LUISS @LawLab LABORATORIO SUL DIRITTO DEL DIGITALE 25 GPDP GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Con il supporto di Google

A SCUOLA DI PRIVACY

Protezione dei dati dei minori: formazione, informazione, consapevolezza

“La protezione dei dati è particolarmente importante per i minori:
hanno bisogno di essere protetti dagli altri e un po’ anche da loro stessi.
E per formare gli studenti è necessario fornire gli strumenti agli educatori”

Bernardo Giorgio Mattarella
Professore Ordinario di Diritto Amministrativo e Direttore del Centro di ricerca sulle amministrazioni pubbliche “Vittorio Bachelet”, Luiss Guido Carli

---

“I nativi digitali non esistono. È solo l’alibi che ci illude che non serva educarli.
Invece, il rapporto tra bambino e adulto - genitore o insegnante - non è cambiato:
resta fondamentale il ruolo di questi ultimi nel guidarli nel mondo del digitale”.

Guido Scorza
Componente del Collegio del Garante per la protezione dei dati personali

Introduzione

QUALCHE DATO

Navigano online circa 5 miliardi di utenti e **un terzo sono bambini**. Si tratta quindi di **un miliardo e mezzo di minori** che già oggi vivono immersi nella dimensione digitale. Un numero destinato ad aumentare in futuro. Secondo un report della società di consulenza strategica Boston Consulting Group, **il 93% dei minori fra 8 e 17 anni ha accesso alla rete e il 72% dice di aver subito almeno una minaccia informatica** (dai pop-up indesiderati a veri e propri casi di cyberbullismo e tentativi di approcci sessuali che rappresentano il 20% del totale). Anche in Italia l'abuso e la violenza ai danni dei più giovani corrono online. Diversi i potenziali rischi: dallo stalking alla diffamazione online; dal revenge porn alla pedofilia; dalla sextortion alla sostituzione di persona, dalla disinformazione all'hate speech. Nel 2022 la polizia postale ha trattato **4.542 casi di reati commessi online** a danno di minori, indagando **1.463 persone** e arrestandone **149**. La rete, proprio per la sua specificità, può risultare uno dei luoghi meno sicuri per i minori: il cyberbullismo, ad esempio, ha le stesse caratteristiche del bullismo tradizionale ma, viste le capacità pervasive di internet, le sue conseguenze sono potenzialmente più gravi del bullismo offline. E spesso gli adolescenti sono anche i carnefici: solo lo scorso anno sono stati **128 i minori denunciati in Italia** dalla polizia postale per cyberbullismo.

IL PROGETTO

È proprio partendo dalla consapevolezza di questi dati che nasce l'idea di un corso da offrire a insegnanti ed educatori, per fornire loro (**cioè a voi!**) gli strumenti per guidare e accompagnare bambini e ragazzi in rete. Nello specifico, questo progetto nasce davanti a un caffè. Lo ha raccontato nell'incontro di apertura **Guido Scorza**, componente del Collegio del Garante per la protezione dei dati personali: "Io e **Pietro Falletta** abbiamo fatto una chiacchierata su un problema che percepiamo tutti, da genitori o insegnanti: **i bambini e i ragazzi pagano in dati personali il loro diritto a esistere nella dimensione digitale**. La gratuità della rete è un'illusione. Ogni volta che guardano un cartone animato o giocano a un videogame pagano con un pezzetto di loro stessi: i loro dati. E questa dimensione coinvolge anche lo studio, basti pensare alla DAD". Da qui l'importanza di fornire ai minori, attraverso i loro insegnanti, le giuste informazioni sul funzionamento del mondo digitale. Nel farlo, questo progetto si pone un obiettivo molto chiaro: "**Mettere a fuoco le opportunità e i rischi del digitale**, rafforzando la consapevolezza dei ragazzi rispetto al rapporto tra **vita vera e digitale**", ha spiegato il professor Falletta , direttore di @LawLab – Laboratorio sul diritto del digitale. Un obiettivo raggiungibile solo se si guarda ai giganti della tecnologia come a degli alleati. **Martina Colasante**, Government Affairs & Public Policy Manager di Google, ha elencato i tre pilastri su cui si basa la strategia dell'azienda in questo campo. Uno: la possibilità per i minori di navigare in modo sicuro e responsabile, con **soluzioni che siano su misura per loro** (ad esempio YouTube Kids), senza profilazione personale e senza che i dati vengano raccolti per scopi economici. Due: dare alle famiglie **la possibilità di un controllo personalizzato** in base a ciascun figlio. Tre: **proteggere i bambini e i loro dati** dai rischi della rete. Questi obiettivi si raggiungono, da una parte, identificando e rimuovendo il più velocemente possibile i contenuti rischiosi e, dall'altra, attivando maggiori tutele sui dati degli account associati a minori. Ma la tecnologia da sola non basta. È necessaria un'attenzione costante di chi ha il compito di educare i ragazzi. I docenti sono figure chiave. Lo dicono, all'unisono, i tre ideatori del progetto: "**Noi senza di voi non possiamo farcela**".

IL VADEMECUM

Questo vademecum si propone di rappresentare uno strumento utile affinché portiate con voi, nelle vostre classi, le competenze apprese durante il ciclo di seminari. Per trasmettere le informazioni ai vostri alunni e guidarli nel mondo del digitale. Ogni capitolo del vademecum, a cui corrisponde un diverso seminario, sarà così strutturato:

Gli interventi degli esperti
Le parole (chiave) sono importanti
Diritti e doveri
Domande e risposte

Buona lettura, allora!
E buona **libertà** a tutti.

1

La protezione dei dati dei minori

1. GLI INTERVENTI DEGLI ESPERTI

Guido Scorza spiega come molti servizi e applicazioni della rete siano riservati **solo ai maggiori di 13 anni** (età minima fissata dal legislatore americano).

"Immaginiamo internet come un enorme parco divertimenti. Ci sono attrazioni aperte a tutti e altre riservate a chi è alto almeno un metro, perché le cinture di sicurezza sono pensate solo per i più grandi. Internet non è mai stato pensato per tutti e continua a non esserlo".

TENERE I BAMBINI E I PIÙ GIOVANI FUORI DAGLI SPAZI DELLA DIMENSIONE DIGITALE NON DESTINATI A LORO

A Palermo una bambina si tolse la vita partecipando a una sfida su TikTok senza avere l'età per essere iscritta. Il Garante della privacy bloccò TikTok e fece campagna **per ricordare come il social sia riservato agli over 13 anni**. Molti genitori scrissero al Garante: erano stati loro stessi a iscrivere i propri figli su quel social perché non lo sapevano.

Cosa fare? Occorre **RAFFORZARE la verifica dell'età** (come sulle montagne russe) nella dimensione digitale. Un primo passo utile anche se non definitivo.

EDUCARE I PIÙ PICCOLI ALL'IDEA CHE INTERNET NON È GRATIS COME SEMBRA. SI PAGA IN DATI E I DATI VALGONO

I bambini (e a volte gli adulti) non hanno la percezione di quanto valgano i loro dati. Nessuno dice al proprio figlio/alunno: "*Non puoi spendere tutti i tuoi dati personali*".

Anche quando sono consapevoli dell'utilizzo dei dati per la profilazione dei loro gusti, pensano: "*Meglio, mi propongono pubblicità che mi interessano*".

Ma a quale prezzo? **Cedendo i nostri dati stiamo cedendo parte della nostra libertà di scelta. Il nostro diritto di autodeterminazione**: i ragazzi, in questo modo, potrebbero non scegliere in futuro cosa vogliono leggere, comprare, guardare... le loro scelte potrebbero essere orientate, o peggio, *manipolate*.

I BAMBINI NON POSSONO CONCLUDERE I CONTRATTI DIGITALI

"*Accetta e continua*": il bambino preme quel tasto inconsapevolmente. Eppure sta firmando un contratto. E **nessun genitore andrà davanti a un giudice ad annullarlo**.

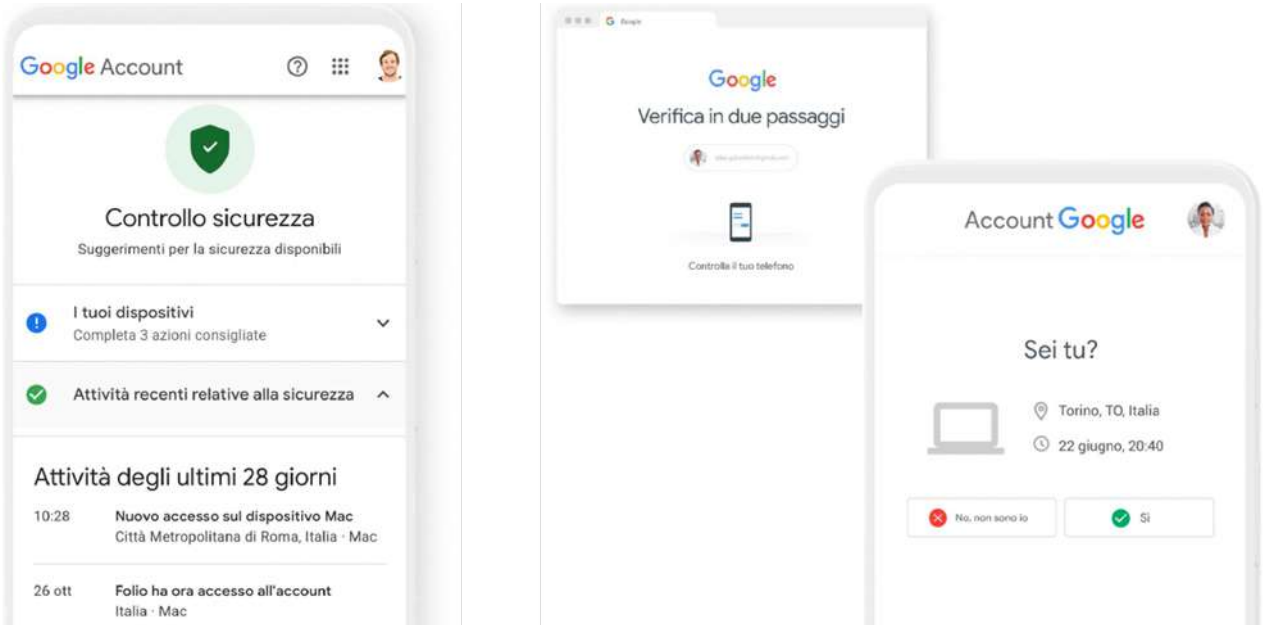
Leggere i termini d'uso di un servizio è un'operazione difficilissima. Pochissimi leggono. Ancor meno capiscono. Nessuno contratta.

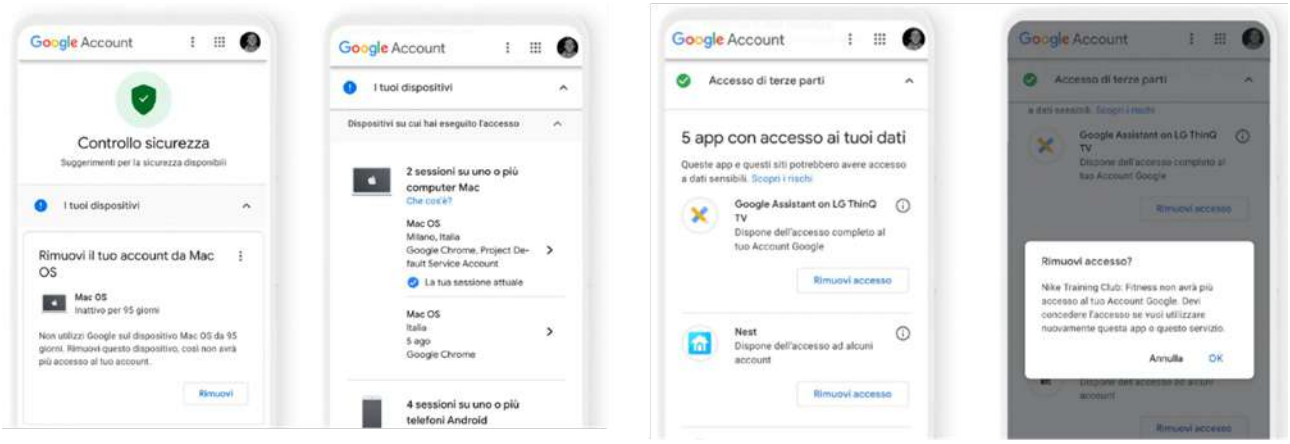
Di chi è la responsabilità? Dei regolatori. Educare gli adulti per educare i più piccoli.

