

Conseguenze sulle persone e sulla società

La tecnologia non è nè buona nè cattiva.

E' uno strumento come lo può essere

l'automobile o il coltello.

Si tratta solo di conoscerla, di capirne i meccanismi e imparare ad usarla consapevolmente (e con prudenza).



Papa Francesco 

@Pontifex_it

...

Ai giganti della tecnologia di smettere di sfruttare la fragilità umana, le vulnerabilità delle persone, per ottenere guadagni.

6:06 PM · 16 ott 2021 · TweetDeck

247 Retweet **17** Tweet di citazione **2.002** Mi piace

I RISCHI

di cui si sente parlare più spesso

Nei confronti di gruppi ristretti di persone

Cyberbullismo: forma di bullismo condotto attraverso strumenti telematici.. Rispetto al bullismo tradizionale, il cyberbullismo si realizza su internet sfruttando la difficile reperibilità, l'indebolimento delle remore etiche, l'assenza di limiti spazio temporali.

Stalking: atteggiamenti che affliggono un'altra persona, perseguitandola, generandole stati di paura e ansia.

Revenge porn ("vendetta porno"): condivisione pubblica di immagini o video intimi tramite Internet, senza il consenso dei protagonisti. (Intelligenza Artificiale)

COME DIFENDERCI

- Per i genitori: pretendere le credenziali degli account dei figli, chiedere loro l'amicizia, diventare loro follower, ...
- Pubblicare il meno possibile le informazioni private.
- Rivolgersi a chi può dare una mano (genitori, educatori, insegnanti)
- Denunciare alla Polizia Postale:
<https://www.denunceviaweb.poliziadistato.it/polposta/wfintro.aspx>
<https://www.commissariatodips.it/>

FAKE NEWS = DISINFORMAZIONE

Consiste nella creazione e pubblicazione di informazioni verosimili ma false.

La pericolosità sta nel fatto che possono orientare il pensiero della gente.

Si basa sul fatto che sul web, specie sui Social, chiunque (agenzie di informazione e persone comuni) può pubblicare ciò che vuole.

Una campagna ben organizzata può provocare danni anche gravi.

L'espressione della propria opinione è una libertà sancita dalla Costituzione

La condivisione del post di altri, dopo averne controllato la veridicità, è un esercizio di democrazia

La condivisione di post non verificati può farci diventare parte del meccanismo di diffusione delle fake news
(attenzione ai finti profili di personaggi conosciuti)

COME DIFENDERCI

Controllare la provenienza e la veridicità della notizia prima di divulgarla o condividerla (FACT CHECKING), che si sia d'accordo o no.

<https://www.bufale.net>
<https://www.federprivacy.org/>
<https://www.idmo.it/author/redattore-idmo/>
(Italian Digital media Observatory)

FAKE NEWS: un esempio

Oriana Fallaci - Storia di un'Italiana

13 marzo alle ore 15:31 · 🌐

Ficcatevi in testa una cosa: la Russia è un paese enorme, stracolmo di materie prime e minerali, in grado di assicurare ai suoi 150 milioni di cittadini sicurezza energetica e alimentare per secoli. Ha un debito netto pari a zero, enormi riserve auree, surplus commerciale e mercati di sbocco alternativi in forte crescita, popolati da più di un terzo della popolazione mondiale (Cina, India, Pakistan, Sud Africa, Brasile). È un paese con una identità fortissima, arte e cultura, abitato da un popolo forgiato nel ghiaccio che da agricoltore e analfabeta in cinquant'anni è arrivato nello spazio. Ed è pure una superpotenza nucleare. Ma voi veramente pensate che un paese così fallisca dall'oggi al domani perché lo dicono i nostri "esperti", quelli del crollo di Wall Street e della Brexit che porterà le cavallette? Spegnete la tivù e iniziate a preoccuparvi di tutto ciò che non abbiamo noi. Che è un problema dannatamente più serio.

