NOI CITTADINI DIGITALI

Conoscere Opportunità e Rischi di Internet per un uso Consapevole e Sicuro della Rete

IC CORROPOLI COLONNELLA CONTROGUERRA
Elaborazione :prof.ssa Flavia Natali

Voi siete cittadini digitali!

Cittadinanza digitale

È la capacità di un individuo di partecipare alla società online

Come ogni attore di una società

il cittadino digitale diviene portatore di

diritti e doveri

fra i quali quelli relativi all'uso dei servizi dell’amministratore digitale

La RISORSA Internet

Mettendo in rete l'intero pianeta, Internet è una grande **risorsa** per creare contatti tra le persone in ogni parte del mondo

Possiamo usarlo per :

studiare, stare in contatto con gli amici, colmare le lacune tra generazioni, imparare a cucinare, vendere oggetti fatti a mano, guardare programmi di intrattenimento o ottenere indicazioni quando ci siamo persi, cercare opportunità di lavoro, trovare istruzioni su come portare a termine un progetto, gestire i nostri soldi, fare acquisti in altri paesi, fare ricerche per i compiti di scuola, pubblicare i propri pensieri su giornali online o "blog", intrattenere, imparare tutto quello che non avremmo mai immaginato potessimo fare….

Internet ha reso il mondo un posto più piccolo che può essere raggiunto con il tocco di un mouse!

Rischi per la sicurezza in Internet

I rischi più comuni ai quali siamo esposti sono:

- **frodi**
- violazione della **privacy**

(ad esempio, la pubblicazione di una fotografia senza espressa autorizzazione da parte del soggetto ritratto)

- violazione del **copyright**
- **grooming**

(adescamento)

- **sexting**

(invio di messaggi sessualmente espliciti anche con immagini)

- **cyberbullismo**

Che fare allora?

Restare off line????

NO!

La Rete è un prezioso strumento per esperienze cognitive, affettive e relazionali

Ma occorre acquisire la consapevolezza dei rischi ai quali siamo esposti navigando e conoscere e praticare comportamenti corretti per evitarli

MA COS'E' INTERNET ???

Provate a rispondere!

Quando è nato Internet?

La rete Internet ha origine dalla grande rete di computer organizzata dal Ministero della Difesa degli Stati Uniti nel **1969**, denominata **Arpanet** e dalla quale si staccò nel **1983**

Dal 1993 sono stati introdotti il servizio **Web** e la **Posta Elettronica** che hanno favorito l'ampliamento della rete a centinaia di milioni di utenti

INTERNET

ASPETTO TECNICO

È un’enorme rete di computer

ad accesso pubblico

estesa a livello mondiale

ASPETTO SOCIALE ED ECONOMICO

è uno strumento di comunicazione, di incontro e di scambio tra milioni di persone sparse in tutto il Globo

La rete delle reti

Quando un dispositivo è connesso a Internet, invia e riceve informazioni comunicando con altri dispositivi connessi

Ogni singola comunicazione deve avere

un MITTENTE ed un DESTINATARIO

Gli altri apparecchi coinvolti nella trasmissione non memorizzano alcuna informazione, ma si limitano a smistare i dati ad altri apparecchi, in modo che giungano a destinazione

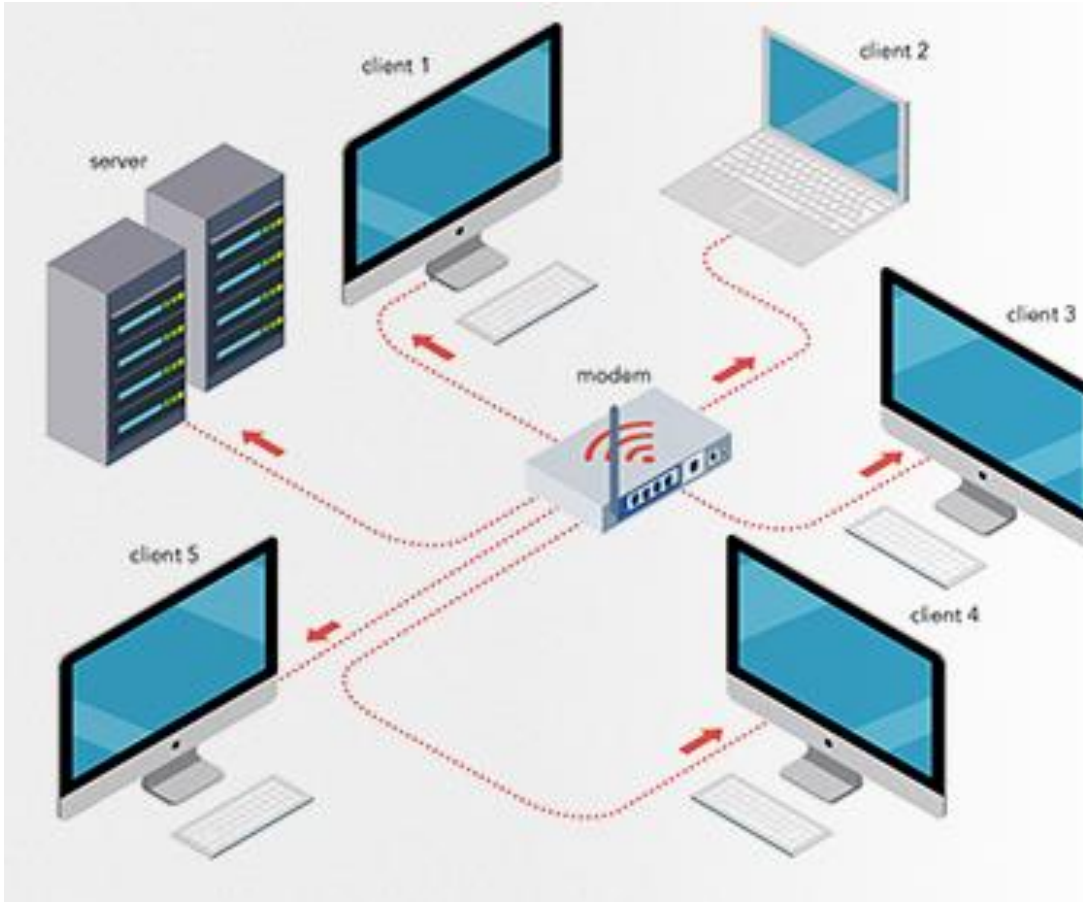
I dispositivi che si occupano dello smistamento delle informazioni si chiamano