2. COME AUMENTARE LA NOSTRA SICUREZZA IN RETE

Questi, ad esempio, sono gli strumenti offerti da Google: basta digitarli.
Il **Controllo Sicurezza** fornisce consigli per rafforzare la sicurezza dell'Account Google:

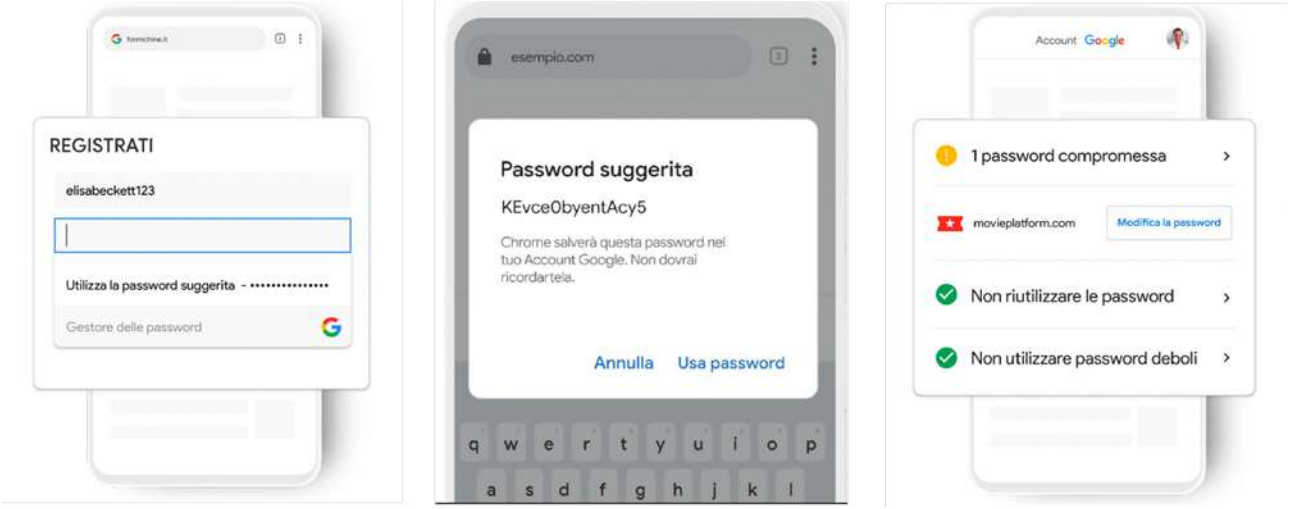
- controllando le "attività recenti sulla sicurezza"
- attivando la "verifica in due passaggi" per accedere all'account
- "gestendo i dispositivi" associati
- controllando (ed eventualmente bloccando) "l'accesso delle terze parti" ai nostri dati





Il Gestore delle password, uno strumento che permette di

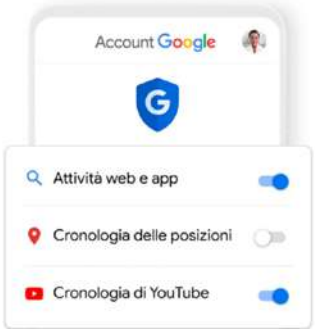
- **Creare e salvare password efficaci e diverse per ogni sito** (che restano criptate e non vengono trasmesse ai server di Google)
- **Ricevere notifiche relative a password non sicure**

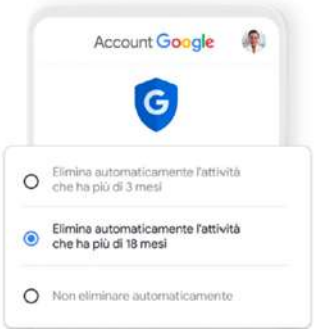


Il **Controllo Privacy** che permette all'utente di gestire:

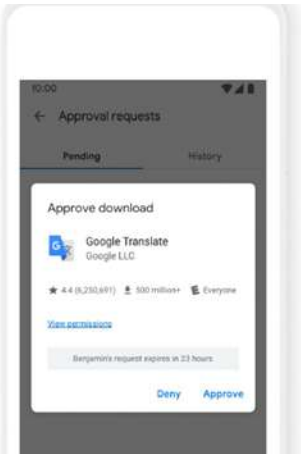
Quali dati salvare sul proprio Account Google

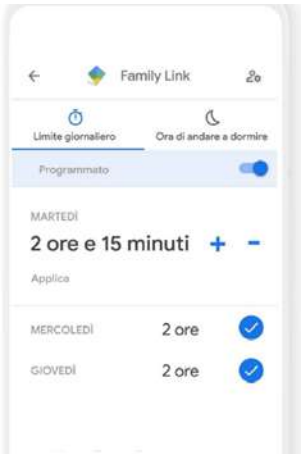
La **personalizzazione degli annunci** (posso scegliere di non ricevere pubblicità personalizzata e di eliminare i dati relativi alle mie ricerche)

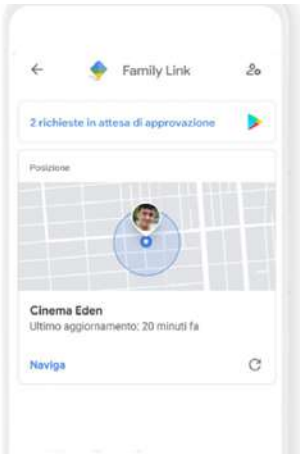




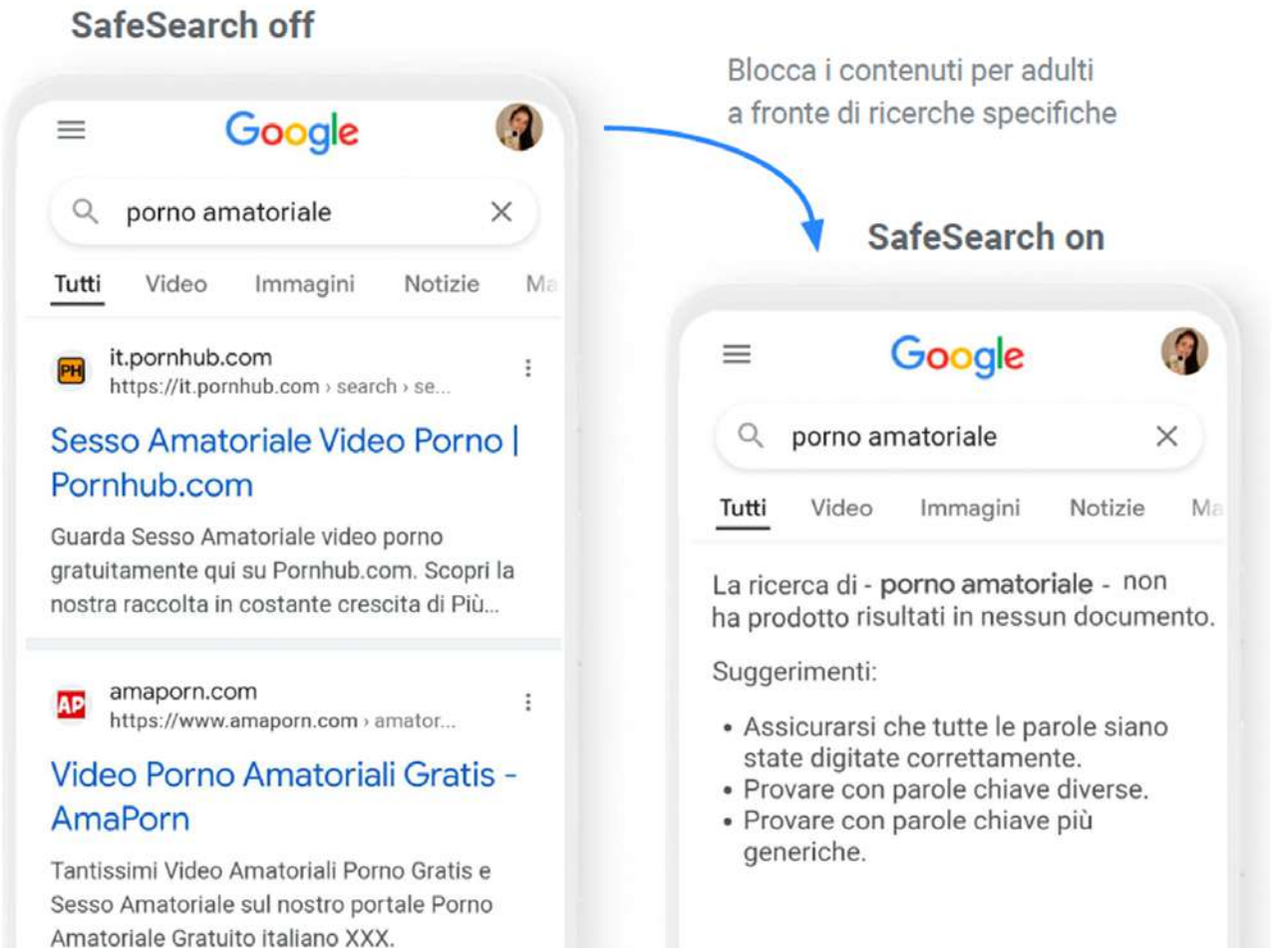
Per le famiglie esiste poi uno strumento che si chiama "**Family link**" che permette ai genitori di controllare diversi elementi dell'account dei propri figli minori di 14 anni: quali app possono scaricare e per quanto tempo si possono utilizzare (impostando dei limiti orari e dei blocchi), fino alla possibilità di controllare la posizione dei figli.







Infine, è possibile attivare nel proprio motore di ricerca l'opzione "**Safesearch**". Normalmente la Ricerca di Google è progettata per non mostrare contenuti che possano turbare le persone. Tuttavia, mostra contenuti espliciti quando vengono espressamente cercati. VICEVERSA: se si attiva Safesearch, vengono ulteriormente filtrati i contenuti sessualmente espliciti. È inserito di default per gli utenti di Family Link e i bambini non possono disattivarlo senza il permesso dei genitori.



3. LE PAROLE (CHIAVE) SONO IMPORTANTI

DATI: la nostra "moneta" su internet, quello che cediamo in cambio dell'utilizzo della rete. Come le monete vere hanno un valore e non andrebbero sprecati.

ETÀ: per ogni cosa c'è un'età giusta, anche su internet. Non tutti i servizi sono per tutti. Molti (strano ma vero) sono solo per i maggiori di 13 anni.

CONSENSO: dovrebbe essere alla base di ogni rapporto. Anche online lo scambio dati-servizi necessita di un consenso reale e informato.

CONTRATTO: ogni volta che clicchiamo su "accetta e prosegui" stiamo firmando un contratto. Se siamo minorenni non lo potremmo fare e in ogni caso pensiamoci: firmeremmo senza leggere nulla se fossimo alla scrivania di un giudice o di un notaio?

PROFILAZIONE: l'insieme delle attività di raccolta ed elaborazione dei dati degli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento e offrire loro servizi o pubblicità personalizzate. Non è un male ma sappiate che c'è.

AUTODETERMINAZIONE: se cediamo i nostri dati e diamo a internet il potere di orientare - o manipolare - le nostre scelte ci priviamo del diritto ad autodeterminarci, cioè di decidere da soli cosa sia meglio per noi stessi.

STRUMENTI: i motori di ricerca e i gestori della rete - spesso - offrono diversi strumenti che possiamo utilizzare per proteggere e gestire al meglio i nostri dati e quelli dei minori. È importante conoscerli e metterli in pratica.

