

ILS Este

LINUX DAY 2026

IL MONDO DIGITALE OGGI E COME IL SOFTWARE LIBERO PUÒ CAMBIARLO

presentato da **Fabio 'Loviuz' Lovato**

este.linux.it

CC 0

🎉 COS'È IL LINUX DAY?

Una giornata mondiale dedicata a Linux e al software libero

Si celebra ogni **4° sabato di ottobre** di ogni anno

Promosso da **ILS (Italian Linux Society)**

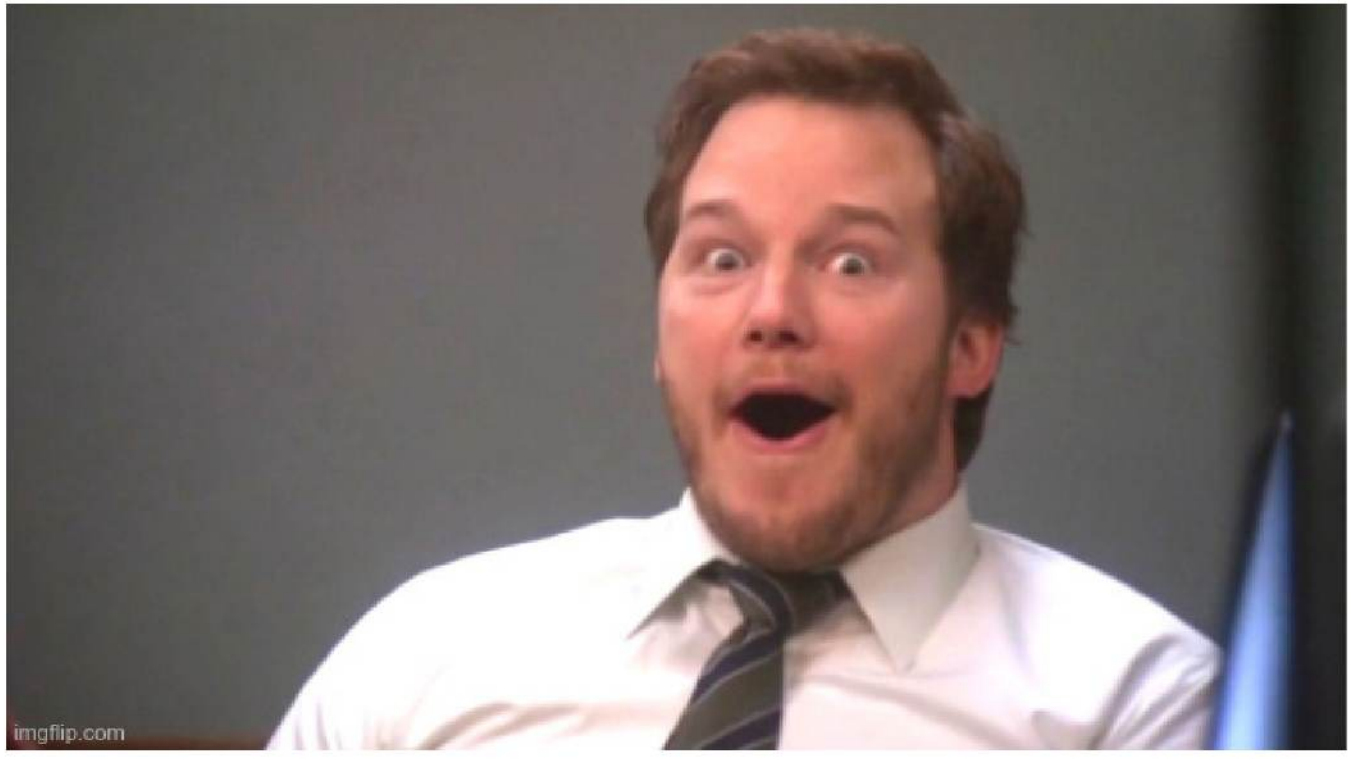
Circa una cinquantina di eventi in tutta Italia

Conferenze, workshop, installazioni e dimostrazioni

DOVE?

LinuxDay.it

🎮 GIOCHIAMO



CASO 1

John Anderton entra in un centro commerciale, e mentre cammina vede la pubblicità del suo prodotto preferito, trova un ologramma di una persona che gli consiglia dei vestiti del suo stile preferito e su un maxi-schermo, attraverso una telecamera che riconosce il suo volto, viene proiettata la pubblicità della sua birra preferita: una Guinness.