ROUTER, che significa proprio ***instradatore***

In una rete Internet lavorano 3 tipi di computer:

- **ROUTER**: si occupano di instradare l'informazione
- **SERVER**: gestiscono i diversi servizi
- **CLIENT**: usati da chi utilizza i servizi

Le reti di Computer

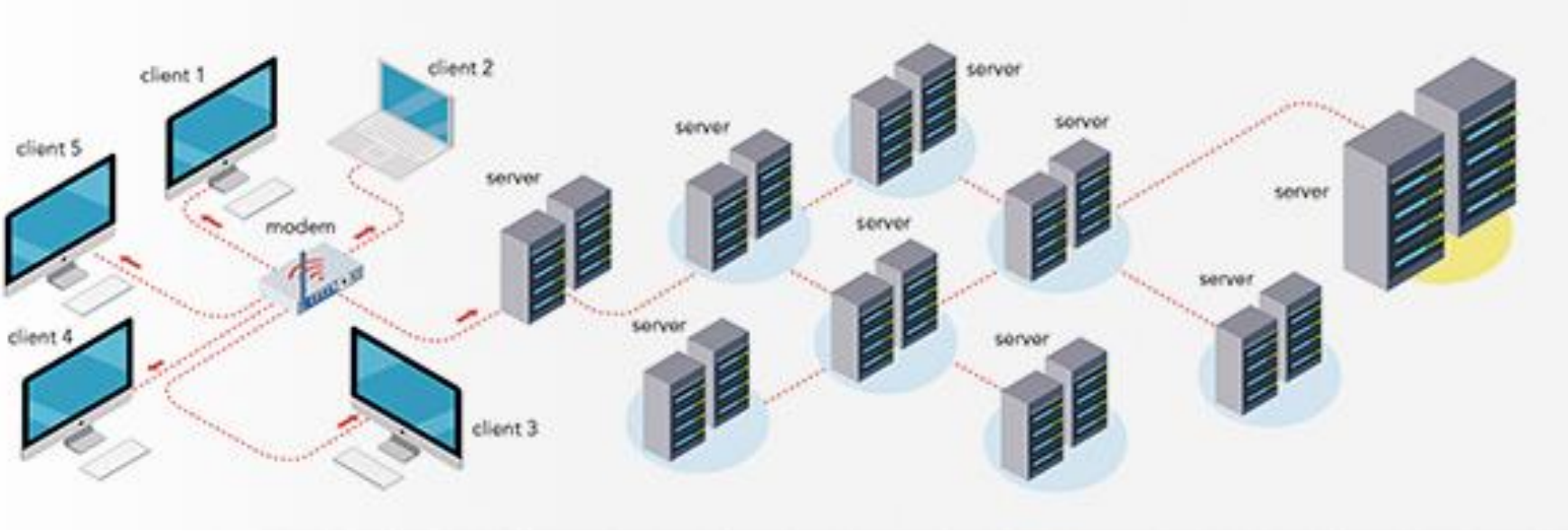


Un computer *server* (servente) fornisce servizi ad altri computer detti *client* (cliente). Quando ti colleghi a Google il tuo dispositivo è un *client* che chiede informazioni a un *server*.

Lo schema di una rete casalinga o di un piccolo ufficio: un dispositivo (modem) collega – via cavo o via Wi-Fi – quattro PC, un portatile e un computer server.

La comunicazione su Internet

I Computer di questa rete locale si collegano a Internet attraverso i server della rete.
In questo modo scambiano informazioni con altri computer connessi a Internet



Il collegamento a Internet

Un computer può collegarsi a Internet in diversi modi:
Attraverso

- una **SCHEDA DI RETE**, i pc sono sempre connessi ad una rete aziendale o universitaria, a sua volta collegata sempre ad Internet
- un **MODEM** (tipo ADSL in genere), connesso alla rete telefonica, i pc domestici o dei piccoli uffici, sono connessi, grazie ad un Provider, solo su richiesta
- un **TELEFONO CELLULARE** (in genere chiavetta USB), i pc portatili o gli smartphone sono connessi da un Provider solo su richiesta
- un'unità radio **WI-FI**, installata all'interno di pc o smartphone, che si collegano via radio ad un punto di accesso Internet, che può essere anche il modem in casa

IL WEB

- World
- Wide
- Web

WWW

"RAGNATELA GRANDE QUANTO IL MONDO"

*E' un **servizio** per chi ha informazioni da diffondere e per chi cerca informazioni*

Le informazioni sono organizzate in **pagine**,
messe su un server Web, collegato a Internet

Sito WEB

- E’ un gruppo di **pagine** collegate tra loro, dedicate ad un certo argomento
- La pagina introduttiva di un sito si chiama

HOME PAGE

- Ogni pagina Web è contraddistinta da un indirizzo che la identifica tra miliardi di pagine presenti su Internet

I SERVIZI DEL WEB

- **Chat** *(= chiacchierata):* scambio istantaneo di messaggi (Whatsapp, Vibel, iMessage)
- **Forum**: pagine nelle quali tutti possono scrivere, ma su un ben preciso argomento
- **Blog**: *(Web Log= diario sul Web)* sito personale per condividere idee e riflessioni
- **Wiki** *(=veloce):* sito Web con una collezione di documenti ipertestuali, sviluppato e aggiornato da tutti gli utenti
- **Condivisione di creazioni** (foto, video, disegni, ecc): Youtube, Flickr, DeviantArt
- **I Social Network** *(= Rete Sociale):* è un gruppo di persone che utilizzano un servizio sul Web per incontrarsi in modo virtuale

I Social Network

- **Profilo personale**: indirizzo di posta elettronica, storia, interessi, lavoro, ecc.

