Il DIGITALE sotto la lente

Ciò che bisogna sapere per usare consapevolmente gli strumenti digitali.

Il DIGITALE sotto la lente

La tecnologia non è ne buona ne 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).

Il DIGITALE sotto la lente

Così come si impara ad usare il coltello e ci si affianca ai bambini in modo che non si facciano male, anche per gli strumenti digitali è necessario imparare a utilizzarli e affiancare chi è inesperto per evitare **che si faccia male**

Il DIGITALE sotto la lente

COSA SONO I GIGA? NULLA!

Chilo (k) = migliaia
Mega (M) = milioni
Giga (G) = miliardi
Tera (T) = migliaia di miliardi

Ma di che???

QUANTITÀ DI DATI (conservati)
Byte (B)
1 Byte = 1 carattere
"C" = 1 carattere
"Come stai?" = 11 caratteri
1 canzone ± 3 MB
1 film ± 7 GB

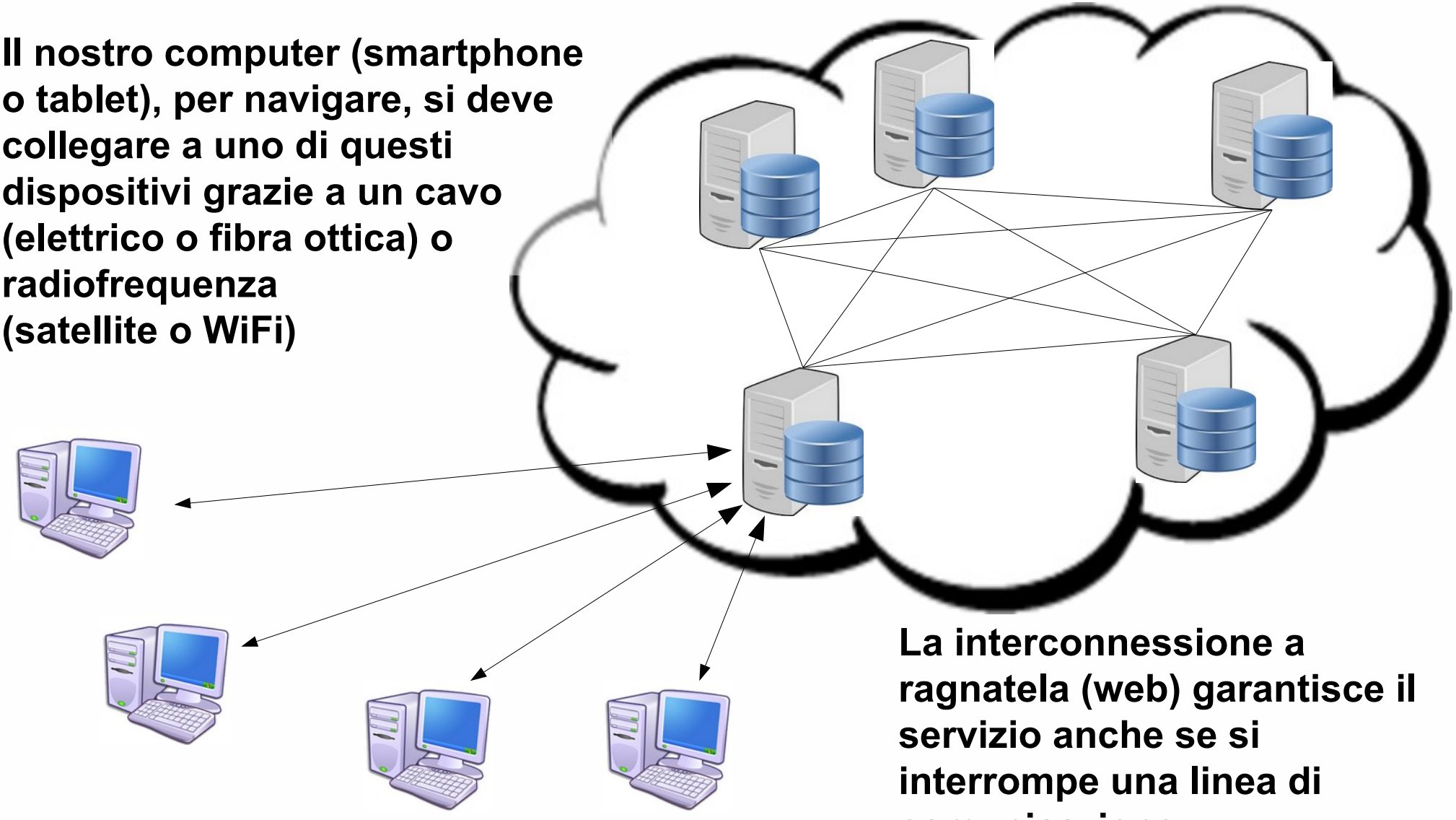
VELOCITÀ DI TRASMISSIONE (dei dati)
Bit Per Secondo (bps)
(1 bit = 1/8 di Byte)
Modem (anni 19) = 56 Kbps**
ADSL = 20 Mbps
Fibra ottica FTTC: fino a 300 Mbps
Fibra ottica FTTH: fino a 2,5 Gbps
La tua connessione? (www.speedtest.net)

COME E' FATTA LA RETE

Internet è una rete di dispositivi interconnessi che in modo automatico trasferiscono dati da un punto all'altro del globo.

Il DIGITALE sotto la lente

Il nostro computer (smartphone o tablet), per navigare, si deve collegare a uno di questi dispositivi grazie a un cavo (elettrico o fibra ottica) o radiofrequenza (satellite o WiFi)



La interconnessione a ragnatela (web) garantisce il servizio anche se si interrompe una linea di comunicazione.

COME FUNZIONA LA RETE

Internet è una architettura CLIENT – SERVER: i nostri dispositivi sono i CLIENT che utilizzano i servizi offerti dai SERVER dei diversi siti.

I server contengono e conservano i dati per comunicarli ai client quando richiesti.

I dati scambiati attraverso un sito (o piattaforma) **vengono conservati sul server** contenente il sito stesso in modo da poterli condividere con altre persone.

Il DIGITALE sotto la lente

Esempio: condivisione di un contenuto (post)

… dove resterà per sempre …

Server della piattaforma social

… in modo che i destinatari lo possano vedere quando vogliono.

Il post viene inviato al server ...