Apparsa su Facebook il 13 marzo 2022



14:18 ...0,3KB/s 📶 📶 66

← oriana fallaci

Città ▾ Gruppi pubblici I miei gruppi

di parlare

-  **Sezione PDL on-line "Oriana Fallaci"**
Gruppo Pubblico · Membri: 2
Gruppo politico on-line che vuole essere un pensatoio politico e di **Iscriviti**
-  **Abbonati: Oriana Fallaci - Storia di un'Italiana**
Gruppo Privato · Membri: 5
-  **INSCIALLAH - ORIANA FALLACI - IL GRUPPO**
Gruppo Privato · Membri: 61
I personaggi di questo romanzo sono immaginari. Immaginarie le **Iscriviti**
-  **Amici a cui piace Oriana Fallaci: fiorentina di ra...**
Gruppo Privato · Membri: 3 **Iscriviti**
-  **ORIANA FALLACI'S STORY**
Gruppo Privato · Membri: 2 **Iscriviti**

I RISCHI

di cui non si parla a sufficienza

Estrazione dei NOSTRI DATI dalla Rete

RACCOLTA: registrazione di quanti più dati possibili diretti o indiretti personali o tecnici (metadati).

ANALISI: con sistemi di Intelligenza Artificiale o con algoritmi tradizionali si incrociano tutti i dati raccolti in modo da poter produrre una ...

PROFILAZIONE: schedatura con interessi, orientamenti, abitudini, ecc... di ognuno. I profili, selezionati in base a criteri ben precisi sono molto appetibili a chi vuole convincere la gente.

TARGETIZZAZIONE: grazie all'enorme potenza di calcolo di cui dispongono, queste società sono in grado di veicolare qualsiasi informazione alle singole persone

PREDIZIONE: elaborando opportunamente i profili è possibile, in modo statistico, prevedere il comportamento di una certa categoria di profili circa un determinata situazione o tema o scelta.

ORIENTAMENTO: è possibile fare arrivare a determinati gruppi di profili specifici messaggi, che possono orientare il pensiero degli stessi

I NOSTRI DATI: dove vengono raccolti?

- Dai **PC** con sistemi operativi proprietari (Windows Apple) che richiedono l'accesso a un account: registrano le attività svolte e per quanto tempo.
- Dallo **smartphone**: posizione (anche senza GPS), foto, video
- Dai **dispositivi smart** (assistenti vocali come Alexa, Google assistant, Siri, smart TV, smart watch, ecc...): ciò che sentono, fotografano, rilevano.
- Dalla **navigazione** che facciamo in Internet:
 - coi traker: siti visitati, per quanto tempo, su cosa abbiamo cliccato;
 - coi cookies: Strettamente necessari (per garantire il funzionamento), Miglioramento dell'esperienza, Misurazione (analisi del comportamento), Targeting e Pubblicità (rilevare gli interessi)
- Dai metadati delle **chat**: data e ora, posizione, identificativo del dispositivo, lunghezza del messaggio, flag di consegna, flag di lettura, ...
- Dai **post** e dalle **reazioni** (like) che pubblichiamo sui Social: data e ora, posizione, identificativo del dispositivo, dati account, testo, immagini, like, condivisioni (con chi).

I NOSTRI DATI: perché vengono raccolti?

La raccolta dei dati è continua ed alimenta enormi archivi.

Questi vengono incrociati con elaborazioni complicatissime svolte da programmi di intelligenza artificiale su computer potentissimi (e energivori), in modo da ottenere un profilo il più accurato possibile (**profilatura** = schedatura), in cui sono evidenziati informazioni personali (dati e foto), interessi, orientamenti, passioni, abitudini, qualsiasi informazione sia stato possibile recuperare.

I dati così (ben) organizzati vengono venduti, selezionandoli in base a criteri precisi, ad aziende o organizzazioni che intendono raggiungere un certo target con le proprie proposte commerciali o di altro genere.

Chi acquista questi dati è disposto a spendere parecchio perché sa che raggiungerà persone sensibili a ciò che gli viene offerto (comunque i costi sono sempre inferiori a quelli di una campagna pubblicitaria tradizionale).

Io non ho nulla da nascondere!