- Scambio di **messaggi** istantanei, posta elettronica, informazioni automatiche sulla propria attività sulla rete

- Es: Facebook, Twitter, Instagram, Snapchat

facebook

è il social network più utilizzato al mondo, con oltre due miliardi di iscritti

Fondato nel 2004 da Mark Zuckerberg, ha impiegato pochi anni per diffondersi in tutto il Mondo

LE ACQUISIZIONI DI FACEBOOK

- Nel **2009** acquisisce **FriendFeed**, social aggregator di contenuti provenienti soprattutto da reti sociali e blog.

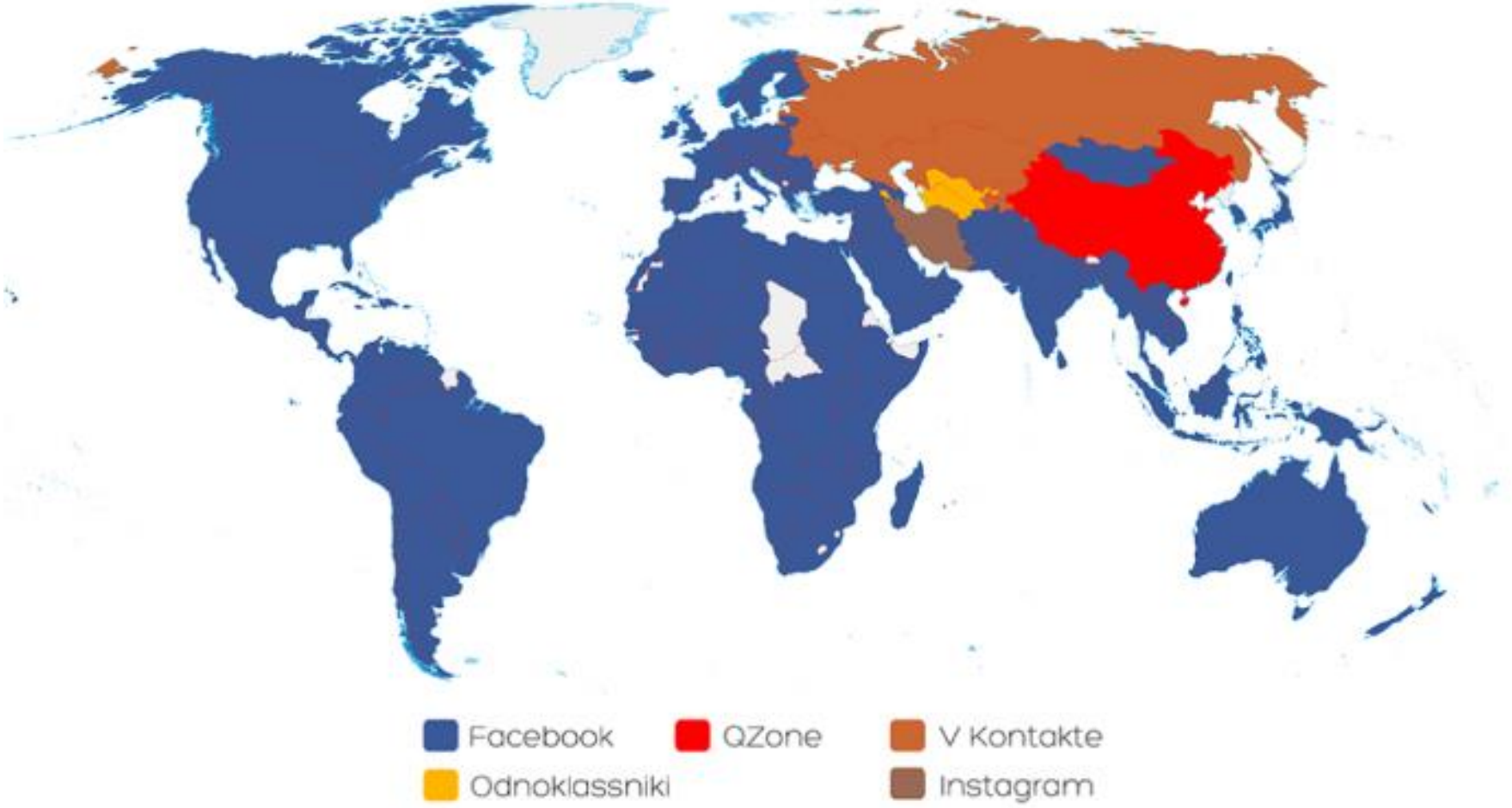
- Nel **2010** Mark Zuckerberg acquista **Snaptu** e **Beluga**, che permettono a Facebook di ottimizzare sia l'esperienza di utilizzo da mobile sia **Facebook Messenger App,** la piattaforma di messaggistica integrata in Facebook. Sempre nel 2010 fa il suo debutto il tasto "Mi Piace" che diventa bene presto una vera e propria icona del social network.

- Nel **2012**, il social network fotografico **Instagram** diventa di proprietà di Facebook. Nello stesso anno passa sotto l'egida Facebook anche **Glancee**, piattaforma sociale che unisce utenti per vicinanza geografica e compatibilità di interessi, fondata da due italiani.