Tutto ciò che produciamo è immagazzinato sui server di qualcuno

Questo meccanismo è identico per qualsiasi servizio di condivisione (mail, chat, messaggi, foto, videogiochi on-line, piattaforme di streaming, ecc…), ed è questo il meccanismo che permette il funzionamento dei dispositivi che richiedono i servizi di Rete come smartphone, tablet e ChromeBook

CONSIDERAZIONI e NOTIZIE

I dati che condividiamo sono accessibili ai gestori dei server, questo è necessario per rendere possibili le operazioni di manutenzione che garantiscono il mantenimento del servizio e la conservazione dei dati.

Dalla posizione geografica dei server dipendono diversi nostri diritti, infatti la loro gestione, e quella dei dati in essa conservati, è regolata dalle norme vigenti nello Stato o Nazione dove essi sono posti fisicamente.

L'Europa ha un regolamento sul trattamento dei dati personali detto General Data Protection Regulation o **GDPR**, molto avanzato, mentre altri paesi (America, Cina, ecc...) hanno regole meno rigide.

Esempio: Ipotizziamo di aver partecipato ad una festa e siamo stati ritratti in una foto, salvata su un Social americano o cinese. In quei paesi è legale applicare il riconoscimento facciale, quindi riconoscere i nostri volti nella foto e taggarla con i nostri nomi. Questo consente ai motori di ricerca di associarci a quella festa, cosa che magari non ci fa estremo piacere.
In Europa, col GDPR, il riconoscimento facciale non è permesso.

Il DIGITALE sotto la lente

Allora è importante valutare chi ci da i servizi

Mi posso fidare di …

Agenzia Entrate

Banca Popolare di Sondrio

INPS Istituto Nazionale Previdenza Sociale

Ministero dell'Istruzione e del Merito

… e diverse altre aziende.

Ed è importante valutare chi ci da i servizi

Mi fido meno di aziende di cui si viene a sapere …

- Xxxxxx: una storia di comportamenti anti-competitivi e dannosi per gli utenti
- Xxxxx, mezzo milione di password in vendita
- Perchè alcune scuole tedesche hanno bloccato Xxxxxxx per rischi sulla privacy
- Xxxxxx, l'app per videoconferenze condivide i dati con Yyyyyyy
- Xxxxxxx, trasparenza e sorveglianza
- Xxxxx e Yyyyyy, multa antitrust per "obsolescenza programmata"

Il DIGITALE sotto la lente

Articolo del 31/03/2009

microsoft: una storia di comportamenti anti-competitivi e dannosi per gli utenti

Scritto da: Commissione Europea (Unione Europea)

ZEUS NEWS

Home Editoriale Recensioni Focus Sicurezza Trucchi Maipiusenza Segnalazioni Sor

Zoom, mezzo milione di password in vendita

Nel dark web a prezzo di saldo.

Articolo multipagina 3 / 3

[ZEUS News - www.zeusnews.it - 13-04-2020]

WIRED.IT Sezioni Live Gallery Wired Next

HOT TOPIC SERIE TV ONEPLUS CORONAVIRUS GOOGLE TRAILER LAVORO FACEBOOK CLIMA INTERNET IPAD WIRED MAGAZINE...

Perché alcune scuole tedesche hanno bloccato Office 365 per rischi sulla privacy

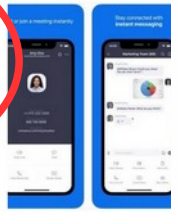
In Assia il garante della privacy ha vietato l'uso di Office 365 nelle scuole. I cloud usati dalla suite di Microsoft violerebbero le norme del Gdpr

la Repubblica

Tecnologia

HOME NEWS SPECIALI MOBILE SOCIAL NETWORK SICUREZZA

Zoom, l'app per videoconferenze condivide i dati con Facebook



Credits: Zoom/Apple Store

BLOG / TABULARIO

Google, trasparenza e sorveglianza

07 Giugno 2017 | Carlo Mazzucchelli

Tecnologia Economia digitale

In evidenza Criptovalute Spread BTP-Bund FTSE-MIB Petrolio

I NOSTRI PODCAST

Silvia Rovere, presidente Assoimmobiliare: «Serve una legge quadro per la rigenerazione urbana»

Intel e Italvolt, partite strategiche dimenticat

Sanzioni per 10 milioni

Apple e Samsung, multa Antitrust per «obsolescenza programmata»

Il DIGITALE sotto la lente

Non ci si dovrebbe fidare di aziende di cui si viene a sapere …

- Xxxx papers, spuntano 10 mila pagine su allarmi ignorati su odio e fake news: perché Yyyyyy rischia la crisi più minacciosa
- Xxxxx può leggere i tuoi messaggi, altro che crittografia end-to-end
- Xxxxx: secondo un documento interno *[omissis]* il Social non ha ben chiaro dove e come vengono usati i dati che raccoglie
- Scandalo Xxxxxx, parla Yyyyyy: “I profili social coinvolti sono 87 milioni”

Il DIGITALE sotto la lente

OPEN

MONDO FACEBOOK • FAKE NEWS • INCHIESTE • INFORMAZIONE • MARK ZUCKERBERG • SOCIAL MEDIA • USA

Facebook papers, spuntano 10 mila pagine su allarmi ignorati su odio e fake news: perché Zuckerberg rischia la crisi più minacciosa

25 OTTOBRE 2021 - 16:24 di Redazione

FEDERPRIVACY

Area Riserva

Home Associazione Attività Informazione Strumenti Community Domande Freq

NEWS OCSE: adottato accordo intergovernativo sulla salvaguardia della privacy nell'accesso

Home › Informazione › Il Punto di Vista › WhatsApp può leggere i tuoi messaggi, altro che c

Tweet Condividi Condividi Condividi

WhatsApp può leggere i tuoi messaggi, altro che crittografia end-to-end

Il punto di vista Lunedì, 13 Settembre 2021 08:40

Facebook: secondo un documento interno ottenuto da Motherboard, il social non ha sempre ben chiaro dove e come vengano usati i dati che raccoglie.

Gli stessi impiegati di Facebook ammettono di fare fatica a tenere traccia di dove finiscano i dati raccolti - problema noto come "discendenza dei dati", *data lineage*. La questione si sarebbe

MENU CERCA la Repubblica R+ Rep: ABBONATI

Tecnologia

HOME NEWS SPECIALI MOBILE SOCIAL NETWORK SICUREZZA PRODOTTI INTERATTIVI

Scandalo Cambridge Analytica, parla Facebook: "I profili social coinvolti sono 87 milioni"

(reuters)

Mark Zuckerberg, a capo del social, stabilisce quindi una volta per tutte quanti profili "potrebbero raggiunti da Cambridge Analytica" soprattutto per influenzare il risultato delle elezioni presidenz

MACCHINE E ALGORITMI!

