta stampata".

## V.2. Dall'informazione alla totale interattività: motori di ricerca, blog, social network e citizen journalism

**Vuoi sapere cosa è successo oggi? Accendi il computer e hai infiniti modi per informarti.** Nell'arco di poco più di un ventennio la Rete ha prodotto migliaia di fonti d'informazione, di fronte alle quali è necessario cogliere le diverse caratteristiche e motivazioni che le animano.

In primo luogo si sono moltiplicati i **motori di ricerca**: oltre a svolgere il proprio compito primario di consentire l'accesso a tutti i dati reperibili sul Web, si sono trasformati in **sostituti dei giornali** attraverso strisce rotative con le notizie continuamente aggiornate, ma anche con veri e propri articoli corredati di foto e link (collegamenti) multimediali.

**Non sempre però è chiara l'effettiva priorità delle notizie**, con il loro rapido accavallarsi e soprattutto con il diffondersi dei colonnini che riportano quelle più cliccate, offrendo un quadro della realtà in corso **quale viene decisa dalla curiosità dei "naviganti"** e non tanto dalla effettiva rilevanza di quanto è accaduto.

Contemporaneamente si è avuta l'evoluzione di alcuni **blog**: nati come espressione di singoli individui o gruppi ristretti accomunati da idee, passioni, obiettivi comuni, sono diventati **essi stessi fornitori di informazioni e notizie**, aperti all'intervento dei lettori e dunque prototipi di quella interattività che ormai è uno dei fattori caratterizzanti della Rete.

A ciò si sono aggiunte tutte le forme di **citizen journalism**, ovvero siti e periodici online dove sono gli stessi lettori a intervenire, correggere, integrare, commentare le notizie in modo anche diverso da quello del giornalismo professionista.



**Tutte queste fonti di informazione possono aprire discussioni e stimolare commenti su notizie non sempre vere o verificabili, talvolta sconfinando in veri e propri illeciti.**

L'esempio più noto è quello di **Wikileaks**, organizzazione internazionale con uno staff per lo più anonimo, che carica sul proprio sito web documenti coperti da segreto (segreto di stato, segreto militare, segreto industriale, segreto bancario)<sup>58</sup>. Sebbene lo scopo dichiarato fosse quello di favorire la "trasparenza da parte dei governi quale garanzia di giustizia, di etica e di una più forte democrazia", la sua attività ha scatenato vaste polemiche e provvedimenti delle autorità internazionali, soprattutto per l'ambiguo e spregiudicato comportamento del suo portavoce Julian Assange, ma anche per il reperimento di informazioni attraverso l'operato di **hackers**.<sup>59</sup>

58 Cfr. [www. http://it.wikipedia.org/wiki/WikiLeaks](http://it.wikipedia.org/wiki/WikiLeaks)

59 Hacker è chiamato "chi commette atti di pirateria informatica, intervenendo su memorie a cui non ha accesso legale per sottrarre o alterare dati" (GRANDE DIZIONARIO HOEPLI, Italiano, ad vocem).



Informarsi in Rete deve dunque essere un atto consapevole, innanzitutto verificando i siti da cui raccogliamo le notizie.

### V.3. L'evoluzione del quotidiano: versione cartacea, online, mobile e su tablet

D'altro lato va tenuto presente che proprio con un'attenta verifica **possiamo trovare eccellenti e importanti esempi di informazione**, commento, obiettività e chiarezza, grazie ai quali riusciamo anche a comprendere e valutare meglio quanto conosciamo attraverso la carta stampata e la televisione.

**Ormai tutti i quotidiani hanno una propria redazione online:** dalle testate internazionali, come il *New York Times* e il *Washington Post*, ai giornali italiani nati come "regionali" ma ampiamente diffusi in tutto il paese o in una gran parte di esso come la *Stampa* o il *Mattino*; a quelli regionali come la *Nazione* o il *Tirreno*; a quelli più strettamente locali e provinciali come il *Corriere di Siena* e il *Corriere di Maremma*.

Per i lettori/naviganti ciò rappresenta la **continuità del marchio**, dell'autorevolezza, o comunque della riconoscibilità di un quotidiano che nella versione cartacea era letto in famiglia da generazioni, o che, nei casi di testate più recenti, viene percepito come strettamente collegato al proprio territorio.