Alcune IDEE di utilizzo dei nostri profili:

- Su Whatsapp racconti al tuo migliore amico di una spiacevole infezione fungina e poi trovi pubblicità per unguento fungicida ovunque, mentre visiti Facebook, e altre persone scorgono ciò che hai sullo schermo
- Ti viene rifiutato un posto di lavoro perché il responsabile del personale ha trovato nel tuo profilo una serata un po' fuori ordinanza, passata con gli amici.
- Viene corretto il prezzo di ciò che stai acquistando (bene o servizio) in base al potere di acquisto rilevato dal tuo profilo
- Si applica il tuo viso a un altro corpo (usando anche la IA) per ottenere immagini di sesso esplicito col quale corromperti (ti ricordo che Facebook ha avuto diversi episodi di perdita di dati e qualche malintenzionato potrebbe averli trovati e/o acquistati nel Dark Web)



Notare le protezioni su microfono e webcam sul PC personale di Mark Zuckerberg

Scenari possibili (o già accaduti)

- Se utilizzati da gruppi di potere economico, politico, o altro, queste tecniche possono essere utilizzate per orientare il pensiero o le scelte di masse molto numerose di persone. Si mette a rischio “l’autodeterminazione e la legittimità della autorità e del governo democratico” (*Shoshana Zuboff, “Il capitalismo della sorveglianza”, Louiss, 2019, p.503*).
- Sfruttando tecniche di ingegneria sociale come gli incentivi (o stimoli positivi) è possibile modificare i comportamenti delle persone, riducendone la individualità a loro insaputa. “Gli incentivi della rete sociale sono i soli strumenti necessari per imporre nuove norme comportamentali”
(*Daniel W. Byork, B.F. Skinner: A life, Basic, New York, 1993, p.220 – Grazie a Shoshana Zuboff da “Il capitalismo della sorveglianza”, Louiss, 2019, p.454*)
- Conoscendo i bisogni e le inclinazioni della gente sarà possibile organizzare (o imporre) una società dove tutto è previsto e pianificato.

Scenari possibili (o già accaduti)

Sei un po' razzista? Facebook può essere usato (e viene usato!) per consolidare il tuo razzismo.

Sei più moderato? Facebook è in grado di selezionare un mix di fonti ambigue per alimentare dubbi sugli stranieri e virare i tuoi riferimenti sempre più a destra attraverso una selezione mirata di post adatti a colpire le tue paure più accentuate.

<https://cagizero.wordpress.com/2019/04/23/matrix-e-whatsapp-un-confronto/>

Scenari possibili (o già accaduti)

Sei sensibile alle violenze sugli animali? Ti verranno messi sotto gli occhi diversi articoli con stranieri che fanno male ad animali. Hai paura delle malattie? Vedrai post sui migranti che portano la peste medievale.

Sei sgrammaticato e non metti alcun like a fonti culturali? Vuol dire che hai una bassa istruzione e nella tua Timeline verranno fatti scorrere contenuti falsi ma dal linguaggio semplice.

Hai una preparazione scolastica media-buona ma non sei quel che si chiama un “divoratore di libri”? Ti piacciono il calcio ed i film di supereroi? Non vedrai molti post ignoranti ma invece tanta roba giustificazionista e qualunquista del tipo “eh, ma in fondo *Tizio* non ha tutti i torti”.

<https://cagizero.wordpress.com/2019/04/23/matrix-e-whatsapp-un-confronto/>

Scenari possibili (o già accaduti)

I noti avvenimenti di Facebook nello scandalo Cambrydge Analytica; l'influenza di Facebook nella Brexit e nell'elezione di Trump hanno reso evidente che le campagne politiche mirate e targhetizzate al singolo utente sono una realtà molto più pervasiva e difficile da monitorare di quanto il grosso della popolazione sospetti. Il ruolo di Facebook nella Brexit, per esempio, é stato tutt'altro che secondario e questo é stato possibile perché chi ha voluto diffondere sul social network delle informazioni false l'ha potuto fare in modo estremamente mirato.

<https://cagizero.wordpress.com/2019/04/23/matrix-e-whatsapp-un-confronto/>

Chi attua questa pratica?

I nomi più di rilievo sono:

Google (Mountain View): Gmail, Drive, Classroom, Meet, Youtube, Android,

Apple (Cupertino): iOS (sistema operativo dei cellulari Apple)

Facebook / Meta (Menlo Park): Facebook, Whatsapp, Instagram, ...

Amazon (Seattle): Amazon Web Services, Alexa Internet, Twitch.tv (A9.com, IMDb, Goodreads)

Microsoft (Redmond): Windows, Office 365, Teams, ...

Comunemente indicati con l'acronimo **GAFAM**

Altre aziende che solitamente estraggono dati per venderli a quelle citate.

Proteggiamo i nostri bambini!