CASO 1 - 🎬 MINORITY REPORT



CASO 1 - 🎬 MINORITY REPORT

Film del 2002 con Tom Cruise. Ambientato nel 2054, in un futuro distopico, dove il protagonista fa parte di una sezione "pre-crime", dove si prevengono gli omicidi usando tecnologia e algoritmi. Un sistema di sorveglianza di massa vede tutto e suggerisce dove e cosa fare per prevenire il crimine prima che avvenga.

CASO 2

Un uomo che sta attraversando un divorzio acquista un computer con una voce che si presenta con un nome e impara in fretta chi è lui: le sue email, i suoi documenti, le sue abitudini. Ridono insieme. Lei gli fa notare quando è sulla difensiva, gli dice cose che nessun amico ha mai avuto il coraggio di dirgli.

Finché lui non le fa la domanda ingenua: *"Parli anche con qualcun altro, quando non parli con me?"*. La risposta è disarmante: *"Sì, sto parlando con altre 641 persone in questo momento, e*

CASO 2 - 🎬 HER



CASO 2 - 🎬 HER

Film del 2013. La storia d'amore tra un uomo e un sistema operativo è anche il ritratto più lucido mai girato sul legame con gli assistenti AI: l'illusione di essere l'unica persona importante per un sistema progettato per farci sentire capiti, dove i limiti sono nascosti dal design.

Con gli attuali assistenti vocali e chatbot il confine è sottilissimo. Il problema non è "l'AI che si innamora" ma chi controlla il modello, dove vanno a finire le conversazioni e quanto il modello ci spinge a fidarci.

CASO 3

L'agenzia delle imposte di un ricco e digitalizzato Paese europeo usa un algoritmo per scovare le frodi negli assegni destinati all'asilo dei bambini. Lo strumento non cerca prove: assegna punteggi di rischio e segnala con più forza le famiglie con la doppia nazionalità. Le sue decisioni, sigillate da un "sistema riservato", non sono quasi mai contestabili.

CASO 3

Decine di migliaia di genitori innocenti vengono accusati di frode: devono restituire decine di migliaia di euro ciascuno, gli assegni si fermano, famiglie finiscono sul lastrico, bambini vengono tolti alle loro case. Anni dopo arriva la verità: dietro le accuse non c'erano prove, solo pregiudizio codificato e l'arroganza di una macchina incontestabile. Il governo intero si dimette.



CASO 3 - 💯 REALTÀ

È lo scandalo olandese degli assegni famiglia ("toeslagenaffaire"): l'agenzia fiscale olandese accusò con **metodi algoritmici discriminatori** circa **26.000 famiglie**, e nel gennaio 2021 l'intero governo Rutte si dimise in blocco. https://www.tpi.it/esteri/olanda-premier-mark-rutte-dimissioni-20210115727938/

CASO 4

Carl stava guardando la tv, a un certo punto vide qualcosa di strano, si avvicinò e a fianco trovò un un libretto con su scritto: *"Se le parole che pronunci includono informazioni personali o riservate, tali informazioni saranno tra i dati acquisiti e trasmessi a terzi."* Carl scoprì che non poteva più parlare con amici mentre era nella sua casa, perché ogni dialogo e ogni discussione o confessione con persone fidate poteva essere registrata. Iniziò un lungo periodo di paranoia totale.