Il rapido perfezionamento dei telefoni cellulari ormai diventati estremamente "intelligenti" (smartphone) ha inoltre portato alla nascita delle **versioni mobile dei principali giornali cartacei**, che oggi sono disponibili per lo più con una registrazione (cioè con un pagamento che contribuisce ai costi del giornale cartaceo).



Un ultimo – e forse **definitivo** – passaggio nell’evoluzione del giornale cartaceo è infine rappresentato dalla sua versione su **tablet**, dispositivo senza tastiera della categoria touch screen, che per struttura e funzionalità costituisce sostanzialmente una via di mezzo tra un telefono cellulare evoluto e un computer portatile<sup>60</sup>.

Questi cambiamenti hanno consentito ai giornali tradizionali di mantenere viva la propria voce nel nuovo contesto della multimedialità.

In effetti, secondo uno studio della Federazione nazionale degli editori (Fieg), tra il 2009 e il 2012 **il numero dei lettori dei quotidiani tradizionali è in costante aumento, però ormai in riferimento alla versione online**. Si tratta di un vero e proprio boom dei lettori di quotidiani sul Web: “Dal 2009 al 2011, il numero degli utenti di siti delle testate, in un giorno medio, è cresciuto del 50%, passando da 4 a 6 milioni di individui”<sup>61</sup>.

Diversa è, però, la questione relativa **all’influenza che i giornali tradizionali (in qualunque versione si presentino) riescono ancora ad avere sull’opinione pubblica**. Si può infatti ritenere che **le generazioni adulte** – da sempre abituate a comprare o almeno a leggere qualche volta i giornali cartacei – siano tendenzialmente consapevoli

<sup>60</sup> Il primo esemplare fu inventato da Steve Jobs della Apple con il nome di iPad.

<sup>61</sup> La stampa in Italia (2009-2011), Roma, Centro studi della Federazione Italiana Editori Giornali, 2012.



delle differenze tra le varie testate. Al contrario **i più giovani**, nel complesso, si informano ricorrendo a quella Rete di cui sono esperti utilizzatori, rischiando di confondere le manifestazioni del giornalismo professionale con quelle più o meno improvvisate e inattendibili. Per questo motivo è indispensabile che ci siano **adulti capaci di trasmettere ai nipoti, ai figli, ai minori in generale, l'abitudine a conoscere e riconoscere la fonte che si utilizza.**

#### V.4. Avviso ai naviganti in cerca di "vere" notizie

La consapevolezza delle fonti d'informazione sarà una garanzia per diventare **cittadini davvero liberi di fronte al "bombardamento" indiscriminato di notizie.**

È il filosofo e sociologo Zygmunt Bauman a metterci in guardia dall'eccesso di fonti d'informazione che ci circondano, **dandoci l'illusione di essere informati** su tutto e, in sostanza, rendendoci sempre meno informati<sup>62</sup>.

Anziché cercare sempre nuove notizie diffuse in modo superficiale dovremmo porre attenzione alla **priorità** delle notizie, all'**analisi critica** degli avvenimenti, al loro **inserimento** nel **contesto** adeguato, al **commento** e all'**approfondimento**.

62 Cfr. Z. Bauman, Il buio del postmoderno, Prefazione di C. Bordoni, Reggio Emilia, Aliberti Editore, 2011;



## GLOSSARIO

*Internet offre molteplici servizi resi disponibili con varie modalità; quelli che verranno citati di seguito si distinguono per l'elevata potenzialità di esporre i minori ai rischi analizzati nel presente Vademecum.*

*La "v" puntata tra parentesi – (v.) – significa "vedi" e segnala che la parola, o l'espressione, immediatamente precedente è definita in un'apposita voce del Glossario.*

### **Blog**

È un vero e proprio diario in rete (il termine è infatti una contrazione dell'inglese "web log") realizzato in appositi siti internet nei quali uno o più soggetti gestori del sito (i c.d. bloggers) pubblicano e condividono con gli utenti che vi accedono, opinioni, informazioni e contenuti multimediali che vengono visualizzati in ordine cronologico.

### **Chat-room**

Si tratta di spazi virtuali (che si differenziano per contenuti tematici o per lingua usata dagli utenti) nei quali si svolge un dialogo (in inglese "chat") realizzato tramite internet. I servizi di chat consentono di mettere in contatto, mediante una apposita finestra di conversazione, due o più soggetti sconosciuti i quali qualificandosi attraverso c.d. nickname (ovvero in forma anonima) possono scambiarsi messaggi scritti in tempo reale, condividere immagini ma anche contenuti audio/video. Tra i più utilizzati si ricordano: Google talk, AOL Instant Messenger, Windows Live Messenger.