Il DIGITALE sotto la lente

Appello di Papa Francesco (14/11/2019)

Stati Generali dell'Innovazione

«Le possibilità della tecnologia sono sempre più elevate. [...] Faccio quindi appello agli ingegneri informatici, perché si sentano anch'essi responsabili in prima persona della costruzione del futuro»

«Tocca a loro, con il nostro appoggio, impegnarsi in uno sviluppo etico degli algoritmi, farsi promotori di un nuovo campo dell'etica per il nostro tempo: la "algor-etica"»

Necessità di un approccio etico agli algoritmi !!!

Webinar Civic Tech Academy «GAP», 6 maggio 2021

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

HARDWARE e SOFTWARE

HARDWARE

E' in pratica, la parte fisica e tangibile del dispositivo.

(Wikipedia)

SOFTWARE

È l'insieme dei programmi e dei dati che determinano il funzionamento del computer. I programmi sono la traduzione degli algoritmi (ragionamenti) in linguaggi comprensibili ai computer.

Tra i due **è più importante il software** perché determina il funzionamento e il comportamento del dispositivo.

È anche **il più facile da sostituire** e/o aggiornare, anche all'insaputa dell'utilizzatore.

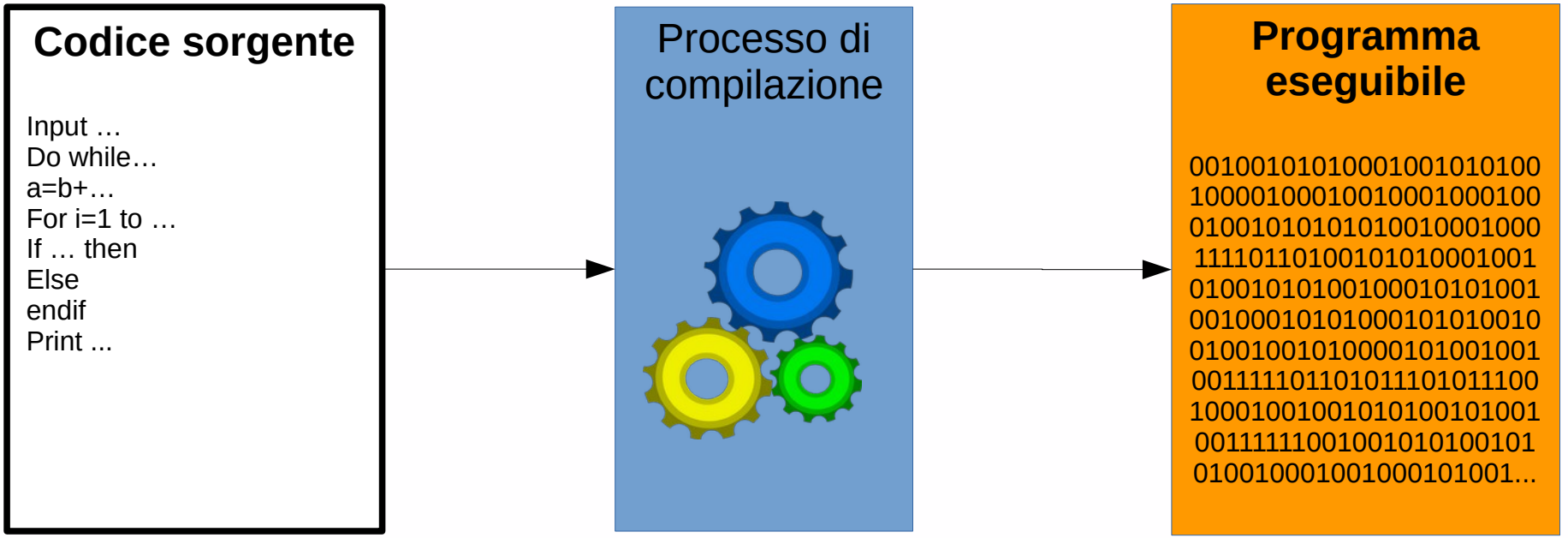
GLI ALGORITMI

Sono l'insieme di processi, decisioni, comportamenti che si intende far svolgere al computer.

Essi sono trascritti con appositi linguaggi in modo che vengano compresi ed eseguiti dai computer, vengono cosi prodotti i programmi (o App).

I programmi costituiscono il SOFTWARE.

COME SI PRODUCONO I PROGRAMMI (APP)



TIPI DI SOFTWARE

PROPRIETARIO

BISOGNA ACCETTARE
I PROGRAMMI ACCOGLIENDO LE DICHIARAZIONI DELL'AZIENDA PRODUTTRICE DATO CHE IL CODICE SORGENTE È SEGRETO.

QUESTIONE DI FIDUCIA!

LIBERO

È POSSIBILE VERIFICARE COME FUNZIONANO I PROGRAMMI PERCHÈ NORMALMENTE È RESO PUBBLICO ANCHE IL CODICE SORGENTE DEL PROGRAMMA.
Open Source (=sorgente aperto)
TRASPARENZA!

Il DIGITALE sotto la lente

ALCUNI TITOLI

PROPRIETARIO

MS Windows

Apple OSx

Microsoft Office

MS EDGE
Chrome

LIBERO

GNU/Linux

LibreOffice

Firefox
Brave
Chromium

Il DIGITALE sotto la lente

ALCUNI TITOLI

PROPRIETARIO

Office 365
Microsoft 365

Google workspace
Google Classroom

Zoom Meeting
Google Meet
Ms Teams

Skype

WhatsApp

LIBERO

NextCloud
OpenCloud

MOODLE

Jitsi
Big Blue Button
Multiparty Meeting

Signal
Telegram (solo client)

I RISCHI

(dal lato tecnico)

VIRUS

Un virus è un insieme ridotto di istruzioni che si inserisce nei file presenti nel computer.
Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto il file infetto, l'utente vede solo l'esecuzione del programma e non si accorge che il virus è ora operativo in memoria e sta compiendo le varie operazioni contenute nel suo codice.
Principalmente un virus esegue copie di sé stesso spargendo l'epidemia, poi svolge operazioni molto più dannose come cancellare, cifrare o corrompere file, far apparire messaggi, disegni o modificare l'aspetto del video, ...

- **Evitare di navigare in siti dubbi**
- **Adottare soluzioni tecniche che proteggono dalle intrusioni nei nostri dispositivi**
- **Usare dispositivi con Sistemi Operativi meno vulnerabili come Linux o Apple**

ALTRI MALVARE

Un **trojan** o trojan horse (dall'inglese per **Cavallo di Troia**), è un tipo di malware che deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; installando il programma o aprendo un file, inconsapevolmente, si esegue anche il codice *trojan* nascosto. Spesso è diffuso con gli allegati delle mail.