- Il **19 febbraio 2014**: Mark Zuckerberg acquisisce anche **Whatsapp**, applicazione di messaggistica istantanea per sistemi mobili

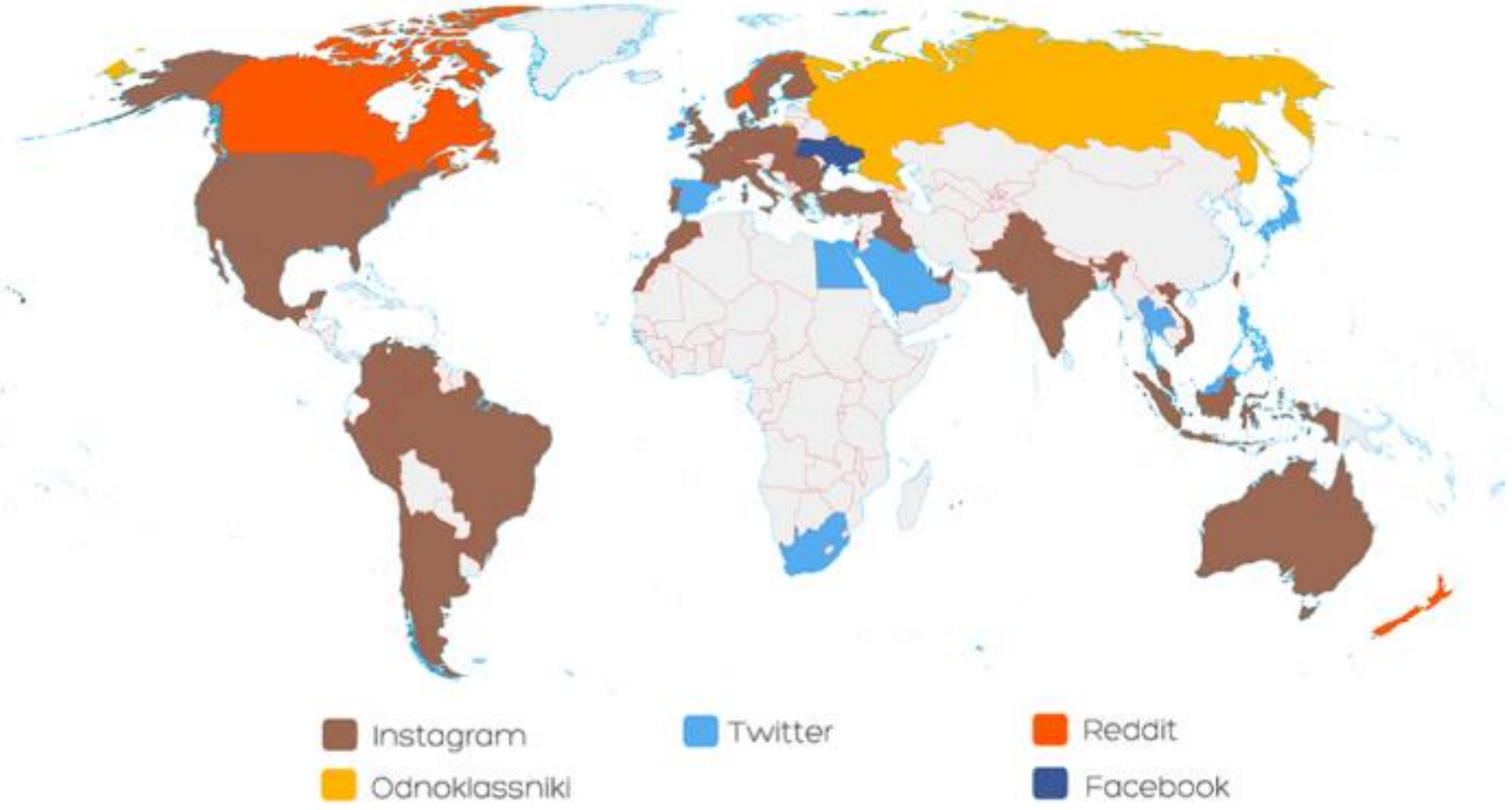
WORLD MAP OF SOCIAL NETWORKS

January 2019

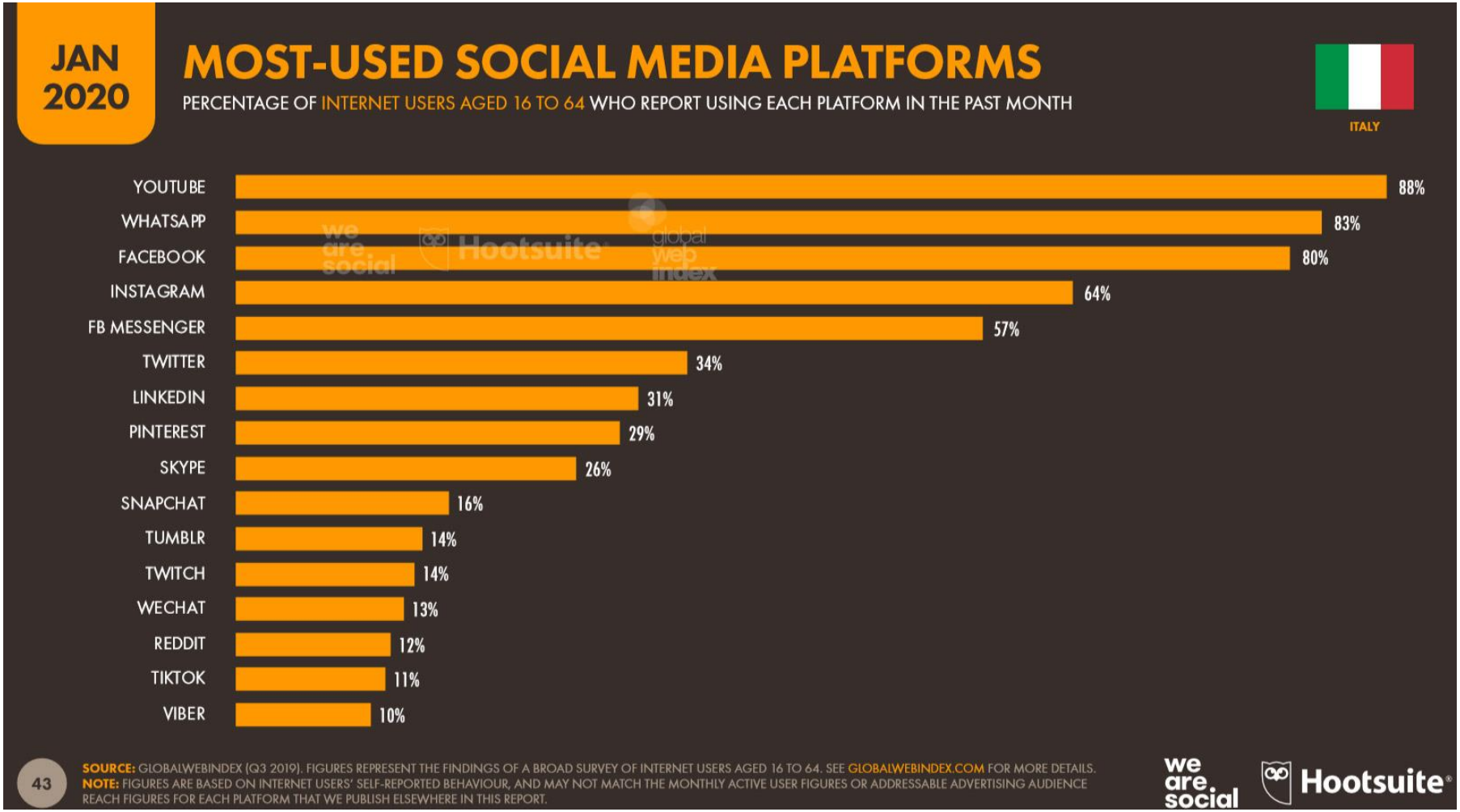


WORLD MAP OF SOCIAL NETWORKS

Ranked 2nd - January 2019



In Italia…


JAN 2020
MOST-USED SOCIAL MEDIA PLATFORMS
PERCENTAGE OF INTERNET USERS AGED 16 TO 64 WHO REPORT USING EACH PLATFORM IN THE PAST MONTH
ITALY
YOUTUBE 88%
WHATSAPP 83%
FACEBOOK 80%
INSTAGRAM 64%
FB MESSENGER 57%
TWITTER 34%
LINKEDIN 31%
PINTEREST 29%
SKYPE 26%
SNAPCHAT 16%
TUMBLR 14%
TWITCH 14%
WECHAT 13%
REDDIT 12%
TIKTOK 11%
VIBER 10%
43
SOURCE: GLOBALWEBINDEX (Q3 2019). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GLOBALWEBINDEX.COM FOR MORE DETAILS.
NOTE: FIGURES ARE BASED ON INTERNET USERS' SELF-REPORTED BEHAVIOUR, AND MAY NOT MATCH THE MONTHLY ACTIVE USER FIGURES OR ADDRESSABLE ADVERTISING AUDIENCE REACH FIGURES FOR EACH PLATFORM THAT WE PUBLISH ELSEWHERE IN THIS REPORT.
we are social
Hootsuite

I problemi di sicurezza di Facebook

- **Marzo 2018**: un'inchiesta del The New York Times e del The Guardian ha fatto emergere che **i dati di milioni di utenti** sono stati ottenuti in modo illecito da un'azienda, infrangendo **le policy di sicurezza di Facebook**.
  Marzk Zuckerberg è stato chiamato a testimoniare anche davanti il Congresso degli Stati Uniti e spiegare ai deputati cosa è realmente accaduto.
- **Marzo 2019:** il bug è stato scoperto dal **giornalista Brian Krebs** che con un post sul proprio blog personale ha spiegato che per diversi anni, le **password di centinaia di milioni di utenti** (stimati tra i 200 e i 600 milioni) non sono state criptate e sono state salvate in un formato facilmente leggibile.
  Le password possono essere state utilizzate per scopi illeciti

La gestione dei DATI in internet e la loro sicurezza

La tematica della **sicurezza informatica** sta diventando sempre più seria con il progredire dei servizi su internet, dall'home banking alle transazioni telematiche, dai blog ai social network.

Al giorno d'oggi, infatti, con il computer di svolgono molte operazioni e questo fa sì che un'enorme massa di dati, tra cui anche sensibili, transiti in pochi secondi su internet.