Una consistente fascia della popolazione **non è consapevole, o sottovaluta, i rischi legati alla vita digitale** e alla semplice presenza su internet, dove ogni dato può essere preda di malintenzionati e usato nei modi più pericolosi. Gli esperti prevedono che entro il 2030, due terzi di tutti i casi di furto di identità avverranno tramite le nuove tecnologie di deepfake (tecnica per la sintesi dell'immagine umana basata sull'intelligenza artificiale).

Condividendo incautamente le foto dei bambini e altri dati, come nomi o età, tramite social media e servizi di messaggistica istantanea, dunque, **i genitori espongono inconsapevolmente i propri figli ai rischi.**

(https://www.hwupgrade.it/news/web/deutsche-telekom-a-quali-rischi-vanno-incontro-i-genitori-quando-condividono-le-foto-dei-loro-figli_118722.html)

<https://www.youtube.com/watch?v=nkV0pQpMGmQ>



Un esempio: le App di messaggistica

Quali sono le informazioni raccolte da alcune App, gli diamo il permesso accettando le CONDIZIONI D'USO.

One of these chat apps is not like the others.



The infographic displays the 'App Privacy' and 'Data Used to Track You' sections for seven chat applications. Signal is the only app shown with a 'Data Not Linked to You' section, indicating it does not track user data. The other apps track various types of data, including contact info, location, and usage data. A red banner at the bottom identifies the apps: WhatsApp, FB messenger, Instagram, Signal, Snapchat, Wechat, and Telegram. A source note at the bottom right reads 'SOURCE: IOS APP STORE'.

SIGNAL DOESN'T TRACK YOUR DATA

WhatsApp
FB messenger
Instagram
Signal
Snapchat
Wechat
Telegram

SOURCE: IOS APP STORE

Sapendo questo, è lecito chiedersi come proteggiamo la riservatezza delle informazioni usando le App di messaggistica commerciali in situazioni come queste:

- Gruppi di genitori delle scolaresche
- Messaggi di servizio tra i funzionari della P.A.
- Messaggi di servizio del personale delle Forze dell'ordine
- Messaggi tra medici e pazienti
- Altre situazioni dove alcuni parlano delle faccende di altri.

I primi a salvaguardare privacy e riservatezza dobbiamo essere noi!

COME DIFENDERCI

- Ricordiamo che non avremo più potere su quanto pubblichiamo.
- Ricordiamo che Internet non dimentica nulla (anche ciò che cancelliamo)

QUINDI

- Pubblichiamo il meno possibile informazioni personali (testi, immagini, video, ...).
- Modifichiamo le impostazioni dei Social in modo che i nostri post siano visibili solo a una cerchia ristretta di persone.
- Non rincorrere la visibilità a tutti i costi (amici, followers, like, ecc...)
- Valutare l'utilizzo di piattaforme e servizi che garantiscono la riservatezza delle nostre informazioni, che non hanno secondi fini cioè non utilizzano algoritmi di profilazione (<https://fediverso.info/>).
- Utilizzare App, programmi per navigare (Browser) e Motori di ricerca di produttori sensibili alla riservatezza (<https://www.lealternative.net/>).
- Utilizzare App di messaggistica meno “spione” (Telegram, Signal, Element)

INTELLIGENZA ARTIFICIALE (IA)

Se ne sente parlare quotidianamente, spesso viene presentata come una specie di panacea o come la soluzione definitiva ai problemi.

La sua peculiarità è quella di saper **immagazzinare**, nella fase di addestramento prima e durante l'utilizzo in seguito, **una quantità impressionante di informazioni** e di casistiche.

Computer estremamente potenti sono poi in grado di **recuperare velocemente ciò che**, secondo loro, in base ad algoritmi statistici, **è associabile alle situazioni e alle domande che gli vengono presentate**. Poi confezionano i risultati secondo i canoni più adatti a chi fa la richiesta (testi, immagini, musiche, parlato, video, ecc...).

INTELLIGENZA ARTIFICIALE (IA)

PERÒ non è in grado di valutare se ciò che produce sia vero, etico, rispettoso, moralmente accettabile, ...

QUINDI se addestrata con informazioni selezionate e veritiere (es.: banche dati mediche) potrà ritornare risposte precise e coerenti, ed essere un enorme aiuto per i ricercatori.