Uno **spyware** è un tipo di software che ,senza farsi vedere, raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete, etc...) senza il suo consenso, e li trasmette tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto.

Il **ransomware** è un malware la cui peculiarità è quella di introdursi in un sistema e bloccarne il funzionamento criptandone i dati. Poi avvine la richiesta di un riscatto (ransom) per poter ripristinare i dati, in caso contrario, i rischi sono due: che i dati vengano sottratti o rivenduti nel dark web.

- **Adottare soluzioni tecniche che proteggono dalle intrusioni nei nostri dispositivi**

IL PHISHING

Si tratta di una presa in giro dell'utilizzatore. Infatti ad essere attaccato non e' il sistema informatico in uso, quanto la psicologia (curiosità, insicurezza, ingenuità) dell'utente che viene ingannato e convinto ad agire in maniera sbagliata inviando a terzi informazioni "delicate" (password, codici di carta di credito, dettagli anagrafici).
Solitamente avviene con un messaggio di posta elettronica, apparentemente serio e ufficiale, inviato da agenzie e enti conosciuti (Poste, Banche, P.A., …), dove si comunica la necessità di cliccare su un link per comunicare dati o sbloccare una situazione. Non farlo, nessuno chiede mai dati in quel modo.
Può essere realizzato anche con SMS, e messaggi Whatsapp.
In questi casi l'unica protezione possibile è il sospetto e il "buon senso".

- **Diffidare delle richieste di dati riservati**
- **Non farsi ingannare da segnalazioni preoccupanti**
- **Comunicare agli istituti di riferimento**

LO SPOOFING

Il criminale si interpone nella comunicazione tra l'utente e agenzia (banca, istituti finanziari, Poste, ecc...). Ad essere attaccato è il meccanismo di comunicazione, dentro al quale si insinua il dispositivo del criminale per carpire dati riservati (password, codici di carta di credito, ecc...)
Quindi è possibile, ad esempio, che durante una normale comunicazione banca-utente per segnalare il codice temporaneo di accesso al conto corrente, il criminale insinui la richiesta delle credenziali. Non darle, nessuno chiede mai dati in quel modo.
Può essere realizzato con SMS, e messaggi Whatsapp.
L'articolo 10 del decreto legislativo 11/2010, ripreso nel decreto legislativo 218/2017, stabilisce che, se il cliente di una agenzia (istituto di credito, Poste, ecc...) nega di aver disposto un'operazione, tocca al prestatore di servizi di pagamento l'onere di dimostrare che l'autenticazione sia avvenuta in maniera corretta, ed eventualmente a rimborsare l'utente.

- **Attivare soluzioni di accesso a 2 fattori, se possibile su 2 canali diversi (PC e cell., Cell e token, ecc...)**

FURTO DI DATI

Di solito si tratta di credenziali di accesso a piattaforme (es.:home banking) in modo che poi qualcun altro le possa usare per vantaggio proprio.
Oltre ad utilizzare il phishing, viene anche usata la tecnica dello **sniffing**, cioè l'attività di intercettazione dei dati che transitano in una rete, solitamente il WiFi.
(Wikipedia)

- **Non usare WiFi pubblici per scambiare informazioni specie se riservate**
- **Cambiare le password originali dei propri WiFi con sequenze complesse ideate da noi.**

Per approfondire: https://menteinformatica.it/sicurezza/

BUONE PRATICHE

Il DIGITALE sotto la lente

Usare bene la RETE, che è ormai un bene comune, è una scelta responsabile.

- Usare la Rete solo per servizi utili ed evitare di fare circolare materiale che non sarà probabilmente più usato (spazzatura) ma che richiede energia per essere conservato.
- Nelle chat:
  - preferire i messaggi scritti agli audio-messaggi (7.000 volte più pesanti) e ai video-messaggi (anche 43.000 volte più pesanti)
  - Solo se necessario inviare gif animate, foto, video, ecc…, una loro copia resterà in memoria dei dispositivi vostro e del destinatario, contribuendo a riempirla.
- Evitare se possibile di fare foto e video con lo smartphone, ne viene inviata una copia sul Cloud a meno che sia stata disattivata tale funzione.
- Memorizzare i siti usati di frequente (ad esempio nei preferiti), non cercare con Google e poi cliccare (si impegna meno la Rete)
- Valutare l'utilizzo di software libero (solitamente meno famelico di risorse)

Il DIGITALE sotto la lente

- Bloccare la riproduzione automatica dei video (molti siti e Social ce l'hanno attivato)
- In videoconferenza disattivare la webcam, e anche il microfono se non si deve parlare.
- Ridurre l'uso del Cloud ai casi in cui si vogliono condividere informazioni (possono essere grandi moli di dati da trasferire e conservare), è consigliabile salvare i dati su dispositivi propri e imparare a farsi le copie di backup.
- Scegliere i servizi e le App da usare in base alla qualità e alla serietà dell'azienda che li offre e non solo perché sono già presenti sui device. Browser, messaggistica, notizie,… spesso sono il risultato di accordi commerciali e generano flussi importanti di dati anche non richiesti.
- Ripulire periodicamente i dispositivi dai media inviati e ricevuti con programmi di messaggistica (audio, immagini, video), e foto o video non più necessarie, in modo da liberare memoria e prolungarne l'efficienza nel tempo.
- Abbassare la qualità delle foto a meno che si intenda stamparle o proiettarle su grandi formati, occuperanno meno spazio e meno banda.
- Ridurre la risoluzione dei video fruiti in Rete per occupare meno banda (il 4K occupa 16 volte in più del Full HD), es.: è inutile guardare un video in 4K sullo smartphone o sul tablet, il 4K è necessario per la visualizzazione su TV di grande formato.

I PERICOLI

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 in Rete di immagini o video intimi senza il consenso dei protagonisti. Grazie alla IA questo materiale potrebbe essere prodotto artificialmente partendo dalla sola foto del viso.

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 (nomi, dati, foto).
- 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'esperessione 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)

I PERICOLI

di cui non si parla a sufficienza

Profilazione, Previsione, Sorveglianza

RACCOLTA e registrazione di quanti più dati possibili diretti o indiretti personali o tecnici (metadati), per ottenere, grazie a sofisticate **ANALISI** con sistemi di Intelligenza Artificiale, una **PROFILAZIONE** degli utenti, cioè una schedatura con interessi, orientamenti, abitudini, ecc…

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.