4. DIRITTI E DOVERI

DIRITTO DI ESSERE INFORMATI sul trattamento dei propri dati (durata, categoria, destinatari, etc).

DIRITTO DI ACCESSO ad una copia dei propri dati.

DIRITTO DI OPPOSIZIONE al trattamento dei propri dati personali:

per motivi connessi alla situazione particolare dell'interessato, da specificare nella richiesta;
quando i dati sono trattati per finalità di marketing diretto (senza necessità di motivare l'opposizione).

DIRITTO DI RETTIFICA in caso di dati inesatti e incompleti.

DIRITTO ALLA CANCELLAZIONE:

se i dati non sono più necessari per le finalità per cui sono stati trattati;
se l'interessato revoca il consenso o si oppone al trattamento;
se i dati sono trattati illecitamente;
se devono essere cancellati per adempiere a un obbligo legale;
se non vi sono altri trattamenti per i quali i dati sono considerati necessari.

DIRITTO ALLA PORTABILITÀ dei dati verso un altro titolare, se il trattamento si basa sul consenso o su un contratto stipulato con l'interessato e viene effettuato con mezzi automatizzati.

OBBLIGO DI RISPETTARE I PRINCIPI SUL TRATTAMENTO FISSATI DALL'ART. 5 DEL GDPR (REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI):

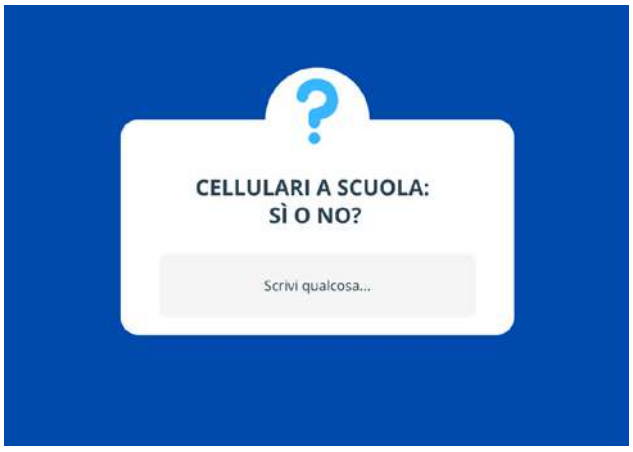
liceità, correttezza e trasparenza
limitazione della finalità del trattamento
minimizzazione dei dati
esattezza e aggiornamento dei dati
limitazione della conservazione
integrità e riservatezza

PRINCIPIO DI "RESPONSABILIZZAZIONE" DEI TITOLARI E RESPONSABILI DEL TRATTAMENTO:

obbligo di tenere un registro dei trattamenti;
obbligo di adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento;
obbligo di notificare al Garante le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", se è probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati

5. DOMANDE E RISPOSTE

La demonizzazione del mezzo non è la strada giusta ma è importante evidenziare i rischi. Serve spiegare ad esempio ai più piccoli che **quello che condividiamo oggi nella dimensione digitale, rimarrà per sempre**. Se oggi pensiamo di condividere contenuti che ci fanno sentire più fighi o simpatici, qualcosa che magari fa ridere i nostri amici, **in futuro quella stessa foto/video ci potrebbe costare un posto di lavoro o una borsa di studio all'università**.
Non solo. Online non sappiamo chi abbiamo di fronte: intessiamo relazioni con sconosciuti che potrebbero un domani utilizzare quel rapporto in un modo che non vorremmo. E ancora: i nostri volti o video innocenti possono essere trasformati - con una tecnologia chiamata *deepfake* - e appiccicati su video pornografici che non abbiamo scelto di realizzare. **Quel video può distruggere la nostra vita**.



Un'opzione potrebbe essere accordarsi con i genitori per **bloccare alcune funzioni del cellulare negli orari scolastici e lasciarne attive altre**. Tecnologicamente è possibile.

Si può valutare quali funzioni di questi strumenti distraggono e quali invece possono invece essere utilizzate perché funzionali all'attività formativa.

In alternativa si possono prevedere strumenti scolastici (come biblioteche digitali o device della scuola) che i ragazzi conoscono e possono utilizzare in classe per alcune attività.

2

Cyberbullismo e Revenge Porn

1. GLI INTERVENTI DEGLI ESPERTI

Cyberbullismo e revenge porn sono fenomeni gravi e diffusi che in molti casi possono riguardare i minori. È importante capire quali meccanismi psicologici li determinino e a quali segnali prestare maggiore attenzione.
Ci aiuta la dottoressa **Flaminia Bolzan**, psicologa e criminologa.

Partiamo dal contesto: i social sono il luogo in cui i ragazzi ottengono gratificazione dai "like" ricevuti. Quando si compie un atto di cyberbullismo o revenge porn **le motivazioni possono essere diverse: vendetta, superficialità, goliardia, desiderio di "ricompensa" o di apprezzamento** da parte della community online. Non sempre chi condivide una foto/un video sessualmente esplicito, ad esempio, lo fa spinto da una "volontà" reale: può non sentirsi in grado di dire di no perché ha paura di non essere accettato. Il lavoro educativo serve anche a individuare queste situazioni.

Riconoscere uno studente "bullo" nella vita reale accende un dubbio sulla possibilità che lo sia anche online. Meno ovvio è scoprire invece che **chi bullizza nella realtà potrebbe essere una vittima in rete**.

CYBERBULLISMO: UN'AZIONE SEMPRE AGGRESSIVA E INTENZIONALE

Il cyberbullismo possiede caratteristiche specifiche che lo distinguono dal bullismo:

- **gli attori sono indefiniti** (un account potrebbe celare chiunque), mentre nel bullismo si agisce di persona;
- online **possono essere coinvolte persone da tutto il mondo**. Viceversa nel contesto reale i bulli fanno solitamente parte di un gruppo specifico;
- il cyberbullismo **non ha limiti di spazio né di tempo**, mentre in presenza si bullizza in un dato luogo e per un periodo limitato (ad esempio durante le ore scolastiche);
- nel cyberspazio chiunque può **modificare la propria personalità** esasperando o inventando del tutto alcuni aspetti, **come l'età**.

ONLINE IL BULLO "NON VEDE" LA SUA VITTIMA

Elemento centrale del cyberbullismo: **niente contatto, niente empatia**. In questo modo si riducono anche le inibizioni.
Le interazioni, inoltre, **non avvengono necessariamente in tempo reale** quindi non è necessario fronteggiare immediatamente la reazione dell'altro.

PER GLI ADOLESCENTI L'IMMAGINE SOCIALE È IMPORTANTE

Se questa viene intaccata, l'impressione è quella di subire conseguenze molto gravi. Gli adulti - insegnanti e genitori - devono quindi offrire loro strumenti utili **a normalizzare gli esiti dei comportamenti subiti**, ridimensionando quella che si percepisce come una catastrofe, **senza però sminuire la gravità del gesto** subito.
È un equilibrio molto difficile ma necessario.

PER AIUTARE I RAGAZZI I DIVIETI NON BASTANO

A volte imporre una regola senza spiegarla spinge gli adolescenti a infrangerla volontariamente. La voglia di rispettarla emerge solo quando si percepisce il **beneficio** che ne deriva. Ad esempio, la riduzione dell'ansia: non dovrò preoccuparmi della sanzione se mi attengo alla regola. Nello stabilire la norma è necessario farne capire le ragioni e dare ai ragazzi la possibilità di **manifestare il proprio dissenso** a parole. Se non viene concesso loro questo spazio, il rischio è che passino direttamente all'azione.

I FATTORI SU CUI FARE LEVA CON I RAGAZZI

empatia: la capacità di mettersi nei panni dell'altro;
monitoraggio dell'utilizzo dei mezzi digitali (operato dalla famiglia e dalla scuola);
contesto (scolastico e familiare) percepito come sicuro, caratterizzato dal rispetto, dalla gentilezza e dall'assenza di pericoli.

ATTORI CHIAVE: LE PIATTAFORME

Nella battaglia contro i reati commessi online giocano un ruolo fondamentale anche le piattaforme. La policy di Google, come spiega **Martina Colasante**, vieta la presenza di contenuti pericolosi. Eppure, viste le caratteristiche della rete (pensate ad esempio a YouTube, una piattaforma aperta su cui vengono caricate circa **500 ore di contenuti al minuto**), a volte riescono a penetrare anche materiali illegittimi e dannosi.

COME AGISCE GOOGLE PER CONTRASTARE (ANCHE) I CONTENUTI LEGATI A CYBERBULLISMO E REVENGE PORN?

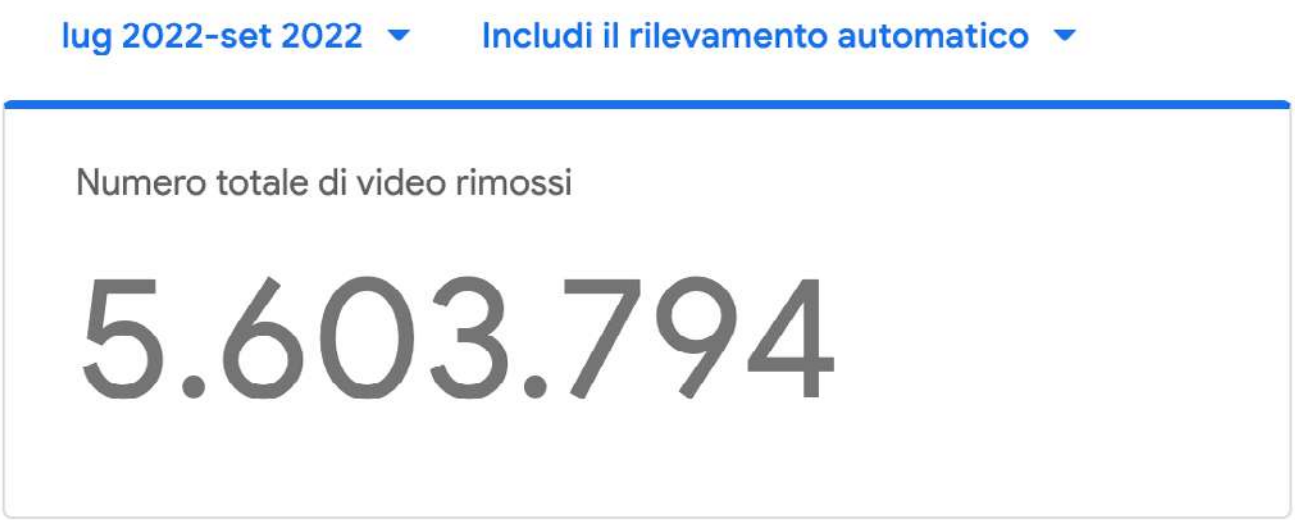
Impossibile prevedere una squadra di persone che analizzi, uno ad uno, minuto per minuto, tutti i contenuti caricati online. Che fare allora?

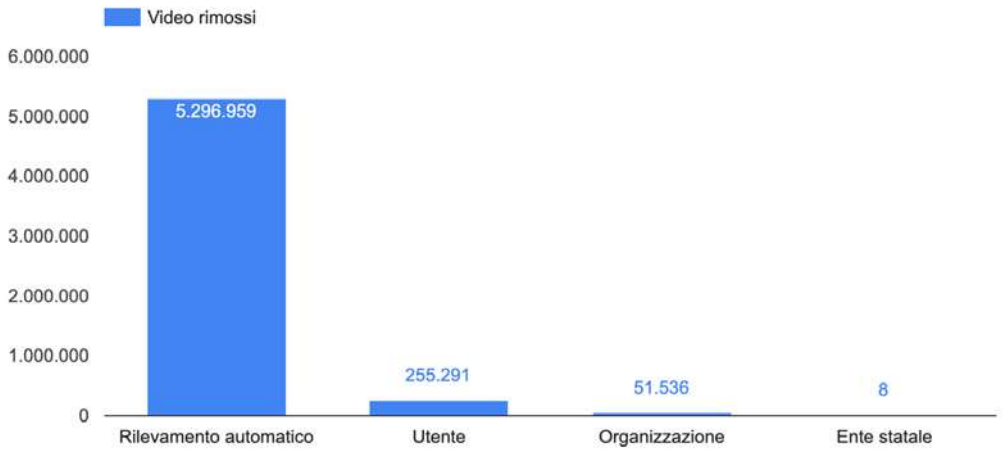
1. RIMUOVERE

il più velocemente possibile i contenuti che violano la policy (la lista comprende bullismo e cyberbullismo, violenza, incitamento a commettere atti pericolosi, truffa, spam, nudo, revenge porn, ecc.). Come si individuano?