### **E-commerce e aste online**

Sono servizi che consentono di comprare e vendere prodotti via internet tramite negozi virtuali presenti in appositi siti web. Tra gli esempi più famosi si possono citare, rispettivamente, Amazon ed eBay.

### **Email**

È un servizio di posta elettronica via web mediante il quale l'utente può inviare e ricevere messaggi (e relativi files allegati) utilizzando un pc o un altro dispositivo elettronico (ad esempio un cellulare) connesso a internet.

### **File-sharing**

È un servizio di condivisione di file realizzato su internet attraverso appositi programmi, da installare sul proprio pc, i quali consentono di mettere in rete più computer che possono scambiarsi, in modalità peer to peer/P2P (v.), dati di qualsiasi natura. Uno tra i più famosi sistemi di *file-sharing* è senz'altro eMule.

## Forum

È un tipico strumento utilizzato online (assieme alle chat-room) per la creazione di comunità di discussione su temi specifici. Si tratta, in particolare, di uno spazio virtuale collocato all'interno di un sito internet (in una apposita pagina web) nel quale gli utenti si confrontano su argomenti concordati al momento della creazione del forum stesso. Come per le chat-room, anche in questo caso il servizio consente di mettere in contatto più soggetti sconosciuti i quali, qualificandosi attraverso nickname, interagiscono scambiandosi messaggi in una sorta di bacheca virtuale; a differenza delle chat, tuttavia, le comunicazioni non avvengono in tempo reale ma in modalità asincrona (la scrittura del messaggio e la relativa risposta, cioè, avviene in tempi diversi). Non sempre è necessaria una registrazione per partecipare ai forum; alcuni di essi prevedono tuttavia la presenza di un moderatore capace di escludere chi invia messaggi fuori tema, aggressivi o volgari.

## Giochi in Rete

Si tratta di servizi online che sfruttano diverse piattaforme (ad esempio siti web, console) per connettere più utenti sconosciuti che interagiscono tra loro sfidandosi in specifici giochi. Alla possibilità di giocare viene spesso associata quella di dialogare in apposite chat-room. Una particolare categoria di giochi in Rete è rappresentata dai MUVE (*Multi User Virtual Environment*) che consistono in simulazioni di ambienti reali, accessibili via internet e creati digitalmente in 3D, nei quali possono interagire più utenti contemporaneamente attraverso avatar grafici (che letteralmente abitano tali ambienti e sviluppano al loro interno una vita propria del tutto simile a quella reale) sfruttando tutte le funzionalità che caratterizzano i *social network*. Tra i mondi virtuali il più famoso è senza dubbio *Second Life*.

## Instant messaging

È un servizio per chat che consente di definire una lista di utenti i quali vengono avvertiti non appena uno di essi si connette alla Rete in modo da poter comunicare tra di loro in tempo reale (ad esempio scambiandosi messaggi di testo o immagini) tramite apposite chat-room (v.). Recentemente questi servizi sono stati resi disponibili anche per gli smartphone (tra le applicazioni più famose, si ricorda WhatsApp).

## Motori di ricerca

Sono servizi forniti attraverso appositi siti web che consentono di effettuare ricerche e recuperare ogni tipo di informazione (documenti, filmati, audio, immagini e così via) su internet, in base a una parola chiave inserita dall'utente. Tra i numerosi motori di ricerca attivi sul web il più utilizzato, a livello mondiale, è Google.

## **Peer to peer/P2P**

Si tratta di una modalità di comunicazione via Internet, utilizzata per lo scambio di file, nella quale due o più computer sono connessi direttamente (fungendo sia da pc cliente sia da pc servente), tramite un apposito programma di file-sharing (v.), senza che vi sia un server centrale. Tale sistema consente agli utenti di collegarsi l'un l'altro e accedere alle risorse che ognuno di essi ha posto in condivisione.

## **Social network**

Rappresentano una delle forme più evolute di servizi di comunicazione esistenti su Internet in quanto inglobano tutte le funzionalità delle chat, dei forum e dei blog aggiungendone ulteriori come, ad esempio, quella di creare un profilo personale pubblico (al quale possono essere associate foto, indirizzi email, preferenze etc.) che consente la rintracciabilità dell'utente da parte di altri utenti con cui, previa registrazione al servizio, è possibile condividere in tempo reale ogni tipologia informazione fruibile online (dai contenuti testuali, alle immagini, ai video, ai files audio, fino alle proprie preferenze su prodotti commerciali). Tra i più famosi *social network* si ricordano: Facebook, Twitter, Myspace.