La sicurezza viene messa a rischio non solo quando i dati abbandonano il singolo pc per diffondersi in rete ma, altresì, quando sono ancora al suo interno (si pensi ai virus che si installano per il solo fatto di avere una porta aperta su internet).

Esistono, inoltre, pratiche molto sofisticate per ottenere informazioni personali.

Alcune definizioni

- **Password**: parola di sicurezza, utilizzata per proteggere l'accesso a dati sulla rete
- **Browser**: particolare programma per navigare in Internet che inoltra la richiesta di un documento alla rete e ne consente la visualizzazione una volta arrivato
- **Virus**: programma pirata, trasmesso tramite reti telematiche, diretto a bloccare o ad alterare il funzionamento di un computer o di una rete.
- **Firewall**: sistema di protezione che difende i calcolatori di una rete aziendale collegata a Internet da accessi non autorizzati.
- **Spyware**: Software scaricato, spesso in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente, generalmente a scopo pubblicitario.

Alcune definizioni

- ***Phishing***
  Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.
- ***Spoofing***
  Manipolazione dei dati trasmessi in una rete telematica, consistente nella falsificazione del proprio indirizzo IP, oppure nell'utilizzo abusivo di user name e password di altri utenti, o anche nel camuffamento di file nocivi per renderli irriconoscibili come tali.

I Cookies

Sono file di testo in cui sono scritte informazioni riguardo il sito visitato ed il computer usato per navigare

Il cookie fa in modo che quando si cerca con Google, i risultati già cliccati siano colorati di viola oppure che quando si entra in Facebook compaiano alcuni aggiornamenti invece di altri nella pagina home delle notizie

I cookie possono memorizzare tutti i tipi di informazioni, compreso il tipo di browser usato, la posizione, il tipo di computer ecc.
In generale queste informazioni possono essere utilizzate per migliorare la navigazione sul sito, ma alcuni siti rilasciano cookie maligni che cercano di rubare informazioni private dai computer degli ignari navigatori
E' bene, quindi, controllare e/o cancellare i cookies memorizzati sul proprio browser, mediante appositi software gratuiti messi a disposizione in rete (*Cookiespy, Spybot, ecc*)