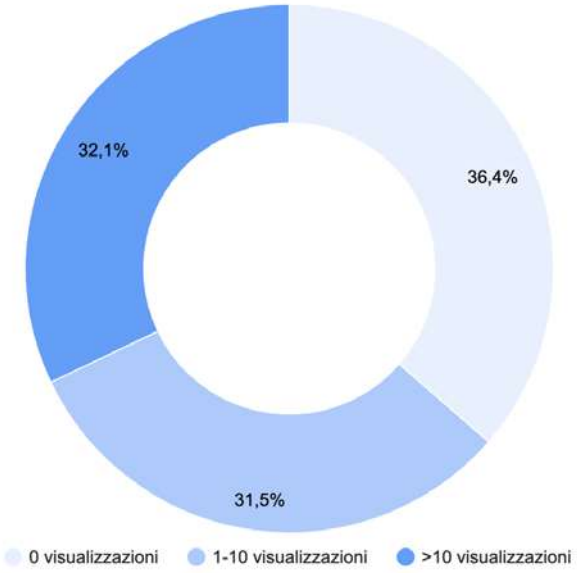
Segnalazioni degli utenti. Tutti (anche voi!) possono segnalare contenuti;
segnalazioni di soggetti autorevoli che conoscono bene il contesto (istituzioni, ong, accademici, forze di polizia, Garante della Privacy), sono in grado di distinguere tra un contenuto divertente e uno abusivo, hanno a disposizione strumenti per segnalazioni molto rapide;
tecnologia: gli algoritmi permettono di individuare ciò che viola la policy. Sono molto efficaci, ad esempio, per nudo e pornografia, meno su altri contenuti, ma si lavora per migliorarli.

Youtube ogni tre mesi realizza un report sui contenuti rimossi. Da luglio a settembre 2022, ad esempio, sono stati rimossi oltre 5,6 milioni di video.
Di questi, la grande maggioranza (**quasi il 95%**) è stata individuata dagli algoritmi.





E **quasi il 68% è stato visualizzato da 0 ad un massimo di 10 volte**. L'obiettivo della piattaforma è proprio questo: arrivare a rimuovere tutti i video **PRIMA che vengano visualizzati** anche una sola volta.



2. DARE VISIBILITÀ A CONTENUTI AUTOREVOLI

Caricati, ad esempio, da testate giornalistiche, fonti istituzionali o di governo.

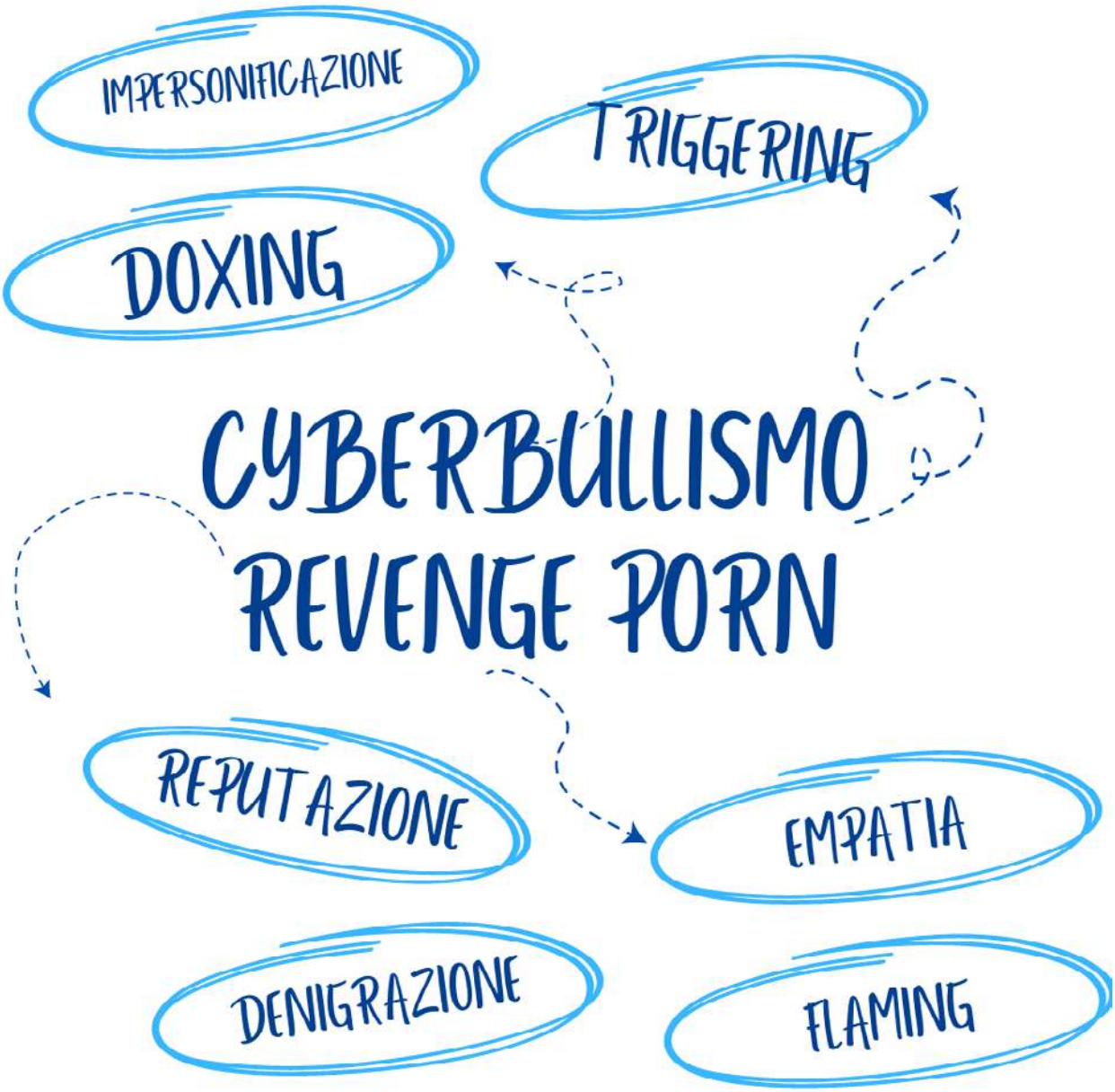
3. RIDURRE I MATERIALI "BORDERLINE"

Non del tutto illeciti ma che potrebbero urtare la sensibilità di alcuni. Google non rimuove questi materiali ma non li promuove.

4. REMUNERARE I CREATOR PIÙ AFFIDABILI

Con l'obiettivo di fidelizzare i creatori di contenuti di maggiore qualità e che non hanno mai violato le norme della community.

2. LE PAROLE (CHIAVE) SONO IMPORTANTI



CYBERBULLISMO: l'insieme di azioni aggressive e intenzionali di una singola persona o di un gruppo realizzate mediante strumenti elettronici (sms, foto, video, email, chat, instant messaging, siti web, telefonate), il cui obiettivo è quello di provocare danni alla propria vittima.

REVENGE PORN: Diffusione in rete di immagini sessualmente esplicite senza il consenso del soggetto ritratto. Spesso la vittima è donna e l'obiettivo è denigrare l'ex partner.

FLAMING: l'offesa, spesso volgare, fatta sui social o nei forum online. Il cyberbullo, in questo caso, cerca di zittire la sua vittima ricoprendola di insulti.

IMPERSONIFICAZIONE: l'atto di fingersi qualcun altro online, cambiando la propria identità, età, ma anche gli aspetti del proprio carattere, per ingannare o bullizzare altre persone.

TRIGGERING: ottenere la fiducia di qualcuno per poi ingannarlo.

DOXING: diffondere in internet dati sensibili o documenti personali di altri.

REPUTAZIONE (ONLINE): è legata all'immagine sociale che ognuno di noi si costruisce in rete.

DENIGRAZIONE: l'atto di denigrare un'altra persona online è legato all'"immagine sociale" che per i più giovani ha un enorme valore. Vedere distrutta la propria immagine online può risultare insostenibile per la vittima.

EMPATIA: è la capacità di mettersi nei panni dell'altro, totalmente assente nei casi di cyberbullismo, dove manca l'interazione diretta tra bullo e vittima. La stessa empatia è invece fondamentale nel rapporto adulto-minore proprio per combattere questi fenomeni.

3. DIRITTI E DOVERI

Dopo aver esaminato il punto di vista psicologico e quello pratico/tecnologico, è bene tenere a mente anche gli aspetti giuridici di questi fenomeni.

Sul cyberbullismo l'approccio della legge del 2017 è **più educativo che repressivo**. Si tratta di una normativa che non aggiunge fattispecie ulteriori ma rinvia a norme già presenti nel Codice penale per sanzionare comportamenti di per sé illeciti come la diffamazione (art. 595 c.p.), lo stalking (art. 612-bis c.p.), le molestie (art. 660 c.p.), il furto d'identità (art. 640-ter c.p.), il trattamento illecito di dati (art. 167, d.lgs. n. 196/2003).

L'art. 2 prevede la possibilità per ciascun **minore di età superiore ai quattordici anni** che sia stato vittima di cyberbullismo, nonché per i genitori e per chi esercita la responsabilità sul minore, di **rivolgersi al titolare del trattamento di dati online o al gestore di un sito internet o di un social media per ottenere "l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso in rete"**.

Il destinatario della segnalazione dovrà **attivarsi tempestivamente**, comunicando entro **24 ore** la presa in carico dell'istanza e provvedendo entro **48 ore** all'oscuramento, alla rimozione o al blocco richiesto.

In caso di inerzia del soggetto o in caso di impossibilità a individuare il titolare del trattamento o il gestore del sito o del social, gli interessati potranno **rivolgersi direttamente al Garante per la protezione dei dati personali**, che nelle successive **48 ore** solleciterà l'adozione di provvedimenti da parte del gestore oppure (più verosimilmente data l'urgenza) disporrà direttamente il blocco dei dati.

L'art. 7 della legge estende inoltre al fenomeno del cyberbullismo la misura dell'**ammonimento del questore** già prevista per il reato di stalking. **Fino a quando non è proposta querela o non è presentata denuncia**, il questore al quale siano stati segnalati gli episodi di cyberbullismo può convocare il minore individuato come autore, alla presenza di almeno un genitore o tutore, per ammonirlo e invitarlo a "tenere una condotta conforme alla legge".

Va infine segnalato il dovere per il dirigente scolastico che venga a conoscenza di atti di cyberbullismo di informare le famiglie dei minori coinvolti, attivando contemporaneamente azioni di carattere educativo ed eventualmente adottando anche provvedimenti disciplinari nei confronti degli autori di tali condotte.

LEGGE 69 DEL 2019 SUL REVENGE PORN:

Attraverso l'introduzione dell'art. 612-ter c.p. da parte della legge 69/2019 si intende tutelare in primis **la libertà di autodeterminazione della persona**.

È punito con la reclusione da uno a sei anni e con la multa da 5.000 a 15.000 euro chiunque, dopo averli realizzati o sottratti, **invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate**.
La stessa pena si applica a chi, avendo **ricevuto o comunque acquisito** le immagini o i video, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate.

La pena **è aumentata** se i fatti sono commessi dal coniuge o **da persona che è o è stata legata da relazione affettiva alla persona offesa o se i fatti sono commessi attraverso strumenti informatici o telematici**.
La pena è aumentata anche se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o di una donna in stato di gravidanza.
Il delitto è punito **a querela** della persona offesa (entro **sei mesi**).