## **Streaming**

Si tratta di un sistema di trasmissione continua e progressiva di flussi di dati audio/video trasferiti, via internet, da un server al pc dell'utente che li decodifica utilizzando appositi software quali ad esempio Windows Media Player, Quick Time o Adobe Flash Video.

## **Video-sharing**

È un particolare servizio di condivisione di files video che, attraverso appositi siti web, consente agli utenti di visionare in modalità streaming (v.) e caricare online filmati. Tra i più famosi si ricordano: YouTube, Google Video, Yahoo!Video.

## **Voip**

Si tratta di servizi che permettono di effettuare telefonate via internet, in modalità audio e video (qualora si disponga di una webcam), ma anche, a seconda della piattaforma utilizzata, di inviare sms e svolgere tutte le attività tipiche delle chat. Il più famoso sistema Voip gratuito è Skype.

## **Web TV**

È il servizio di televisione fruito tramite internet in modalità streaming (v.).

## HELP DESK

### LINK WEB

- <http://www.poliziadistato.it/articolo/982>
- <http://www.poliziadistato.it/articolo/1106>
- <http://www.poliziadistato.it/articolo/10309>
- <http://www.carabinieri.it/Internet/Cittadino/Consigli/Tematici/Internet>
- <http://www.interno.gov.it/mininterno/export/sites/default/it/temi/minori/sottotema002.html>
- <http://www.garanteprivacy.it>

### DENUNCE E SEGNALAZIONI

- <http://www.commissariatodips.it>
- <http://www.114.it>

### RECAPITI UTILI

#### CO.RE.COM TOSCANA

Via de' Pucci, 4 - 50122 Firenze

tel. 055.2387880 - fax. 055.2387871

Email: [corecom@consiglio.regione.toscana.it](mailto:corecom@consiglio.regione.toscana.it)

<http://www.corecom.toscana.it>

#### AGCOM - AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI

Sede principale di Napoli

Centro Direzionale, Isola B5 - 80143 Napoli

tel. 081.7507111 - fax 081.7507616

Sede secondaria operativa di Roma

Via Isonzo 21/b, 00198 Roma

tel. 06.69644111 - fax. 06.69644926

<http://www.agcom.it>

**GARANTE PER L'INFANZIA  
E L'ADOLESCENZA DELLA REGIONE TOSCANA**

Via Cavour, 4 - 50129 Firenze

tel. 055.2387563

Email: [garante.infanzia@consiglio.regione.toscana.it](mailto:garante.infanzia@consiglio.regione.toscana.it)

**COMPARTIMENTO POLIZIA POSTALE TOSCANA**

Via della Casella, 19 - 50142 Firenze

tel. 055.7876711

Email: [poltel.fi@poliziadistato.it](mailto:poltel.fi@poliziadistato.it)

**ARMA DEI CARABINIERI – LEGIONE TOSCANA**

Via d'È Pilastrì, 54 - 50121 – Firenze

tel. 055.2065417-530 - fax 055.2065409

[lgtsnurp@carabinieri.it](mailto:lgtsnurp@carabinieri.it)



## **CO.RE.COM TOSCANA**

Via de' Pucci, 4 - 50122 Firenze

tel. 055.2387880 - fax. 055.2387871

Email: [corecom@consiglio.regione.toscana.it](mailto:corecom@consiglio.regione.toscana.it)

<http://www.corecom.toscana.it>

<http://www.facebook.com/corecom.toscana>

<http://www.youtube.com/corecomtoscana>

## **COMITATO**

Sandro Vannini (Presidente), Giancarlo Magni (Vice Presidente),

Renato Burigana, Letizia Salvestrini, Maurizio Zingoni

## **STRUTTURA DI ASSISTENZA**

Cinzia Guerrini (Dirigente), Giacomo Amalfitano, Vanna Castaldi,

Silvia Chiarantini, Luciano Dell'Anna, Vanna Giacobbe, Mario Ginanni,

Iolanda Giusteschi Conti, Elisabetta Gonnelli, Antonella Gori,

Alessandra Mariani, Claudia Napoletti, Federica Nebbiai, Annamaria Petrella,

Francesca Sarti Fantoni, Luciano Senni, Stefano Sivieri.