In particolare è possibile, elaborando opportunamente i profili in modo statistico, **prevedere il comportamento** di una certa categoria di profili circa un determinata situazione o tema o questione...

… oppure è possibile fare arrivare, a determinati gruppi di profili specifici, dei messaggi che possono **orientare il pensiero e le scelte degli utenti**.

Dove e quando vengono raccolti?

•Dallo **smartphone**: posizione, 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, dove si clicca, dove si legge;
- coi cookies: per garantire il funzionamento (tecnici), o per 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** che pubblichiamo sui social: data e ora, posizione, identificativo del dispositivo, account, testo, immagini, like, condivisioni.

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)

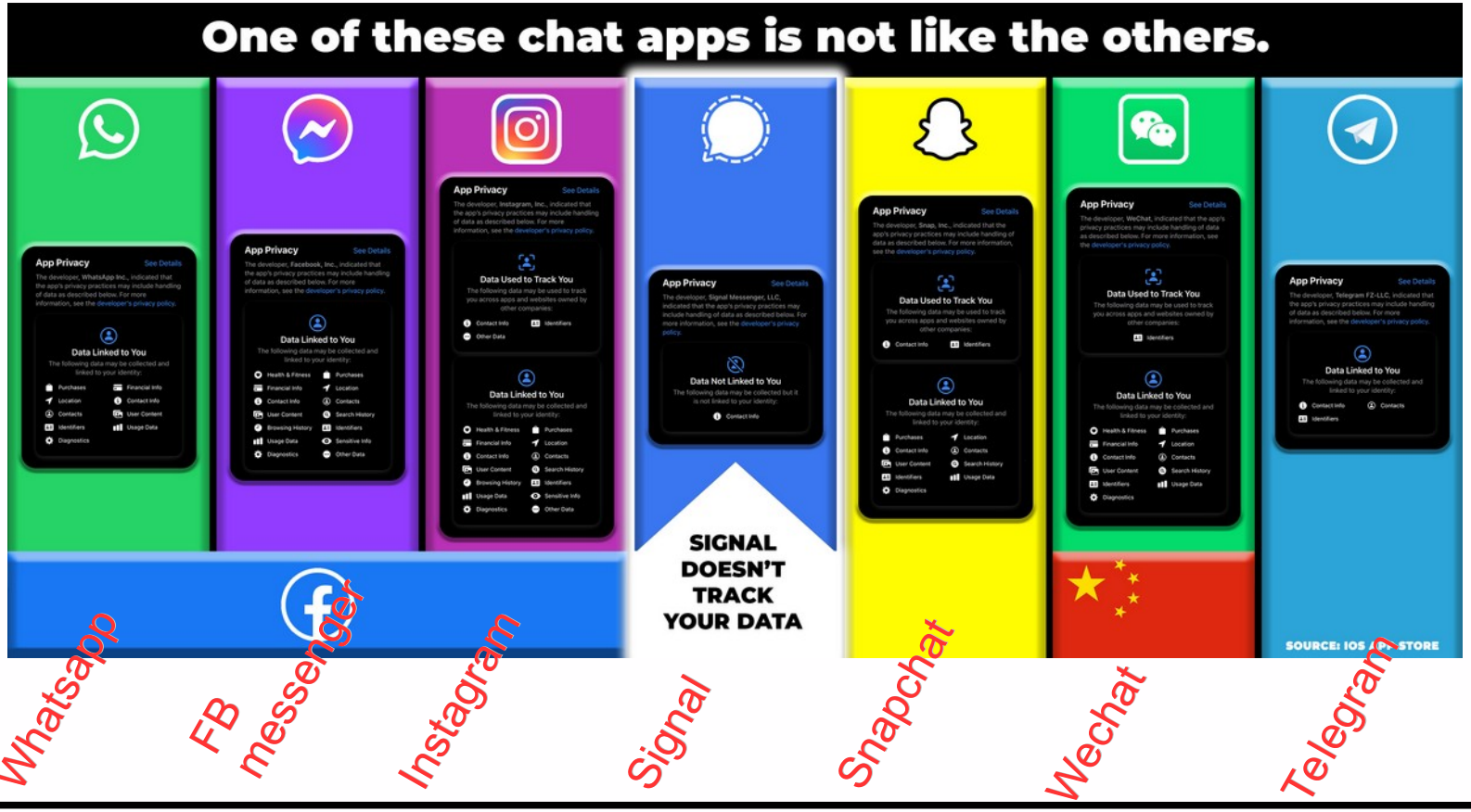
Microsoft (Redmond): Windows, Office 365, Teams, …

Comunemente indicati con l'acronimo **GAFAM**

Dove guadagna Google: https://www.ilsole24ore.com/art/google-ecco-come-fa-big-g-guadagnare-montagna-soldi--AEZUk26E

Un esempio: le App di messaggistica

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



Il DIGITALE sotto la lente

Sapendo che le App commerciali di messaggistica ...

- raccolgono dati e metadati senza una reale necessità tecnica
- la crittografia End to End è dichiarata ma non è possibile verificare
- sono prodotte da aziende che basano il loro profitto sulla vendita dei dati raccolti

...è lecito chiedersi come possiamo proteggerci quando le usiamo, specie in situazioni che richiedono riservatezza come:

- Gruppi di genitori delle scolaresche
- Comunicazioni di servizio tra i funzionari della P.A. e 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!

Il DIGITALE sotto la lente

COME DIFENDERCI

- Ricordiamo che non avremo più potere su quanto pubblichiamo.
- Ricordiamo che Internet non dimentica nulla (mantiene 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, 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)

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, tra situazioni sensazionali o divertenti, sport, contenuti di violenza, sesso, odio, 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 viene a conoscenza della totalità delle informazioni (tra le quali si sono anche quelle contrastanti).
Questo spiega le **estremizzazioni** di pensieri e comportamenti di certi gruppi di persone.

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.

Per approfondire: https://pressbooks.pub/intelligenzaartificiale/ capitoli 12 e 13.

DIPENDENZE

•**dalla marca:** tendenza ad utilizzare dispositivi di una certa marca

•**dalle applicazioni digitali** (lock-in): adattarsi ad usare soluzioni software (programmi, app, piattaforme, …) imposte dal mercato; non ci si preoccupa di valutare alternative più adatte, più etiche, che considerino maggiormente libertà e privacy personali.
Spesso si sente dire "… mandami un whatsapp …" o "… ti mando un file excel …", che inducono gli interlocutori ad utilizzare quei programmi, si diventa così parte del meccanismo. Ma sono frasi simili a "… vieni a casa con la Fiat 500!".
Le Big Teck 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.

•**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.