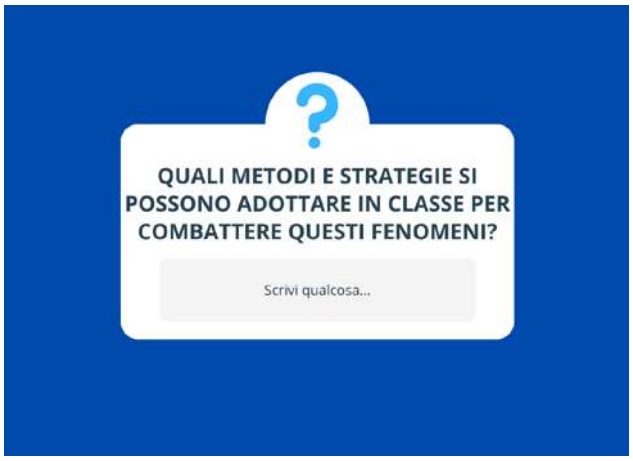
Ma **il diritto da solo non basta**: è fondamentale una collaborazione con i **soggetti istituzionali e le piattaforme**.

Ne è un esempio la procedura di *notice and take down* prevista dall'**art. 144-bis del Codice privacy**. Secondo questa procedura chiunque (anche i minori con più di 14 anni o i genitori o i tutori) abbia fondato motivo di ritenere che registrazioni audio o video o altri documenti a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso, può segnalare il pericolo al Garante per la protezione dei dati personali, il quale, entro 48 ore, decide il da farsi.

Per segnalare il pericolo di revenge porn, è possibile utilizzare l'apposito form presente nel sito del Garante, in cui dovranno essere indicate le piattaforme (social network, messaggistica, ecc.) attraverso le quali si teme la diffusione, nonché le motivazioni.

Dovranno poi essere trasmesse all'Autorità – tramite un link che sarà comunicato dopo la presentazione della segnalazione – le immagini o i contenuti sessualmente espliciti dalla cui divulgazione ci si intenda tutelare.
Il Garante potrà quindi adottare un provvedimento che sarà notificato alle piattaforme coinvolte nel tentativo di contrastare la diffusione.

4. DOMANDE E RISPOSTE



Lavorare in piccoli gruppi: la possibilità di lavorare in piccoli sottogruppi (max 10 persone), che possano comunque essere eterogenei, permette di lasciare più spazio ai ragazzi per esprimere le loro considerazioni e soprattutto per supportarli nella gestione delle emozioni. Un lavoro di questo tipo, strutturato in più momenti, favorisce un clima di collaborazione e stimola la partecipazione.

Utilizzare questionari anonimi: si possono distribuire e far compilare alla classe per sondare la situazione. Ci si può basare su esempi già realizzati oppure crearne di nuovi. In fondo al capitolo troverete un fac simile sviluppato come adattamento dal questionario per la rilevazione del bullismo di Olweus. Sulla falsariga di questo è possibile svilupparne di nuovi che includano domande del medesimo tenore, magari più specifiche rispetto alle esigenze della classe. Sarebbe opportuno somministrare questi questionari trimestralmente per indagare e monitorare la situazione e il relativo andamento.

Peer education: educazione tra pari. È una metodologia importante e da utilizzare. È necessario conoscere molto bene i propri studenti e individuare, nel gruppo, chi siano i più rappresentativi, i leader. Saranno loro a farsi promotori della trasmissione di informazioni e competenze. Da notare: i leader della classe hanno generalmente caratteristiche diverse rispetto a quelli di un'azienda. Non sempre il "bulletto" è anche il leader, anzi, negli ultimi anni i punti di riferimento della classe possiedono sempre più spesso caratteristiche positive.

Tre esempi:

Wonder (libro e film): Auggie, nato con una rara malattia, si trova ad affrontare la scuola per la prima volta. L'amore della sua famiglia e una grande dose di coraggio lo aiutano a trovare il suo posto nel mondo e nel cuore dei compagni di classe.
Clickbait (serie tv): la vicenda ha inizio nel momento in cui su internet viene caricato un video/clickbait in cui un uomo, Nick Brewer, marito e padre affettuoso, mostra un cartello su cui ha scritto: "Io abuso delle donne. A 5 milioni di visualizzazioni morirò". Tutti si chiedono se si tratti di un fake o se il video sia vero. L'unica cosa certa è che le visualizzazioni si moltiplicano di secondo in secondo e la vita di Nick sembra appesa a un filo. Nick non risponde al telefono, i detective iniziano a indagare e l'immagine di marito e padre perfetto piano piano si frantuma in seguito alla scoperta di particolari segreti sulla sua vita. Il pubblico scatena tutta la sua cattiveria sul web. Ma dove sta la verità? Nick è morto in seguito ai cinque milioni di visualizzazioni o è ancora vivo?
Tredici (serie tv): il suicidio della diciassettenne Hannah Backer sconvolge l'intera comunità scolastica e in particolare Clay Jensen che entra in possesso di tredici cassette registrate in cui Anna spiega quali siano stati i motivi e le persone che l'hanno portata all'estremo gesto. Nel corso delle stagioni la serie mette in risalto la necessità di parlare di questi argomenti e di insegnare ai ragazzi vittime di bullismo come affrontare la situazione.

QUESTIONARIO DI RILEVAZIONE DI ATTI DI BULLISMO

PARTE 1. I RAPPORTI CON LA SCUOLA E I TUOI COMPAGNI

Sei un maschio o una femmina?

- ☐ Maschio
- ☐ Femmina
- ☐ Altro/preferisco non rispondere

Ti piace la scuola?

- ☐ Non mi piace per niente
- ☐ Non mi piace
- ☐ Mi è indifferente
- ☐ Mi piace
- ☐ Mi piace molto

Quanti amici hai in classe?

- ☐ nessuno
- ☐ 1
- ☐ 2 o 3
- ☐ 4 o 5
- ☐ 6 o più

Sei soddisfatto del tuo rapporto con gli insegnanti? (1 risposta)

- ☐ molto
- ☐ abbastanza
- ☐ indifferente
- ☐ poco
- ☐ per niente

Quale momento preferisci trascorrere con i compagni di classe? (1 risposta)

- ☐ La ricreazione
- ☐ Il tempo libero fuori da scuola
- ☐ Le lezioni
- ☐ Nessun momento

Ti accade di restare solo perché nessuno dei tuoi compagni vuole stare con te?

- ☐ Sì, durante la ricreazione
- ☐ Sì, mi lasciano sempre solo
- ☐ Sì, durante le lezioni
- ☐ No, sto sempre con gli altri ragazzi

Quante volte ti sei sentito escluso o ignorato?

- ☐ mai
- ☐ una o 2 volte
- ☐ 2 o 3 volte al mese
- ☐ circa una volta alla settimana
- ☐ Più volte al mese

Sei stato picchiato, maltrattato, spinto?

- ☐ mai
- ☐ una o 2 volte
- ☐ 2 o 3 volte al mese
- ☐ circa una volta alla settimana
- ☐ Più volte al mese

Le tue cose (materiale scolastico, lo zaino, altro) sono state maltrattate o sono sparite?

- ☐ mai
- ☐ una o 2 volte
- ☐ 2 o 3 volte al mese
- ☐ circa una volta alla settimana
- ☐ Più volte al mese

Qualcuno ha diffuso voci false e offensive sul tuo conto?

- ☐ mai
- ☐ una o 2 volte
- ☐ 2 o 3 volte al mese
- ☐ circa una volta alla settimana
- ☐ Più volte al mese

Sei stato minacciato o forzato a fare cose che non volevi?

- ☐ mai
- ☐ una o 2 volte
- ☐ 2 o 3 volte al mese
- ☐ circa una volta alla settimana
- ☐ Più volte al mese

Ti hanno affibbiato nomignoli o fatto commenti sulla tua persona che ritieni offensivi?

- ☐ mai
- ☐ una o 2 volte
- ☐ 2 o3 volte al mese
- ☐ circa una volta alla settimana
- ☐ Più volte al mese

CONTINUA A RISPONDERE ALLE DOMANDE CONTENUTE NELLE SUCCESSIVE PARTI DEL QUESTIONARIO SOLO SE RITIENI DI ESSERE STATO VITTIMA DI ATTI DI BULLISMO O CYBERBULLISMO O PENSI DI AVER ASSISTITO AD ATTI DI BULLISMO COMPIUTI NEI CONFRONTI DEI TUOI COMPAGNI.

GRAZIE PER LA TUA COLLABORAZIONE!

PARTE 2. SEI STATO VITTIMA DI ATTI DI BULLISMO

RISPONDI A QUESTE DOMANDE SOLO SE PENSI DI ESSERE STATO VITTIMA DI BULLISMO O CYBERBULLISMO (esclusione, offese, minacce ripetute) ALTRIMENTI PASSA ALLA PARTE 3.

Quali dei seguenti mezzi sono stati usati per offenderti?

- ☐ WhatsApp
- ☐ Facebook
- ☐ Instagram
- ☐ TikTok
- ☐ Altro:

In quale classe si trovano gli studenti che hanno compiuto atti di bullismo?

- ☐ Nella mia
- ☐ Non nella mia ma in una della stessa scuola
- ☐ Ho paura di scriverlo
- ☐ Non si trovano in questa scuola

Sei stato vittima di bullismo da parte di maschi o femmine?

- ☐ Principalmente da una ragazza
- ☐ Da più ragazze
- ☐ Principalmente da un maschio
- ☐ Da più maschi

Da quanti studenti?

- ☐ 2-3
- ☐ 4 o più

Per quanto tempo?

- ☐ 1 o 2 settimane
- ☐ circa un mese
- ☐ 2-3 mesi
- ☐ lo scorso anno scolastico

In quali luoghi?

- ☐ in classe
- ☐ nel corridoio
- ☐ nei bagni
- ☐ in palestra
- ☐ nel pullman scolastico
- ☐ in internet

In quali momenti?

- ☐ durante l'intervallo
- ☐ durante il cambio dell'ora
- ☐ durante la lezione
- ☐ prima o dopo la scuola
- ☐ altri

Quando qualcuno se la prende con te, tu... (1 sola risposta)

- ☐ Mi sforzo di rispondere
- ☐ Cerco aiuto tra i miei compagni o le mie compagne
- ☐ Vorrei reagire, ma ho troppa paura
- ☐ Spero che qualcuno si accorga di come mi sento
- ☐ Cerco di capire perché se la prende con me

Secondo te i tuoi compagni e le tue compagne... (1 sola risposta)

- ☐ Si divertono
- ☐ Gli dispiace per me, ma hanno paura di intervenire
- ☐ Mi disprezzano perché sono il più debole
- ☐ Sono dalla mia parte
- ☐ Se ne fregano di me e di come posso sentirmi

Ne hai parlato con qualcuno?

- ☐ con un amico
- ☐ con i genitori
- ☐ con una sorella/un fratello
- ☐ con un docente
- ☐ con nessuno

PARTE 3. SEI STATO SPETTATORE DI ATTI DI BULLISMO

COMPLETA QUESTA PARTE SOLO SE HAI ASSISTITO AD ATTI DI BULLISMO, ALTRIMENTI PASSA ALLA PARTE 4.

Hai assistito ad atti di bullismo negli ultimi due mesi?

- ☐ mai
- ☐ una o 2 volte
- ☐ 2 o 3 volte al mese
- ☐ circa una volta alla settimana
- ☐ Più volte al mese

Che tipo di atti?

- ☐ Colpi
- ☐ offese
- ☐ furti
- ☐ minacce
- ☐ non rivolgere la parola
- ☐ storie sul conto altrui
- ☐ esclusione dai giochi

In quali luoghi?

- ☐ in classe
- ☐ nel corridoio
- ☐ nei bagni
- ☐ in palestra
- ☐ nel pullman scolastico
- ☐ in internet

In quali momenti?

- ☐ durante l'intervallo
- ☐ durante il cambio dell'ora
- ☐ durante la lezione
- ☐ prima o dopo la scuola
- ☐ altri:

Ne hai parlato con qualcuno?