Video

Social network

- https://www.youtube.com/watch?v=BqtnYcfgLbM&ab_channel=Garanteperlaprotezionedeidatipersonali

App

- https://www.youtube.com/watch?v=MopODAPI5HY&ab_channel=Garanteperlaprotezionedeidatipersonali

Rischi

- https://www.youtube.com/watch?v=6eF-mwKhrVo&ab_channel=Garanteperlaprotezionedeidatipersonali
- https://www.youtube.com/watch?v=MJxtTIyuqlI&ab_channel=Registroit

Spam

- https://www.youtube.com/watch?v=hDOH09EcFr0&ab_channel=Garanteperlaprotezionedeidatipersonali

Cookies e Privacy

- https://www.youtube.com/watch?v=Mut-YXSExnw&ab_channel=Garanteperlaprotezionedeidatipersonali

Accorgomenti per la tutela dei dati

La miglior difesa per la tutela della privacy consiste, nell'utilizzare il buon senso e nell'utilizzare piccoli accorgimenti:

- adottare **password** imprevedibili e con codici alfanumerici, cambiandole frequentemente e diversificandole a seconda dei siti;
- evitare di comunicare la propria password e conservarla in un luogo sicuro, non sul computer che va in rete;
- installare e configurare ***firewall*** e ***antivirus*** tenendoli costantemente aggiornati;
- procurarsi un ***antispyware*** in grado di ripulire efficacemente il sistema;
- tenere sotto controllo i ***cookies***, ogni tanto cancellandoli completamente e utilizzando cookie manager che permette una gestione effettiva da parte dell'utente;
- utilizzare un ***trace eraser***: talune tracce elettroniche persistono dopo l'utilizzo di un computer. Cancellare queste tracce è spesso molto complicato e l'utilizzo di software specifico è consigliato;
- non aprire **allegati** di e-mail provenienti da utenti sconosciuti o sospetti; oltretutto si evitano il *phishing o lo spoofing;*
- leggere le licenze e le disposizioni riguardo alla **privacy** prima di installare un qualsiasi software.

Conseguenze negative sull'utente

In rete circolano spesso molte **informazioni personali** da parte di utenti inesperti che consentono tracciabilità ed una facile definizione del profilo.

Si pensi al fatto che spesso le domande di assunzione nelle ditte sono filtrate dalle aziende con **indagini** effettuate proprio **sui social network**. In altri termini, quello che viene scritto nei curricula viene verificato con quello che viene pubblicato su internet dove le persone hanno meno filtri (si pensi ai blog o ai commenti sui blog altrui).

Un altro tipo di ricerca posta in essere dai datori di lavoro può essere quello sullo stato di salute del lavoratore attraverso le dichiarazioni che vengono rilasciate nei forum, nelle chat o nelle richieste dirette a medici esperti attraverso cui vengono messe in circolazione, **dati sensibili**, facilmente acquisibili ed utilizzabili da altri.

Le avvertenze di rischio

Il Garante della privacy ha raccomandato per questi siti l'inserzione della cosiddetta **avvertenza di rischio**, attraverso cui l'utente, quando deve inserire la richiesta o la domanda, è costretto a barrare un'apposita casella per confermare di aver preso visione delle conseguenze (raccomandazione, che nella prassi, non è quasi mai seguita dai vari siti).

Qualunque dato messo su internet è per sempre su internet!

Questo dato di fatto porta a **conseguenze** dannose ancora più gravi per l'utente debole:

- **atti persecutori**: nonostante si neghi la configurazione del reato di stalking via mail, il molestatore, attraverso l'uso di internet (si pensi soprattutto a Facebook in cui vicende di questo tipo sono note), può carpire dati sensibili e giungere facilmente all'individuazione dei luoghi frequentati dalla vittima e porre in essere la sua condotta criminosa;
- permettere l'azione di **truffatori** di ogni genere, dai ladri di identità ai ladri di "cose".

I rischi legali dei Social Network

- L'Articolo 595 del **Codice penale** sostiene che "chiunque […] comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a 1032 Euro".
  A ciò si aggiunga che "se l'offesa consiste nell'attribuzione di un determinato fatto, la pena aumenta, e se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516".
- **Si presti attenzione a quanto si decide di pubblicare online.**
  Secondo il parere della Corte di Cassazione infatti la pubblicazione di un commento offensivo può essere ritenuta una vera e propria diffamazione.
- Poiché il **reato di diffamazione**, per essere considerato tale deve essere accessibile a una moltitudine di persone, deve offendere la reputazione di un soggetto, in maniera consapevole, attraverso un mezzo stampa o di pubblicità.
- I Giudici della Corte hanno stabilito che anche **la sola iscrizione al Social network** determina la possibile diffusione a più persone di un commento, questo nonostante le offese siano scritte attraverso un profilo privato.

La cronaca

A Milano, 12 liceali sono stati sospesi da scuola (e costretti a lavori socialmente utili) perché avevano fatto girare le immagini hot di una loro compagna, realizzate alle medie dal suo ex fidanzatino.
Ma a parte il provvedimento disciplinare, l'inchiesta sta valutando se si rientra in un caso di

cyberbullismo

normato dalla legge 71/2017.

Questa legge contiene una novità importante, ovvero la possibilità per i ragazzi di difendersi da soli: se hanno più di 14 anni possono chiedere la rimozione di un contenuto offensivo.

Anche se **la cancellazione può risultare inutile, se c'è stata condivisione**

Ancora un dettaglio da sottolineare: chi paga. I genitori, ovvio.

A Sulmona, una coppia ha dovuto sborsare 100mila euro di risarcimento alla famiglia di una ragazzina che si era fatta fotografare nuda per gioco da un compagno che poi le aveva fatte girare.

E chi è responsabile di un minore?

Pubblicazione di fotografie online

La pubblicazione di fotografie online si inquadra pacificamente nel trattamento di dati personali e sensibili, e costituisce interferenza nella vita privata del minore.

In tal senso occorre fare particolare attenzione nel pubblicare immagini di minori, anche se si tratta dei propri figli.