CONCESSIONE ACRITICA DI CREDITO

Frasi come “L’ha detto la TV” o “L’ho visto su Internet” ...
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 generativa** (Gemini, ChatGPT) perché essa è in grado di produrre contenuti realistici e credibili ma non necessariamente veri. Chi non ha competenze sull’argomento trattato o pensiero critico insufficiente può essere ingannato molto facilmente.

TECNOLOGIE E FENOMENI A CUI PRESTARE ATTENZIONE

INTELLIGENZA ARTIFICIALE (IA)

Se ne sente parlare quotidianamente, spesso in modo superficiale o errato.

La sua peculiarità è quella di immagazzinare, nella fase di addestramento, una quantità impressionante di informazioni e di casistiche.

Computer estremamente potenti sono di grado di recuperare velocemente ciò che, secondo loro, è associabile alle situazioni che gli vengono presentate, poi le confezionano secondo i canoni più adatti a chi fa la richiesta (testi, immagini, musiche, ecc…).

Non è in grado di valutare se ciò che produce sia vero, etico, moralmente accettabile, dipende dalla qualità dei dati usati durante l'apprendimento.

Chi imposta gli algoritmi e i dati da utilizzare nella fase di addestramento e della fase operativa quale IMPOSTAZIONE darà al sistema?

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/

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.

BUONE PRATICHE

- Essere sempre attenti e un po' sospettosi.
- Considerare gli strumenti digitali come STRUMENTI!
- Non lasciarsi travolgere da realtà virtuali come i videogiochi 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 lasciarci condizionare dai contenuti che vengono proposti.
  - verificare le notizie e le fonti prima di condividerle
  - mantenere un pensiero critico rispetto a ciò che viene proposto.
- Internet non dimentica nulla, attenzione a ciò che si pubblica.

Il DIGITALE sotto la lente

BUONE PRATICHE

Interessante CANDID CAMERA Belga

https://youtu.be/qYnmfBiomlo

IMPATTO AMBIENTALE DEL DIGITALE

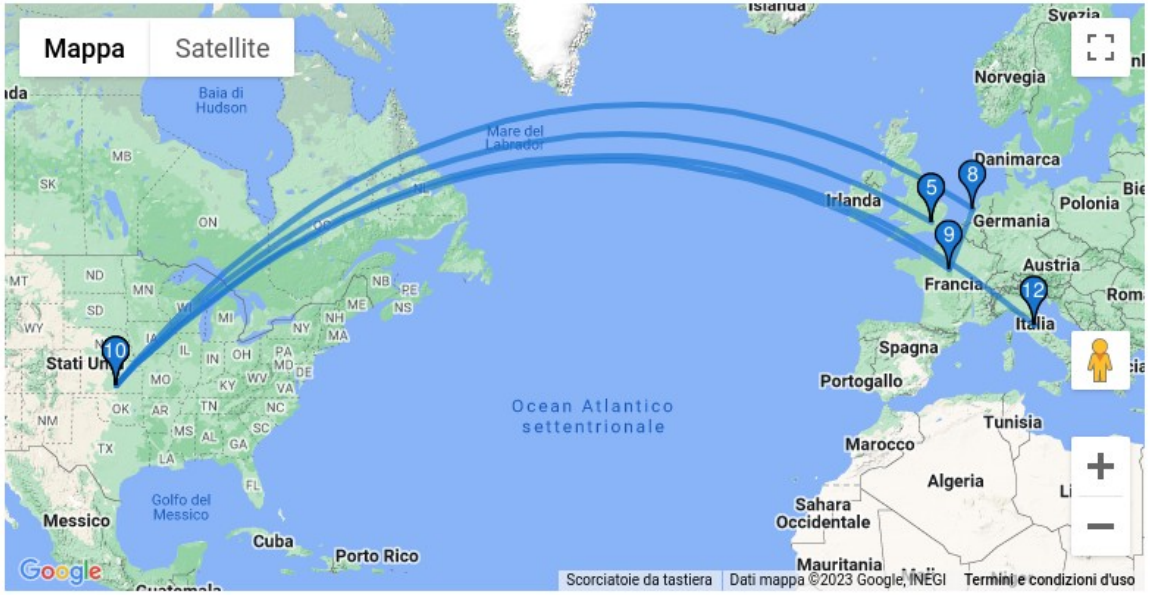
Il DIGITALE sotto la lente

È pensiero comune che il digitale permetta un minor impatto sull'ambiente rispetto ai mezzi tradizionali.

Ma è così veramente?

Il DIGITALE sotto la lente

IMPATTO AMBIENTALE
La navigazione



traceroute to goggle.it (195.110.124.133), 30 hops max

Hop	Host	IP	Time (ms)
1	dgw1-wan-uk-lon1.ipv4.upcloud.com	83.136.248.1	0.157ms
2	100.69.6.161	100.69.6.161	0.270ms
3	172.17.255.217	172.17.255.217	0.275ms
4	172.17.255.6	172.17.255.6	0.221ms
5	te0-3-1-4.rcr51.lon17.atlas.cogentco.com	149.11.141.9	0.491ms
6	be2971.ccr42.lon13.atlas.cogentco.com	154.54.39.81	1.152ms
7	be2869.ccr22.lon01.atlas.cogentco.com	154.54.57.162	1.441ms
8	ae5.cr12-lon1.ip4.gtt.net	154.14.40.57	1.434ms
9	et-5-1-0.cr0-mil2.ip4.gtt.net	89.149.184.57	21.230ms
10	simply-transit-gw.ip4.gtt.net	77.67.90.194	31.549ms
11	81.88.51.250	81.88.51.250	41.018ms
12	opus.register.it	195.110.124.133	31.413ms

Percorso del pacchetto quando ho digitato **google.it** *(https://gsuite.tools/traceroute)*