MA se addestrata con qualsiasi informazione che si possa trovare in Rete, come fa ChatGPT, c'è il rischio reale che ritorni risposte imprecise o errate o false, mostrandole per veritiere dato che sono ben confezionate.

IN TAL MODO genera negli utilizzatori disinformazione e confusione.

**Chi imposta gli algoritmi e decide le fonti di informazione nella fase di addestramento?
E nella fase operativa quali CRITERI utilizzerà per selezionare cosa estrarre e cosa scartare?**

Un esempio di articolo prodotto dalla AI (testi scritti interamente da ChatGPT4 e immagini generate da Dall E 2, entrambi di OpenAI)
<https://www.mistersommelier.com/tecnica/tappi-per-bottiglie-di-vino-vetro-e-silicone-allavanguardia-nella-conservazione-del-nettare-degli-dei/>

INTELLIGENZA ARTIFICIALE (IA)

Noi, per comprendere il mondo circostante ci basiamo sul modello che abbiamo di esso, basato sull'esperienza fisica, ma anche sul modo in cui il nostro cervello registra la realtà. Questo ci consente di fare analogie e previsioni, ma anche di distinguere il bene dal male. L'IA non ha un modello del mondo ma solo relazioni tra parole (o tra forme, nel caso di informazioni grafiche) e quindi 'non sa di cosa parla'.

Lavora 'per sentito dire', quindi potremmo dire che 'da opinioni da bar'.

Interessante è il caso dell'avvocato Steven Schwartz che ha presentato ad una corte statunitense, un documento a difesa delle sue tesi che citava molte sentenze, tutte inesistenti.

Questo documento era stato prodotto da una IA (ChatGPT in particolare).

L'avvocato si è difeso dicendo di aver chiesto a ChatGPT se le informazioni fossero veritiere, ottenendo risposta affermativa.

È evidente che ChatGPT non possiede il concetto di 'veritiero' ma solo la relazione tra 'testimonianza' e 'veritiera'.

CONDIZIONAMENTI

Per generare profitto i Social commerciali (FB, Instagram, YouTube, ecc...) hanno bisogno di conoscere una quantità notevole di nostre informazioni (post letti, Like, amicizie, ...), e di proporci informazioni (pubblicità, notizie vere o false, ecc...).

Per raggiungere questi obiettivi **devono tenere l'utente quanto più possibile connesso**, lo fanno utilizzando algoritmi che presentano contenuti che attraggono e oscurano quelli che allontanano, scegliendo tra situazioni sensazionali o divertenti, sport, contenuti di violenza, sesso, odio, i contenuti che interessano l'utente in base alla sua profilazione.

Questo meccanismo è pericoloso perché si viene **paralizzati in una bolla di informazioni**, sono chiamate "filter-bubble" (bolla generata dai filtri) e/o "knowledge bubbles" (bolla di conoscenza). Conseguenza di ciò è che di ogni questione si osserverà solo l'aspetto che ci interessa/piace e non si verrà a conoscenza della totalità delle informazioni (tra le quali ci sono anche quelle contrastanti). Questo spiega le **estremizzazioni** dei pensieri e dei comportamenti di certi gruppi di persone, e il meccanismo che può portare a orientare opinioni e scelte della gente.

**Chi controlla il controllore, cioè colui che crea l'algoritmo che decide cosa far vedere?
È importante prendere le proprie informazioni anche da fonti diverse dai Social.**

DIPENDENZE

- **dalla marca:** tendenza ad utilizzare dispositivi di una certa marca
- **dalle applicazioni digitali (lock-in):** adattarsi ad usare soluzioni software (programmi, app, piattaforme, ...) proposte e imposte dal mercato; non ci si preoccupa di valutare alternative più adatte, più etiche, che limitino meno la propria libertà; spesso ci inducono ad obbligare gli interlocutori ad utilizzare lo stesso programma per poter interagire con noi diventando così parte del meccanismo. Le Big Tech da tempo si affidano a questo meccanismo, tant'è vero che fanno offerte non rifiutabili a scuole, associazioni, ministeri. È la stessa tecnica dei pusher.
- **dallo smartphone:** è normale averlo sempre con se, lo si usa anche per attività per cui non è necessario, vengono proposti sempre più "utilizzi", anche inutili, pur che lo teniamo sempre vicino e diventi sempre più insostituibile.