- ☐ con un amico
- ☐ con i genitori
- ☐ con una sorella/un fratello
- ☐ con altri familiari (nonni, zii)
- ☐ con un insegnante
- ☐ con nessuno

Questi atti di bullismo o cyberbullismo colpiscono un ragazzo o una ragazza della tua scuola?

- ☐ Si
- ☐ No

Chi ha compiuto atti di bullismo o cyberbullismo frequenta la tua scuola?

- ☐ Si
- ☐ No

Quando qualcuno fa il bullo, i compagni... (al massimo 2 risposte)

- ☐ Si divertono e fanno il tifo per il bullo
- ☐ Cercano di aiutare il più debole
- ☐ Sono spaventati
- ☐ Lasciano da solo il bullo
- ☐ Fanno finta di niente
- ☐ Escludono dal gruppo chi è vittima

Qual è il tuo atteggiamento nei confronti di chi subisce prepotenze? (1 sola risposta)

- ☐ Lo prendo un po' in giro
- ☐ Nei momenti di calma cerco di dargli una mano
- ☐ Penso si meriti di essere trattato così
- ☐ Non fa parte del mio gruppo e non mi interessa
- ☐ Faccio finta di niente

Qual è il tuo atteggiamento nei confronti del bullo? (1 sola risposta)

- ☐ Lo ammiro, sa fare il capo e ci fa divertire
- ☐ Sono contento quando si trova in difficoltà
- ☐ Evito tutti i contatti con lui perché ho paura
- ☐ Reagisco apertamente alle sue prepotenze
- ☐ Sono indifferente

Se ti capita di INTERVENIRE, è perché... (1 sola risposta)

- ☐ Il "bullo" se la prende con un mio amico/a
- ☐ I prepotenti non mi piacciono
- ☐ Sono più forte di lui
- ☐ È un problema che ci riguarda tutti
- ☐ Non ho paura di nessuno

Se ti capita di NON INTERVENIRE, è perché... (1 sola risposta)

- ☐ Con me si comporta bene, quindi non sono fatti miei
- ☐ Ho paura di andarci di mezzo
- ☐ Io e la vittima non siamo amici, quindi non mi interessa
- ☐ Ci si deve difendere da soli
- ☐ Non voglio essere escluso dal gruppo

PARTE 4. SE SENTI IL BISOGNO DI CONFIDARTI CON QUALCUNO

Se hai bisogno di aiuto o, semplicemente, senti il bisogno di raccontare la tua storia o quella di altri, puoi raccontarla scrivendo su questo foglio la tua testimonianza.
Se hai bisogno di parlare con qualcuno sappi che i tuoi insegnanti sono pronti ad ascoltarti in privato e possono garantirti la massima discrezione.

3

Dati & pubblicità

1. GLI INTERVENTI DEGLI ESPERTI

I gestori della rete competono per catturare la risorsa fondamentale che fa funzionare il loro modello di business: **la nostra attenzione**. Più tempo passiamo su una pagina e più avranno la possibilità di "**profilarci**": raccogliere i nostri dati, da utilizzare per capire i nostri gusti, le abitudini, le paure, gli stili di vita, e offrirci pubblicità ritagliate su di noi, più capaci di attrarre il nostro click.

È **Guido D'Ippolito**, funzionario dell'Autorità Garante per la protezione dei dati personali, a parlare del rapporto tra i nostri dati e la pubblicità online.

LA PUBBLICITÀ PERSONALIZZATA È IL PRINCIPALE MOTORE CHE FA FUNZIONARE INTERNET: MONOPOLIZZA IL NOSTRO TEMPO E SFRUTTA LE INFORMAZIONI CHE CI RIGUARDANO

Le piattaforme offrono i loro servizi in cambio della nostra attenzione e competono tra di loro per averla: si parla di **mercati dell'attenzione**.

Se osserviamo il funzionamento dei social network, è facile notare i meccanismi: i video (ad esempio su TikTok) partono da soli, la bacheca dei contenuti è potenzialmente infinita, al termine di un contenuto ne vengono suggeriti altri, così come alla fine di un film o di una serie su Netflix.

Così, le piattaforme monetizzano: estraggono valore dai nostri dati e lo offrono agli inserzionisti, ai quali potranno dire non solo **QUANTI** utenti frequentino la loro pagina, ma anche di **CHE TIPO** (giovani, anziani, con quali gusti, con che abitudini di spesa...).

SIAMO NOI CHE USIAMO INTERNET O VICEVERSA?

Se da un lato la profilazione può avere risvolti utili nel suggerirci contenuti e nel semplificare diverse attività (quando è fatta correttamente), bisogna sottolinearne anche i **molteplici rischi**. Si tratta di un enorme trattamento dei dati personali, di un monitoraggio costante e di un'ampia condivisione tra soggetti diversi. Ed è tutto automatizzato: dietro questi meccanismi non c'è un essere umano ma un algoritmo.

LA PUBBLICITÀ PROFILATA INCIDE SULLE SCELTE E SUL MODO DI VEDERE LA REALTÀ

Lo abbiamo già sottolineato nei capitoli precedenti: se l'algoritmo sceglie tutto, sarà lui a decidere per noi. Come essere certi allora che ciò che ha scelto sia davvero la cosa migliore e non solo frutto di un accordo economico? Il rischio di **un'alterazione della scelta** è alto e lo è di più se si tratta di minori, i cui gusti non sono ancora ben formati. Così come il rischio che i dati raccolti per scopi pubblicitari finiscano poi in mani terze: **cedere la conoscenza su noi stessi potrebbe esporci**.

COME CI DIFENDIAMO? IL SEGRETO È IL CONTROLLO

Il primo modo per difenderci è **informarci**. Sappiamo che nessuno legge davvero le informative sulla privacy e questo è un fallimento normativo che purtroppo coinvolge tutti.

Quello che però possiamo fare è (almeno) prestare più attenzione a ciò che clicchiamo quotidianamente. Ad esempio, quando ci appare il banner dei cookie su una pagina internet è importante notare quale **finalità** sia indicata: se leggiamo "finalità pubblicitarie" bisogna controllare chi è il soggetto a cui andranno i nostri dati. Si tratta di terze parti? E chi sono queste terze parti?

In più è necessario fare attenzione alle caselle **pre-spuntate** e ai **dark patterns** (interfaccia ingannevoli fatte apposta per indurre gli utenti ad accettare le condizioni); controllare **quello che chiedono le app** (ad esempio l'accesso a microfono,

fotocamera, geolocalizzazione, contatti rubrica); disabilitare le funzioni o disinstallare **le app non utilizzate**; controllare **con chi vengono condivisi i dati e per quanto tempo vengono conservati** (ad esempio sulle app di dating, quelle per le attività sportive, o per monitorare il ciclo mestruale...)

Dobbiamo in sostanza accertarci di essere noi a (voler) dare il consenso, che deve essere **libero, effettivo, non implicito o presupposto, non forzato, non condizionato, non estorto** (con l'inganno o con l'utilizzo di grafiche).

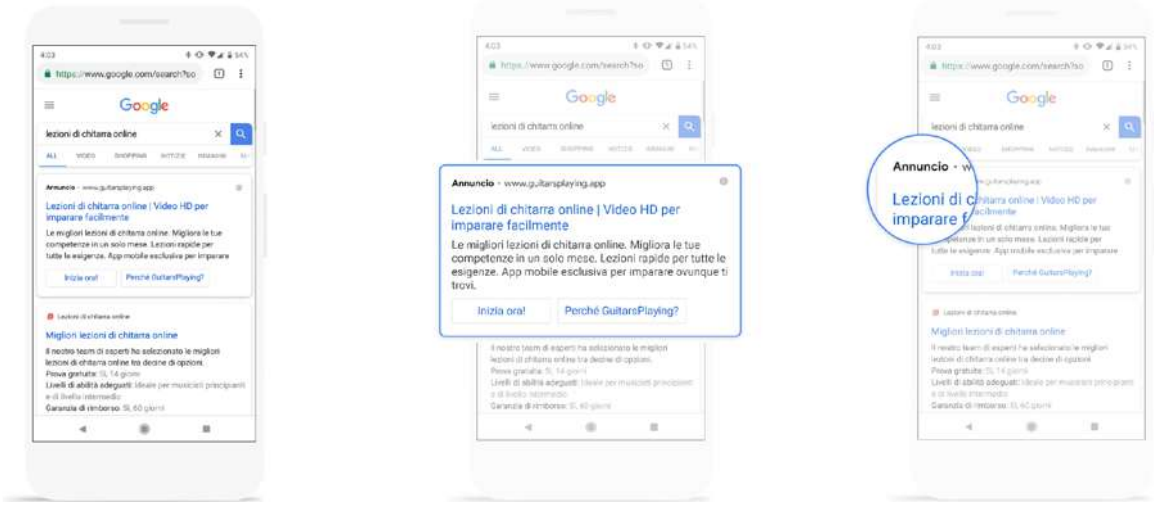
Saranno tendenzialmente **illeciti** quei servizi digitali che non ci chiedono un consenso per l'invio di pubblicità, specie se personalizzata o targettizzata. In questi casi è possibile esercitare la propria opposizione con diversi strumenti:

Tramite le impostazioni offerte dal servizio stesso;
esercitando i diritti garantiti dalla normativa europea "GDPR";
facendo un reclamo al Garante.

LA CHIAVE PER FAR IN MODO CHE LA TECNOLOGIA SMETTA DI ESSERE UNO STRUMENTO DI MANIPOLAZIONE E TORNI AD ESSERE "AMICA": LA CONSAPEVOLEZZA

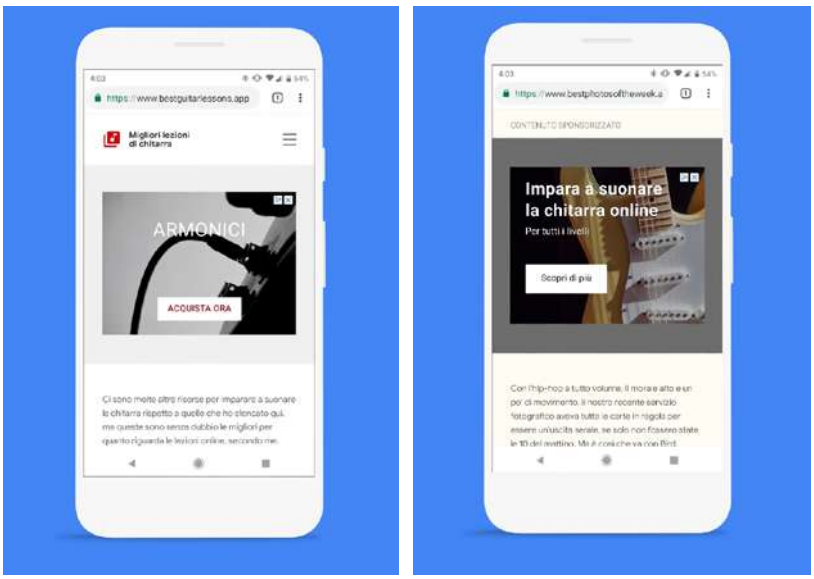
È importante conoscere gli strumenti che le piattaforme ci mettono a disposizione. Ne parla **Martina Colasante**.

Quando svolgiamo una ricerca su Google, ad esempio "lezioni di chitarra online", riceviamo risultati organici (cioè non sponsorizzati) oppure sponsorizzati (pagati) da un inserzionista. Questi ultimi sono segnalati da un'etichetta con la scritta "adv" o "contenuto sponsorizzato" o "annuncio". Se gli utenti scelgono di cliccare su questo contenuto, Google gua-



dagna.
"Questo modello è quello che esiste sin dal principio. Negli ultimi 20 anni Google è cambiato e ha sviluppato molti servizi ma questo tipo di pubblicità corrisponde ancora all'80% dei suoi guadagni", spiega la dottoressa Colasante. "È questo modello che permette a Google e a tutti i siti di essere gratuiti".