In quest'ottica una recente sentenza del tribunale di Mantova (novembre 2017) ha stabilito che per la pubblicazione delle foto dei figli occorre il consenso di entrambi i genitori. In assenza dell'accordo dei due genitori, la foto non è pubblicabile, in quanto **viola**:

- l'articolo 10 del codice civile in tema di diritto all'immagine, 4
- gli articoli 4,7,8 e 145 del d. lgs. 30 giugno 2003 n. 196 (Codice Privacy) riguardanti la tutela della riservatezza dei dati personali
- gli articoli 1 e 16, I comma, della Convenzione di New York del 20/11/1989 sui diritti del fanciullo, ratificata dall'Italia con legge 27 maggio 1991 n. 176.

Minori e protezione dati personali

La tutela dei dati personali e della privacy dei **minori** è divenuta un problema rilevante con l'avvento dei social network.
La minore età, infatti, è legata a diritti rafforzati rispetto agli adulti, per cui il trattamento da parte delle aziende dei loro dati deve essere regolamentato in maniera differente.

Regolamentazione europea dal 25 maggio 2018

General Data Protection Regulation

Social Media e Pubblica Amministrazione

Minori e servizi digitali
(social network, messagistica)

- Il nuovo Regolamento Europeo (**GDPR**) ha fissato, con l'articolo 8, il divieto di offerta diretta di servizi digitali (quindi **iscrizione ai social network e ai servizi di messagistica)**, ai minori di 16 anni, a meno che non sia raccolto il consenso dei genitori o di chi ne fa le veci.
  In sostanza **il GDPR introduce una deroga** per i casi specifici indicati (i requisiti) **alla regola generale** fissata dall'ordinamento, abbassando il limite dei 18 anni (per l'Italia), quindi una sorta di maggiore età digitale raggiunta la quale è ammesso il consenso al trattamento dei propri dati personali anche con riferimento a profilazione.

- Inoltre, tale limite può essere ulteriormente abbassato dagli Stati nazionali (ma il limite non può scendere al di sotto dei 13 anni). In tale prospettiva **il legislatore italiano ha fissato il limite di età da applicare in Italia in 14 anni,** col decreto di adeguamento del Codice Privacy.

Servizi online

Attualmente la regolamentazione dei vari servizi online in Italia prevede questi limiti di età:

- **Facebook**: i minori di 13 anni non possono iscriversi, i minori di 14 potranno iscriversi solo col consenso del genitore;
- **Whatsapp**: i minori di 13 anni non possono iscriversi, per i minori di 14 occorre il consenso del genitore;
- **Twitter**: i minori di 16 anni non possono usare Periscope (un'applicazione di Twitter per trasmettere in diretta una ripresa fatta con il proprio smartphone)

La realtà

In **Italia il divieto sussiste fino ai 14 anni**. Nello specifico, un minore non può iscriversi su **Facebook, Instagram, Twitter, Snapchat o WhatsApp** sotto i 13 anni, mentre tra i tredici e i 14 serve la supervisione dei genitori.

La realtà, tuttavia, è molto diversa. Secondo una ricerca effettuata nel 2019 da **Osservare Oltre** (Associazione Nazionale Presidi ed eTutorweb) per il Tg3 è emerso che **l'84% dei ragazzi tra i 10 e i 14 anni è in possesso di un profilo social.** Per farlo, nessuno ha dichiarato la sua vera età al momento dell'iscrizione, che per il 22% è avvenuta addirittura in presenza di un genitore.

E siccome in Italia **le false dichiarazioni sono reato** solo se fatte **a un pubblico ufficiale**, di fatto i minori si iscrivono sui social e nel caso dei baby influencer ne diventano protagonisti.

La tutela dei DIRITTI del minore

A riprova che la norma è disegnata per tutelare il minore, non certo per ostacolare la messa a disposizione dei minori di servizi, si specifica anche che

"**il consenso del titolare della responsabilità genitoriale non deve essere necessario nel quadro dei**

servizi di prevenzione o di consulenza forniti direttamente ai minori".

Il riferimento è a servizi di tutela dei minori quali quelli previsti in materia di **cyberbullismo**

o in genere di sostegno all'infanzia (es. **Telefono azzurro**).

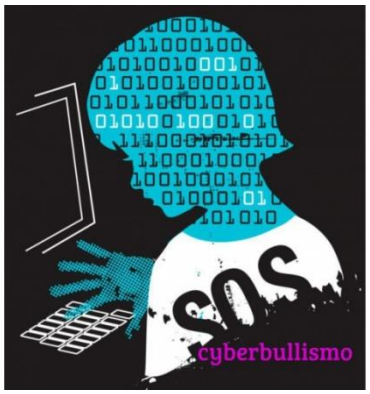
Infatti, le norme in materia riconoscono al minore ultraquattordicenne la possibilità di esercitare
i diritti previsti a propria tutela contro il cyberbullismo.

Bullismo e Cyberbullismo

- **BULLISMO** è l'aggressione o la molestia ripetuta a danno di una vittima in grado di provocarle ansia, isolarla o emarginarla attraverso vessazioni, pressioni, violenze fisiche o psicologiche, minacce o ricatti, furti o danneggiamenti, offese o derisioni

- Se tali atti si realizzano con strumenti informatici si ha il **CYBERBULLISMO**, il bullismo telematico e informatico