DIPENDENZE

- **dai Social:** necessità di esserci pubblicando qualcosa o esprimendo reazioni (like, follower, visualizzazioni, ...). È esattamente ciò che vogliono i Social: tenere agganciate le persone quanto più possibile.
- **Incapacità di affrontare problemi** e di ipotizzare soluzioni perché abituati a cercare soluzioni e risposte su Internet. Le proposte che ci sono sono talmente numerose che non lasciano spazio alla creatività di ognuno (atrofizzazione).

CONCESSIONE ACRITICA DI CREDITO

Frasi come “L’ha detto la TV” o “L’ho visto su Internet” si sentono da decenni ...
È fondamentale identificare comunque le fonti di notizie e informazioni.

Considerare gli ultimi modelli di dispositivi o le versioni più recenti dei software sempre migliori rispetto ai precedenti. Non è detto, vanno verificate. Ad esempio da anni molti produttori di software rendono disponibili nuove versioni, testate appena, lasciando agli utilizzatori il compito di trovarne i difetti.

Essere convinti di possedere (conoscere / saper usare) la tecnologia. Questo produce una pericolosa disinvoltura quando si utilizza il digitale (“ma si provo tanto non succede nulla”). È un atteggiamento indotto dall’ambiente dell’elettronica di consumo (“è facile da usare, non richiede impegno per apprenderne l’uso, alla portata di chiunque, non ci sono rischi)

Attenzione particolare va data alla **Intelligenza Artificiale** perché essa è in grado di produrre contenuti realistici e credibili ma non necessariamente veri. Chi non ha competenze sull’argomento trattato o possiede un pensiero critico insufficiente può essere ingannato molto facilmente.

ATROFIA

CALCOLATRICE: si diceva anni fa che avrebbe fatto perdere la capacità di fare i calcoli a mente, cosa è successo?

CORRETTORE: frasi sgrammaticate e con punteggiatura errata nelle chat

ABBONDANZA DI INFORMAZIONI: può generare l'incapacità di ricercare quelle utili, corrette o che servono, ci si accontenta delle prime trovate.

ABBONDANZA DI GUIDE ED ESEMPI: può creare la riduzione della capacità di affrontare e risolvere problemi (problem Solving)

USO DEI VIDEO determina la riduzione del pensiero critico (mai accorti?), ricordo che la lettura è considerato il sistema principe per allenare al ragionamento e alla capacità critica (<https://libreriamo.it/libri/perche-leggere-ogni-giorno-10-benefici-lettura/>).

INTELLIGENZA ARTIFICIALE potrebbe causare, in alcuni casi, la riduzione della capacità di ideare, creare, inventare, ...

La tecnologia ha sempre prodotto questo rischio, sta a noi non farci sopraffare.

TECNOLOGIE E FENOMENI A CUI PRESTARE ATTENZIONE

METAVERSO

Meta (Facebook) sta spingendo (pubblicizzando) questo sistema come strumento per ampliare le possibilità di comunicazione e la conoscenza.

Si tratta di un mondo virtuale dove ognuno può entrare con un suo AVATAR, un personaggio virtuale che lo rappresenta. L'avatar interagisce con quella realtà virtuale e con gli avatar delle altre persone.

C'era già stato un tentativo, si chiamava SECOND LIFE, un flop.

Quale sarà l'obiettivo di chi scrive gli algoritmi alla base del Metaverso?

Chi potrà garantire che questi non manipolino le interazioni tra gli avatar e/o tra questi e la realtà?

Potremmo avere questa certezza solo se il codice che descrive questi algoritmi è aperto e disponibile per essere analizzato.

IOT = Internet Of Things

È uno degli utilizzi della rete internet: gli oggetti (le "cose") si rendono riconoscibili e possono comunicare dati propri e accedere ad informazioni degli altri. Le sveglie suonano prima in caso di traffico, le scarpe da ginnastica trasmettono tempi, velocità e distanza percorsa, i vasetti delle medicine avvisano se ci si dimentica di prendere il farmaco, ecc... Tutti gli oggetti possono acquisire un ruolo attivo grazie al collegamento alla Rete.

Questi oggetti connessi che sono alla base dell'Internet delle cose, vengono chiamati "smart object" (in italiano "oggetti intelligenti") e possono identificarsi, connettersi, fornire la propria localizzazione, sono capaci di elaborare dati e di interagire con l'ambiente esterno.