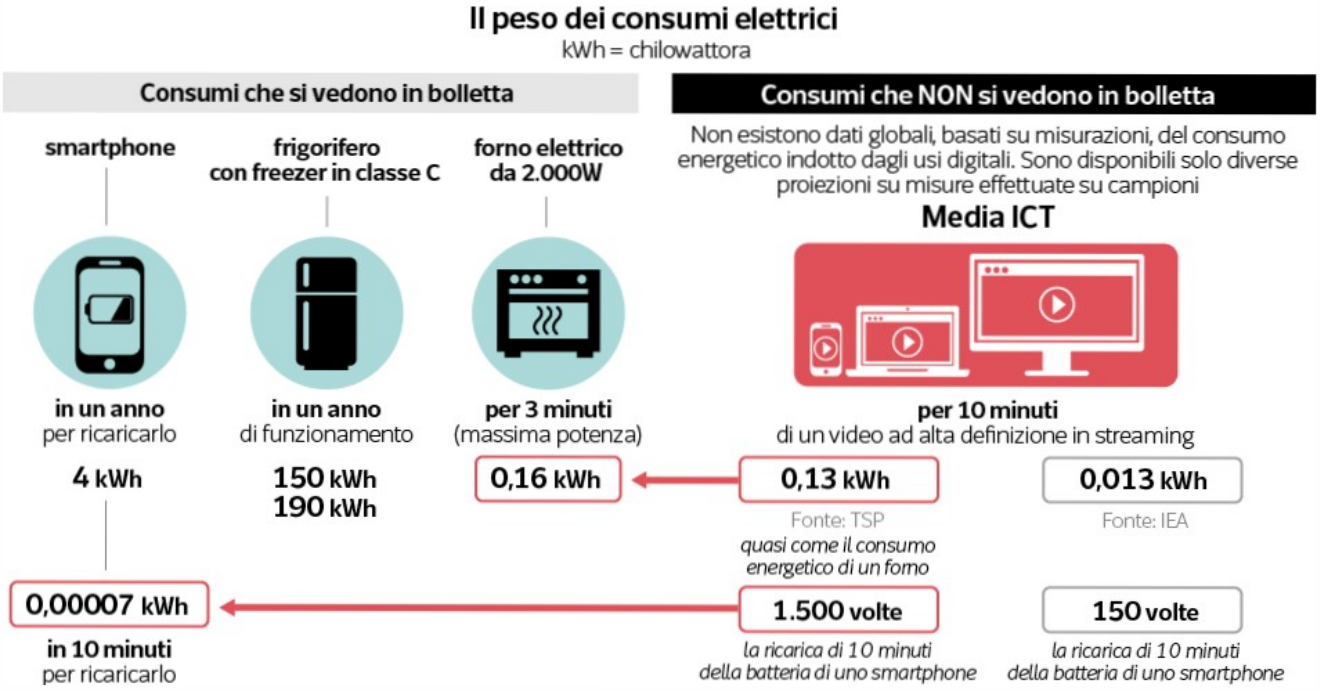
Ma non fa sempre lo stesso percorso!

Il DIGITALE sotto la lente

IMPATTO AMBIENTALE

Lo streaming

10’ di streaming
=
3’ di un forno elettrico
o
18.570’ di carica dello smartphone (12,8 giorni)



Data Room di Milena Gabanelli - gennaio 2021

https://www.corriere.it/dataroom-milena-gabanelli/emissioni-co2-ambiente-internet-quanto-inquina-nostra-vita-digitale-effetto-serra-consumi-invisibili-streaming-app-video/eb680526-5363-11eb-b612-933264f5acaf-va.shtml

Alcuni calcoli (approssimativi, le aziende non forniscono dati precisi. Fonte TSP):

Secondo i valori presentati 1 flusso di stream continuo consuma 6830 Kwh/anno
Un trasmettitore della Rai consuma 438.000 Kwh/anno = 64 flussi stream

IMPATTO AMBIENTALE
Altri esempi e perplessità

L'IA richiede computer estremamente potenti con enormi capacità di memorizzazione. Addestrare una IA per capire la frase "come e dove è stato sconfitto il corso più famoso" emette CO_2 5 volte più di quella emessa dalla vita media di una automobile, produzione inclusa. *(Data Room di Milena Gabanelli 10 gennaio 2021)*.

C'è mancanza di trasparenza da parte delle aziende che sviluppano reti neurali e sistemi di IA, sembra che l'impatto del solo addestramento di GPT-3 avrebbe generato circa 550 tonnellate di CO2. *(https://www.greenme.it/scienza-e-tecnologia/impatto-ambientale-intelligenza-artificiale/)*

Alcuni calcoli (approssimativi, le aziende non forniscono dati precisi):

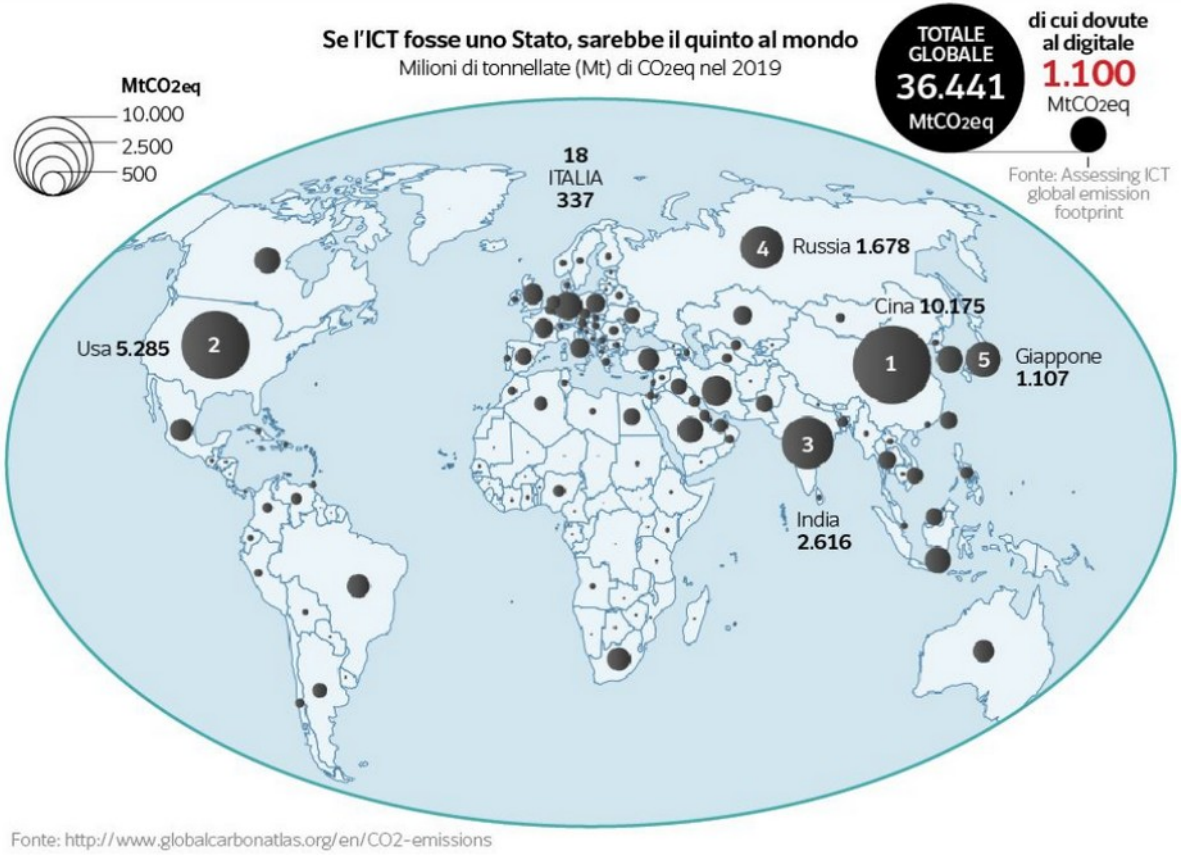
Al 26/01/2023 ChatGPT sembra utilizzasse 30.000 GPU (Grafic Process Unit).
Le GPU di alte prestazioni per la IA consumano a pieno carico 250-300W.
300X30.000x24 = 216.000.000w/giorno = 216 Mwh/giorno
Meta intende acquistarne 350.000 GPU (10 Migliardi di dollari)