Cyberbullismo



La Legge 71 del 2017

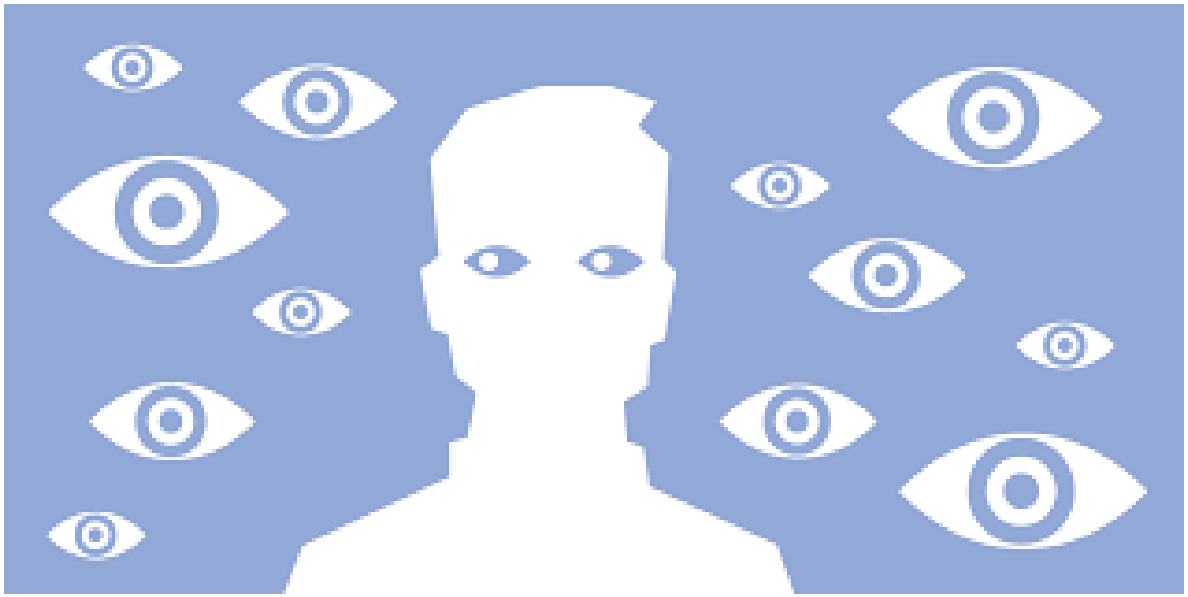
“Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”

ha previsto degli specifici compiti da parte dell’Autorità Garante della Privacy in materia di cyberbullismo
La legge prevede misure di prevenzione ed educazione nelle scuole, sia per la vittime che per gli autori di atti di cyberbullismo.
Inoltre, i minori potranno chiedere **l'oscuramento** o la **rimozione** di contenuti offensivi senza dover informare i propri genitori.
La richiesta va inoltrata al gestore del sito o al titolare del trattamento, e, in seconda battuta (questa volta a mezzo dei genitori), al Garante, che interverrà in 48 ore

Modello per la segnalazione reclamo in materia di cyberbullismo

Attenzione!

La rimozione dei contenuti offensivi può non essere efficace se i dati sono stati condivisi!!!!



Il lessico del Cyberbullismo

- **FLAMING**: invio di messaggi offensivi, soprattutto sui social.
- **SEXTING**: invio di messaggi sconci, sessualmente espliciti, in genere privati.
- **HARASSMENT**: molestie, anche sessuali.
- **CYBERSTALKING**: persecuzione per mezzo di strumenti informatici.
- **SEXTORSION**: estorsione, ricatto con minaccia di pubblicare o diffondere foto e video osé o a carattere sessuale.
- **CHALLENGE AUTOLESIVE**: sfide autolesionistiche che spingono a procurarsi dolore fisico e ad infliggersi ferite e a condividere online le proprie imprese.

Il lessico del Cyberbullismo

- **HATE SPEECH**: discorsi di incitazione all'odio, basati su intolleranza, discriminazione, ostilità.

- **VAMPING**: fenomeno per cui i teenager rimangono svegli tutta la notte o si svegliano appositamente per inviare o rispondere ai messaggi, pubblicare foto oppure commenti sui social network (da "vampire", vampiro).

- **HIKIKOMORI**: diffuso dapprima in Giappone, fenomeno riscontrato tra gli adolescenti, che consiste nel ritiro fra le mura domestiche e la mancanza di qualunque rapporto sociale.

Fatti e cifre

In Italia le ragazze sono più di frequente vittime di cyberbullismo: **7,1%** rispetto al **4,6%** dei ragazzi

Le prepotenze più comuni consistono in offese con brutti soprannomi, parolacce o insulti (**12,1%**), derisione per l'aspetto fisico e/o il modo di parlare (**6,3%**), diffamazione (**5,1%**) esclusione per le proprie opinioni (**4,7%**) aggressioni con spintoni, botte, calci e pugni (**3,8%**).

Nel corso della propria carriera il **75,8%** dei dirigenti scolastici si è trovato a gestire il **65%** di casi di bullismo tradizionale e il **52%** di cyberbullismo

In tutto il mondo
1 ragazzo su 3
tra i 13 e i 15 anni
è vittima di cyberbullismo

Aumenta la percentuale
di ragazze e ragazzi che vivono
esperienze negative navigando
in Internet: erano il 6 %
nel 2010, sono diventati
il 13 % nel 2017.

Fonti: UNICEF/CENSIS/ISTAT/MIUR

Ma nel 58% dei casi
gli intervistati ammettono
di non aver fatto nulla
per difendere le vittime.

Il 31% degli 11-17enni
dichiara
di aver visto online messaggi
d'odio o commenti offensivi
rivolti a singoli individui
o gruppi di persone, attaccati
per il colore della pelle,
la nazionalità o la religione.

Conclusioni

La Rete è parte delle nostre vite e lo sarà sempre di più nel futuro
Per questo dobbiamo imparare a farne un uso consapevole e corretto

Netiquette

- Navigare evitando siti web rischiosi
- Non compromettere il funzionamento della Rete e degli apparecchi che la costituiscono con programmi (virus ecc.) costruiti appositamente
- Rispettare la Privacy altrui non pubblicando o condividendo, tramite i Social Network, dati personali senza l'esplicito consenso dell'interessato
- Denunciare qualsiasi forma di abuso, violazione, cyberbullismo, attraverso gli strumenti resi disponibili

E soprattutto….

Basta un click per fare del male

agli altri e a te stesso

Ora che conosci le conseguenze e le regole da seguire

condividile con i tuoi amici per diventare

cittadini digitali di un mondo migliore

CYBERBULLISMO

No, grazie!

BULLISMO E
CYBERBULLISMO