Come tutti gli oggetti connessi alla Rete devono fare riferimento a un server.

**Chi gestisce il server quale riservatezza garantisce ai dati a cui può accedere?
E se si spegne il server, o fallisce l'azienda che lo gestisce a cosa serviranno gli smart object?**

Influencer, Youtubers e Tiktokers

“Gli influencer sono persone che, grazie a un raggio d'azione molto ampio (followers), hanno il potere di influenzare le abitudini di acquisto o le azioni di altre persone caricando una qualche forma di contenuto originale, spesso sponsorizzato, su piattaforme di social media...”

(https://it.wikipedia.org/wiki/Marketing_di_influenza)

Guadagnano dalle sponsorizzazioni, cioè dalle aziende che li pagano perché propongano, utilizzino e promuovano i loro prodotti.

È per loro necessario mantenere o aumentare quanto più possibile il numero dei followers, in questo modo le sponsorizzazioni saranno più elevate. In certi casi, i meno onesti, sono disposti a diffondere notizie false o di etica discutibile spesso utilizzando in modo irresponsabile la IA.

Il pericolo sta nel fatto che i followers **spesso seguono in modo acritico i loro influencer** per cui questi hanno il potere di orientare le masse. Da ciò deriva una **enorme responsabilità**.

BUONE PRATICHE

- Essere sempre attenti e un po' sospettosi.
- Considerare gli strumenti digitali come STRUMENTI!
- Non lasciarsi travolgere da realtà virtuali come i videogiochi, che devono restare solo divertimento.
- Chat, Social, blog:
 - ▶ non pubblicare informazioni personali (dati, foto, attività) e ridurre il numero dei destinatari con gli appositi filtri.
 - ▶ non lasciarsi condizionare dai contenuti che vengono proposti.
 - ▶ verificare le notizie e le fonti prima di condividerle
 - ▶ mantenere un pensiero critico rispetto a ciò che viene esposto.
- Internet non dimentica nulla, attenzione a ciò che si scrive.

BUONE PRATICHE



Interessante CANDID CAMERA Belga

<https://youtu.be/qYnmfBiomlo>

Vanessa [redacted]
Forse nn ci siamo capiti che nn appena il microchip diventerà obbligatorio vi traceranno in ogni luogo per controllare ogni persona! E questo il marchio della bestia che vi metteranno sottopelle e voi pecore sottomesse al volere!
5 h Mi piace Rispondi 4

Giovanni [green]
Pensi seriamente che ci sia bisogno di un microchip per "controllarci" e sapere ad esempio che tu la settimana scorsa eri a Napoli in via [redacted] da [redacted] che stavi mangiando una pizza col cornicione ripieno insieme a tuo marito, cognato, tua sorella, 3 bambini e una signora?
5 h Mi piace Rispondi 18

Vanessa [redacted]
Ora tu mi spieghi come lo sai!
5 h Mi piace Rispondi 5

Giovanni [green]
Sono un hacker e sono entrato nel tuo cellulare, quello che porti pure al cesso e che ti rende rintracciabile in ogni secondo della tua vita.
5 h Mi piace Rispondi 36

Giovanni [green]
Sto scherzando, idiota. Hai facebook pubblico, mi è bastato scorrere la tua bacheca per vedere che ti sei registrata in mille posti, con annessi tag e foto. Il bello è che fate "lotte" al grido di "ci vogliono controllare!" quando con la vostra stupidità sputtunate già al mondo ogni dettaglio della vostra vita altrimenti vi sentite delle nullità.
Ma non ti mettere il microchip ehh mi raccomando
5 h Mi piace Rispondi 73

Commenti CLERICABILI CO.

PER APPROFONDIRE

GARANTE per la privacy

<http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1614258>



<http://www.generazioniconnesse.it>

Documenti, siti e numeri telefonici utili, sul sito del LUGMan
https://lugman.org/IncontriInternet19#Materiali_e_Approfondimenti

I **Linux Users Group Italiani**
organizzano annualmente
il **Linux Day**
giornata Nazionale di
Linux e del Software Libero
Quarto sabato di Ottobre



A Mantova è attivo il
Linux Users Group Mantova
<http://www.lugman.org>
info@lugman.org
<https://lists.linux.it/listinfo/lugman>