Il DIGITALE sotto la lente

IMPATTO AMBIENTALE
Consumo & Emissioni

IL FUNZIONAMENTO DELL'ITC* è responsabile del **5,5%** del consumo globale di **energia elettrica**.

… e del **3,7%** delle **emissioni di CO_2** equivalente.
(dati del 2019)



Sito consigliato:
Data Room di Milena Gabanelli

***ICT:** Information & Communica Tecnology - insieme dei dispositivi digitali presenti nel mondo, compresi i server che ospitano siti e piattaforme e quelli che conservano i dati in rete.*

...E I RIFIUTI ELETTRONICI?

- Statisticamente la vita media di uno smartphone è di 20 mesi, per un PC portatile è di 3-5 anni.
- Vengono proposti dispositivi sempre più sottili, questi richiedono una più massiccia integrazione dei componenti che porta a una minore possibilità di accesso per eventuali riparazioni.
- Il continuo rinnovamento dei software, non sempre necessario, e tecniche che inducono alla obsolescenza programmata obbligano spesso a sostituire i dispositivi.

CONSEGUENZA: enorme produzione di rifiuti elettronici (RAEE*).

* RAEE = Rifiuti da Apparecchiature Elettriche ed Elettroniche

BUONE PRATICHE: dispositivi

- TV e monitor, più sono grandi più consumano
- Spegnerli e scollegarli dalla rete elettrica (no stand-by, sono comunque accesi e spesso operativi)
- Usare i dispositivi fino a fine vita
- Riuso:
  - dispositivi datati possono essere riutilizzati per usi meno pesanti
  - Utilizzare software, solitamente liberi, meno pesanti di quelli più diffusi per ottenere il PC efficiente più a lungo. (https://alternativeto.net/, https://www.lealternative.net/, http://www.theopendvd.it/)
  - I PC, con modifiche abbastanza economiche e l'uso di sistemi operativi liberi, come Linux, possono ritornare perfettamente efficienti (e molto sicuri).
- Valutare gli smartphone modulari e riparabili, offerti da alcuni produttori https://shop.fairphone.com/it/#electronic-waste-neutral
- Utilizzo consapevole e meno compulsivo (rif.: ridurre l'uso della memoria sul cell).
- Vedere se nella propria zona sono presenti REPAIRS CAFÉ (https://www.nonsprecare.it/repair-cafe)

Il DIGITALE sotto la lente

https://www.vatican.va/content/francesco/it/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.html

...limitare al massimo l'uso delle risorse non rinnovabili, moderare il consumo, massimizzare l'efficienza dello sfruttamento, riutilizzare e riciclare. Affrontare tale questione sarebbe un modo di contrastare la cultura dello scarto...

Paragrafo 22

GRAZIE PER L'ATTENZIONE

I **L**inux **U**sers **G**roup Italiani
organizzano annualmente
il **Linux Day**
giornata Nazionale di
Linux e del Software Libero
Ultimo sabato di Ottobre

A Mantova è attivo il

Linux **U**sers **G**roup **Man**tova
http://www.lugman.org
groups.google.com/group/lugman

Sitografia

https://gsuite.tools/traceroute

https://www.altroconsumo.it/hi-tech/computer-portatili/news/windows-10

https://www.ilsole24ore.com/art/apple-e-samsung-multa-antitrust-obsolescenza-programmata-AEtILnUG

https://www.wired.it/internet/regole/2019/07/16/office-365-privacy/

https://www.zeusnews.it/n.php?c=28015

https://www.repubblica.it/tecnologia/social-network/2018/04/04/news/scandalo_facebook-cambridge_analytica_i_profili_social_coinvolti_sono_87_milioni-192991515/

https://www.repubblica.it/tecnologia/sicurezza/2020/03/27/news/zoom_l_app_per_videoconferenze_condivide_i_dati_con_facebook-252458567/

https://www.zeusnews.it/n.php?c=28547

http://www.ecis.eu/2009/03/microsofts-history-of-anticompetitive-behaviour-and-consumer-harm/

https://www.solotablet.it/blog/tabulario/google-trasparenza-e-sorveglianza

https://www.agendadigitale.eu/cultura-digitale/nanotargeting-cosi-facebook-influenza-il-dibattito-politico-come-possiamo-difenderci/

https://www.huffingtonpost.it/entry/qanon-e-fake-news-sul-voto-usa-facebook-sapeva-linchiesta-del-new-york-times_it_6174165be4b010d933117739/

Sitografia

https://www.tomshw.it/hardware/facebook-non-sarebbe-in-grado-di-controllare-adeguatamente-i-dati-degli-utenti/

https://feddit.it/post/1499?scrollToComments=true

https://www.federprivacy.org/informazione/punto-di-vista/whatsapp-legge-i-tuoi-messaggi-altro-che-crittografia-end-to-end

https://www.open.online/2021/10/25/usa-inchiesta-facebook-papers/

https://www.corriere.it/economia/tasse/21_maggio_04/per-amazon-2020-d-oro-44-miliardi-ricavi-zero-euro-tasse-pagate-746028c4-acd1-11eb-b89d-9c2f0a2ddccd.shtml

https://www.vatican.va/content/francesco/it/speeches/2019/november/documents/papa-francesco_20191114_convegno-child%20dignity.pdf

https://www.corriere.it/tecnologia/24_febbraio_01/i-social-a-processo-negli-stati-uniti-avete-le-mani-sporche-di-sangue-bd5f5c16-f5ba-4ed4-961a-e262c09f2xlk.shtml?refresh_ce

Ebook: IA per gli insegnanti: un libro aperto (https://pressbooks.pub/intelligenzaartificiale/)