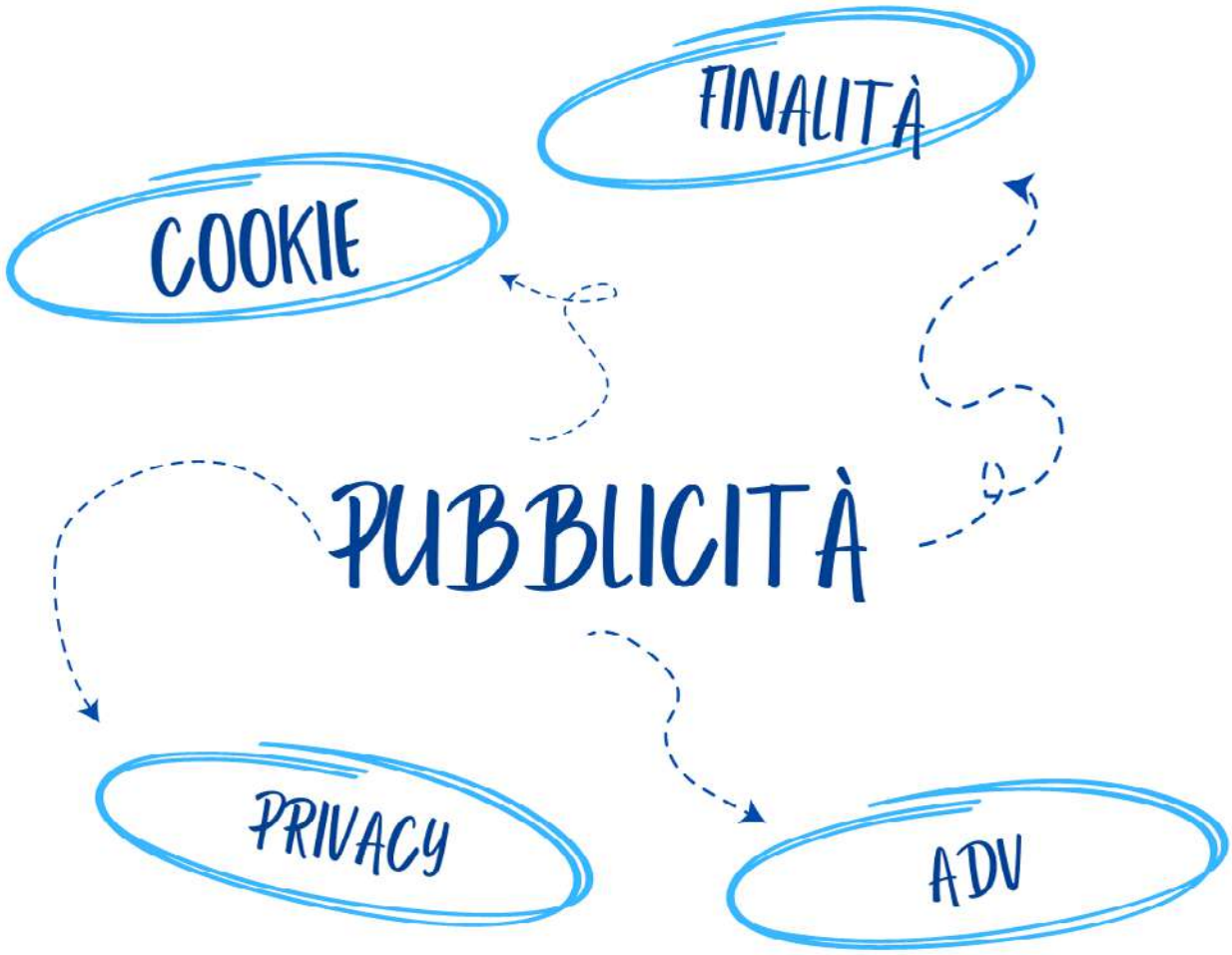
Un altro modo in cui Google guadagna è collaborando con entità partner (creatori di contenuti) per **vendere gli spazi pubblicitari** al loro interno. In un sito che offre lezioni di chitarra potremmo trovare, ad esempio, pubblicità di strumenti musicali.
Oppure, dopo aver visitato quel sito per lezioni di chitarra, potremmo andare su un altro con "le migliori foto del giorno". Entrandoci, potremmo ritrovare la pubblicità delle lezioni di chitarra online. Questo accade perché le nostre ricerche pregresse - e le nostre preferenze - sono state memorizzate (grazie ai cookie) per **offrirci inserzioni inerenti**. In questo modo i siti che ospitano le pubblicità guadagneranno (e se Google fa da mediatore per la vendita tratterà una parte dei ricavi), permettendoci di accedere gratuitamente ai loro contenuti.



È anche possibile che il sito di lezioni di chitarra decida di rivolgersi a un pubblico che la sua pagina non l'ha mai visitata. Qui subentra l'algoritmo di Google e degli altri soggetti che fanno pubblicità. Grazie all'analisi dei comportamenti pregressi, riescono a stimare quali persone con caratteristiche comuni potrebbero essere interessate alle lezioni di chitarra.

Google offre sempre la possibilità di capire perché riceviamo una certa pubblicità: basta cliccare sulla X vicino all'inserzione per sapere **chi è il soggetto che sta pagando** per quella pubblicità, **come mai siamo stati profilati** per riceverla ed eventualmente **decidere di non riceverla più** (una specifica o in generale tutta quella personalizzata). In quest'ultimo caso la pubblicità comparirà comunque nelle pagine che visiterò ma non sarà più personalizzata.

2. LE PAROLE (CHIAVE) SONO IMPORTANTI



PUBBLICITÀ: il contenuto che permette alle piattaforme e ai creatori digitali di sostenersi e mantenere gratuito l'accesso ai propri siti. Può essere "non profilata", e quindi legata solamente alle ricerche che facciamo in quel momento online, oppure "profilata", quindi personalizzata, basata su ciò che la piattaforma sa di noi (età, abitudini, gusti, stili di vita, ...).

COOKIE: frammenti di dati degli utenti, memorizzati e utilizzati (anche) per creare pubblicità personalizzata (si veda nei prossimi paragrafi). I cookie possono essere "di terze parti", cioè creati e gestiti da un sito diverso da quello che stiamo visitando.

FINALITÀ: è importante fare attenzione, nei banner, alle finalità indicate (ad esempio, "pubblicitarie") e a chi siano i soggetti cui andranno i nostri dati.

ADV/SPONSORIZZAZIONE: tra i risultati che otteniamo quando cerchiamo qualcosa online potremmo trovare contenuti inerenti alla nostra ricerca ma pagati dagli inserzionisti/creator digitali. Se clicchiamo, Google ci guadagnerà.

PRIVACY: nelle attività di profilazione online è importante che venga rispettata, tra le altre cose, la privacy degli utenti. È necessario (ma non semplice) trovare un equilibrio tra questa e le esigenze del mercato.

3. DIRITTI E DOVERI

I minori meritano **una specifica protezione** relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia, nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di profilazione (**Considerando 38, Regolamento UE 2016/679 - GDPR, General Data Protection Regulation**).

Costituisce **una pratica commerciale scorretta** quella con cui un inserzionista include in un messaggio pubblicitario un'esortazione diretta ai bambini affinché acquistino o convincano i genitori o altri adulti ad acquistare loro i prodotti reclamizzati (**Direttiva 2005/29/CE**).

I fornitori di piattaforme online non possono presentare sulla loro interfaccia una **pubblicità basata sulla profilazione** (come definita all'articolo 4, punto 4, del regolamento UE 2016/679) che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore (**art. 28, Regolamento UE 2022/2065**)

Le piattaforme digitali devono **richiedere un consenso esplicito ai propri utenti** per trattare i loro dati personali al fine di profilarli e poter così offrire loro anche della pubblicità targettizzata (**Pronuncia Garante privacy irlandese contro Meta, 31 dicembre 2022**).

I cinque principi di correttezza per l'advertising online rivolto ai minori (**Studio 2022 Commissione europea**):

Le vulnerabilità dei bambini dovrebbero essere prese in considerazione dai fornitori di servizi nel momento della progettazione della pubblicità o dell'ideazione di tecniche di marketing che potrebbero essere viste da bambini.
La particolare vulnerabilità dei bambini a causa della loro età o credulità **non può essere sfruttata** dai fornitori di servizi.
Quando l'advertisement è rivolto ai bambini o è probabile che sia visto da loro, la finalità di marketing **dovrebbe essere indicata in modo chiaro e comprensibile per i bambini**.
I bambini **non devono essere destinatari** di annunci tailor-made, o sollecitati all'acquisto di contenuti in-app o in-game. I giochi commercializzati gratuitamente non dovrebbero richiedere acquisti in-app o in-game per un'esperienza d'uso soddisfacente.
I bambini **non devono essere profilati** per scopi pubblicitari.

4. DOMANDE E RISPOSTE

Si chiamano cookie tutte quelle parti di codice che descrivono il modo in cui ci comportiamo online. Quando visitiamo un sito, diamo (o no) il consenso alla raccolta dei cookie per fini pubblicitari oppure lo concediamo solo a quelli essenziali (raccolti per ragioni di sicurezza, per la verifica di comportamenti malevoli, etc ...).

Quando diamo il consenso, i cookie vengono automaticamente iscritti nel browser e rimangono salvati in un luogo specifico (sempre accessibile e cancellabile).

I cookie comunque sono solo il più famoso degli strumenti che permettono di tracciare gli utenti. Ci sono altri sistemi che lo fanno. È importante cancellare (attraverso le funzioni che offre, ad esempio, Google) non soltanto il cookie in sé ma l'informazione registrata.

Per quanto riguarda la pubblicità online, è importante trovare un (non facile) **equilibro tra il diritto alla privacy degli utenti e quello di impresa delle piattaforme**.

Il principio cardine che il mercato deve rispettare è **la libertà di scelta**. Gli utenti devono poter scegliere se e quale pubblicità ricevere, senza **condizionamenti**. Sono da stigmatizzare, infatti, tutti quei comportamenti di influencer che sponsorizzano prodotti senza rendere noto che si tratti di pubblicità, ingannando così gli utenti che tendono a fidarsi di un consiglio (non) disinteressato.

Fondamentale è infine il tema della sicurezza, sia per gli utenti sia per gli inserzionisti. Le pubblicità devono rispettare **canoni** precisi: nel 2022, ad esempio, Google ha rimosso oltre 6 miliardi di pubblicità perché rappresentavano rischi o non rispettavano standard qualitativi.

4

Le regole di Internet

1. GLI INTERVENTI DEGLI ESPERTI

Partiamo da due dati: 45 milioni di italiani hanno una connessione internet e il 120% della popolazione italiana possiede un cellulare. Cosa significa questo?

LA PRESENZA DELLE PIATTAFORME DIGITALI NELLE NOSTRE VITE È UN DATO DI FATTO.

"Non possiamo negare la digitalizzazione. Dobbiamo affrontarla, consapevoli che si tratta di un terreno in gran parte sconosciuto che suscita curiosità ma anche paura, soprattutto a chi non è più giovanissimo". Lo sottolinea il dottor Francesco Nicodemo, esperto di comunicazione strategica e innovazione nonché fondatore di Lievito Consulting.

Possiamo regolare la rete? Non del tutto.

"La regolamentazione di internet oggi sostanzialmente non esiste. Esistono normative di settore ma regolare in toto un sistema così ampio e complesso è impossibile", ci avverte il professor Falletta.
Ancora una volta però è la conoscenza (dei meccanismi di internet) a venirci in soccorso.
In passato il sistema comunicativo prevedeva alcune fonti (giornali, tv) che parlavano a tante persone: il cosiddetto sistema "**one to many**". Noi, in quanto fruitori, ricevevamo quel messaggio (spesso unico) senza poter interagire o rispondere.

Ora ci troviamo al contrario in un sistema "**many to many**": grazie alla rete, la produzione e la distribuzione dei contenuti non è più verticale e unidirezionale, ma orizzontale e circolare. Siamo potenzialmente tutti fonti informative perché possiamo scrivere un post, condividere una notizia, inoltrare un messaggio, pubblicare un video. I contenuti non sono più unici e condivisi da tutti, sono molteplici, così come le fonti.

Si tratta di un sistema rivoluzionario che comporta grandi potenzialità ma anche qualche rischio.

IL SISTEMA "MANY TO MANY" GENERA UN "OVERLOAD" (SOVRACCARICO) INFORMATIVO

Riceviamo costantemente una quantità di dati immensa e difficile da elaborare.

Un primo grande rischio di questo sistema è la presenza di **fake news** e di **disinformazione** online. Non sempre è semplice dare una definizione chiara di questi fenomeni, spesso influenzati dal meccanismo della **polarizzazione** (che sui social funziona benissimo) e della **propaganda** politica.

Come possiamo quindi aiutare i ragazzi a capirci qualcosa e a "difendersi"? Quali strumenti possediamo?

La soluzione "giuridica" (norme e regolamenti) ha dei limiti: arriva dopo che i fatti sono già accaduti e rischia di essere desueta rispetto al problema, sempre nuovo, che si crea. Inoltre, regolare attraverso il diritto fenomeni che hanno a che fare con la libertà di espressione può rivelarsi inutile e anche pericoloso.

Si tratta di un sistema rivoluzionario che comporta grandi potenzialità ma anche qualche rischio.

LA SOLUZIONE "EDUCATIVA/POLITICA" È LA PIÙ EFFICACE E IMPORTANTE

Insegnare ai ragazzi come funzionano i sistemi e trasmettere loro la capacità di lettura critica dei media è un elemento primario.

Altro metodo fondamentale è l'utilizzo dei corpi intermedi (cioè le strutture collettive) che hanno la funzione di educare all'utilizzo di questo sistema.
Ma viene da chiedersi: il diritto deve quindi restare in disparte rispetto a tutto ciò che accade in rete? No. Anche se oggi non è ancora chiaro, come lo era un tempo, quale sarà il ruolo che dovrà ricoprire.

La funzione del diritto è quella di anticipare i comportamenti, attraverso norme generali e astratte. Ma come immaginare oggi tutto ciò che avverrà, ad esempio, con l'intelligenza artificiale? Basti pensare che non esiste, al momento, alcuna norma su questo tema, né a livello italiano né europeo.

Per affrontare il dilemma, la risposta data finora, soprattutto in sede europea, è stata applicare un principio di realtà:

L'EGEMONIA SUL WEB NON È NÉ DELLA POLITICA NÉ DEL DIRITTO MA DELLE GRANDI MULTINAZIONALI

Sono loro a decidere come funzionano le piattaforme, come viene orientato il dibattito pubblico e verso quale progresso.

Stabilito questo, è facile capire perché si sia deciso di coinvolgerle nella stesura delle regole di internet. L'Unione Europea ha introdotto negli anni una serie di atti (libri bianchi, raccomandazioni, codici di condotta) che sono stati scritti insieme alle grandi piattaforme e che hanno contribuito a migliorare il "clima" digitale (le piattaforme sanno che mantenere la loro reputazione è importante per evitare che gli utenti vadano altrove).

Ciò su cui ci si interroga di più è però la possibilità di delegare completamente le decisioni alle piattaforme. È giusto far decidere a loro i confini della libertà di espressione, cedendo - di fatto - un potere pubblico? Non esiste una risposta giusta ma è chiaro che le istituzioni al momento non hanno le risorse per affrontare da sole, esaurientemente e tempestivamente, tutte le attività che si svolgono in rete.

2. LE PAROLE (CHIAVE) SONO IMPORTANTI

REGOLE: stabilire delle regole definitive in un campo, come quello di internet, così vasto e imprevedibile è sostanzialmente impossibile. Ciò che si può fare è collaborare con chi detiene il potere più grande online (le piattaforme) e soprattutto puntare sulla conoscenza. Capire, spiegare, educare: queste sono le "armi" più efficaci.

OVERLOAD INFORMATIVO: la quantità di informazioni che riceviamo (e contribuiamo a diffondere) ogni giorno da e tramite internet è ampissima. Questo genera un sovraccarico informativo nel quale dobbiamo imparare a muoverci.

DISINFORMAZIONE: in questa grande quantità di informazioni non è raro imbatterci anche in notizie false, del tutto o in parte. Dobbiamo esserne consapevoli per poterci difendere, consci del fatto che l'educazione è sempre la strategia migliore.

POLARIZZAZIONE: dividersi in gruppi a seconda di opinioni su argomenti o notizie è un meccanismo che funziona molto bene sui social, dove la costruzione di comunità con posizioni simili è costante. Spesso viene utilizzato per ragioni di propaganda politica.

DELEGA: nello stabilire le regole di internet, le istituzioni cooperano con le grandi piattaforme. Ma la questione è: quanto è possibile (e corretto) delegare?

3. DIRITTI E DOVERI

Per discutere di internet e dei suoi meccanismi, legati soprattutto alla libertà di espressione, è fondamentale partire dalle basi. Per questo è utile citare le norme fondamentali e capire che **nessuna libertà, nemmeno quella di espressione, è assoluta**.

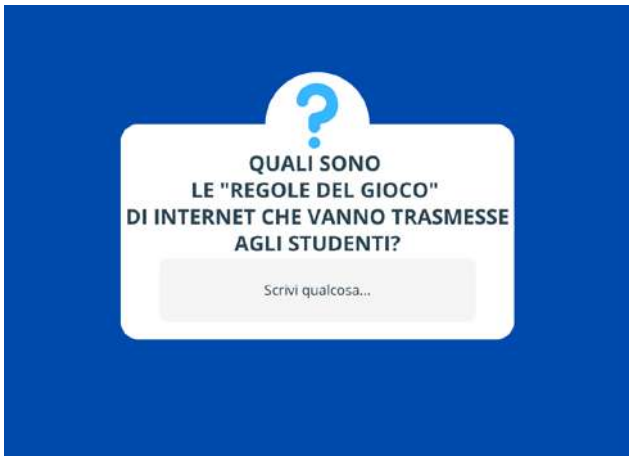
ARTICOLO 21 DELLA COSTITUZIONE:
"Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione".

ARTICOLO 11 DELLA CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA:
"Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. La libertà dei media e il loro pluralismo sono rispettati".

Compito delle autorità pubbliche, nonché delle piattaforme digitali, è far sì che il godimento delle libertà sulla rete sia oggetto di **un bilanciamento** così da impedire che una di queste libertà venga sacrificata per effetto dell'esercizio abusivo o "tirannico" di un'altra.

L'importante, seppur controverso, ruolo delle piattaforme nel contrasto a condotte illecite online è ribadito nel recente **Digital services act**, approvato dall'Unione Europea e che entrerà in vigore nel 2024.
Il DSA mira a creare uno spazio digitale più sicuro in cui siano protetti i diritti fondamentali di tutti gli utenti dei **servizi digitali**. Si rivolge principalmente agli intermediari e alle piattaforme online, quali, ad esempio, mercati online, social network, piattaforme per la condivisione di contenuti, app store e piattaforme di viaggio e alloggio online. L'obiettivo è responsabilizzare queste piattaforme affinché garantiscano, in collaborazione con le autorità pubbliche, **i diritti degli utenti** che le frequentano.

4. DOMANDE E RISPOSTE



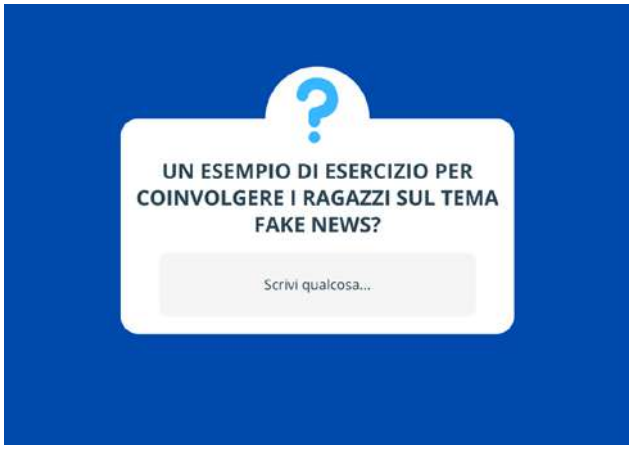
I ragazzi vivono e si informano sui social. Le loro fonti informative sono spesso TikTok e Instagram. Per questo è necessario offrire loro una "cassetta di strumenti" base, in modo da aiutarli a ragionare su questi strumenti.
Come?

Non negare la presenza delle piattaforme ma **imparare a conoscerle**;

parlare un linguaggio vicino ai ragazzi ma senza farsi attrarre, perché si rischia di diventare ridicoli (va trovato un equilibrio);

utilizzare le piattaforme per fare educazione e per coinvolgere i ragazzi (ci sono tanti esempi di insegnanti che su TikTok spiegano diverse materie in modo semplice e accattivante);

far comprendere loro l'importanza dell'**incrocio** di più **fonti**: spiegare che se una notizia è riportata da una sola fonte è (quantomeno) dubbia. Probabilmente è falsa, va verificata. E anche quando la fonte è all'apparenza affidabile, è sempre necessario applicare uno spirito critico.



Un'idea semplice ed efficace può essere analizzare insieme ai ragazzi i contenuti digitali: vedere ad esempio con loro un video virale su TikTok o un reel su Instagram nel quale si spiega un fenomeno o si racconta un fatto di attualità (o di politica) e analizzare in classe tutte le (eventuali) fake news presenti. Cercarle insieme ai ragazzi, spiegare quali sono gli errori e i meccanismi sottostanti può aumentare il loro coinvolgimento ma soprattutto la loro consapevolezza del fenomeno.

Gruppo di lavoro e ringraziamenti

Il presente vademecum riporta i passaggi più rilevanti degli incontri svolti presso la Luiss Guido Carli, da gennaio ad aprile 2023, nell'ambito del progetto di educazione digitale "Protezione dei dati dei minori: formazione, informazione, consapevolezza".

Il progetto è stato realizzato grazie alla virtuosa sinergia tra il Laboratorio Luiss @LawLab, il Garante per la protezione dei dati personali e Google, con il sostegno di Digital Angels, e rientra tra le iniziative del Manifesto di Pietrarsa, a cui la Luiss Guido Carli ha aderito attraverso @LawLab e il Centro di ricerca per le amministrazioni pubbliche "Vittorio Bachelet".

I più sinceri e affettuosi ringraziamenti per l'ideazione e la buona riuscita del progetto vanno a Guido Scorza, che ne ha posto "la prima pietra", e molte altre a seguire, e a Martina Colasante, che ha seguito con intelligenza e passione ogni fase del suo sviluppo.

Grazie anche a Flaminia Bolzan, Guido d'Ippolito, Francesco Nicodemo e Piermario Tedeschi, relatori nel corso dei seminari, per la profonda disponibilità e competenza.

L'ideazione, selezione e redazione dei testi del vademecum sono opera di Linda Giannattasio e Ambra Orengo.

Hanno proficuamente collaborato allo svolgimento degli incontri i ricercatori junior di @LawLab, Alessio Barca e Lorenzo Quattrucci.

Un ringraziamento speciale va, infine, rivolto alla Luiss Guido Carli per aver donato, come sempre, una cornice di libertà e bellezza al nostro lavoro. Si ringrazia, in particolare, per l'incessante collaborazione l'Ufficio Orientamento, Tutorato e Skill development, diretto da Lia Di Giovanni, e Marianna Astorino, sostegno prezioso e insostituibile nella gestione efficiente dell'intero ciclo di seminari.

“Appare necessario realizzare iniziative per accrescere il livello di consapevolezza dei minori riguardo ai rischi cui sono esposti e costruire intorno ai giovani utenti un ambiente digitale sicuro, sollecitando la responsabilità delle piattaforme digitali a questo scopo. Ciascun bambino, in ogni parte del mondo, ha diritto a un’infanzia felice. Garantire questo diritto è un dovere che richiede il contributo e lo sforzo di ciascuno”.

Sergio Mattarella, maggio 2022

“La privacy non è un ostacolo, ma la via grazie alla quale le innovazioni scientifiche e tecnologiche possono legittimamente entrare nelle nostre società e nelle nostre vite”.

Stefano Rodotà, settembre 2004

LUISS