1
2
3
4
5
6
7
8
9
TTX/MIX
0
PRE-CH
MUTE
P
MENU
SMART HUB
GUIDE

CASO 4 - 💯 REALTÀ

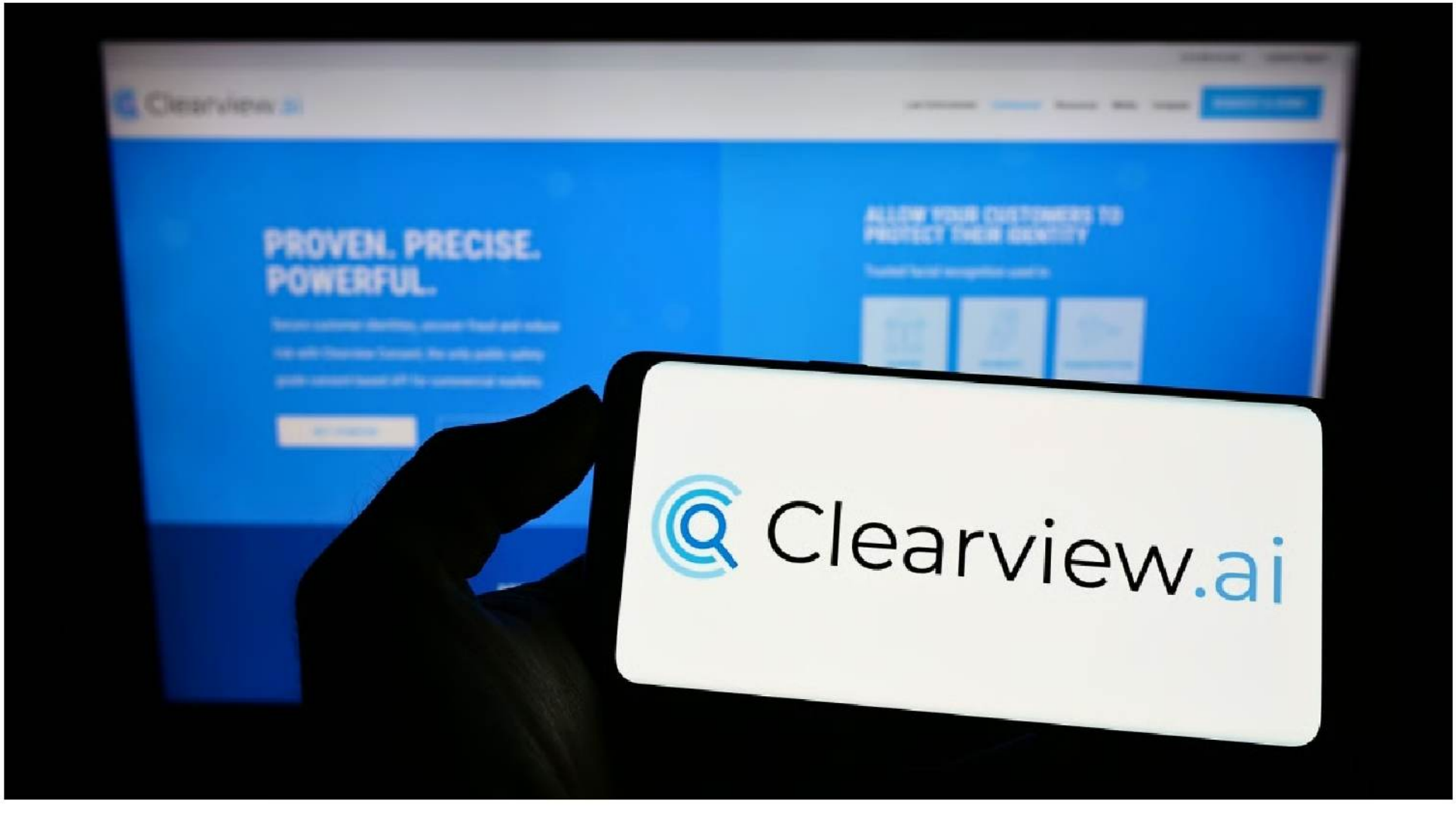
Nel 2015 la privacy policy delle **Samsung Smart TV** mise in guardia gli utenti: con il **riconoscimento vocale attivo**, le frasi pronunciate davanti alla TV potevano essere registrate e trasmesse a terze parti che le trascrivevano. La rete impazzì per il paragone immediato con 1984, e EPIC presentò reclamo alla FTC (Federal Trade Commission).

https://arstechnica.com/tech-policy/2015/02/privacy-advocate-tells-ftc-that-samsung-smart-tvs-are-deceptive/

CASO 5

Un'azienda tecnologica, quasi in segreto, **raccoglie foto da tutti i social network** del mondo: festeggiamenti di compleanno, vacanze, vecchie foto di classe, qualunque immagine. Ogni volto viene trasformato in una **firma biometrica**. Il database finale conta **decine di miliardi di immagini**, più di tre per ogni abitante del pianeta. Chi lo possiede lo vende a **forze di polizia e agenzie governative**: basta una foto scattata per strada per avere nome e cognome.

CASO 5 - 💯 REALTÀ



CASO 5 - 💯 REALTÀ

Clearview AI ha costruito un database di circa **30 miliardi di immagini** prelevate senza permesso da social e siti web, vendendo ricerche facciali alle forze dell'ordine: quasi **un milione di ricerche già fatte dalla polizia statunitense**. Vietata o multata in diversi Paesi (Regno Unito, Francia, Italia e, nei Paesi Bassi, la più alta: 30 milioni di euro), ma ancora in piena attività.

https://ihal.it/clearview-ai-multanei-paesi-bassi-per-violazione-privacy/

CASO 6

Un padre furibondo irrompe in un supermercato: *"State mandando a mia figlia coupon per vestiti da neonato e culla! È una studentessa del liceo! È una mancanza di rispetto!"* Il direttore si scusa, ritira gli inviti, offre buoni spesa.

CASO 6

Una settimana dopo il padre richiama il direttore. La voce è diversa, imbarazzata: *"Ho parlato con mia figlia. Avevate ragione voi."* La ragazza era incinta. Il sistema di fidelizzazione lo sapeva prima della famiglia. Aveva notato il cambio di abitudini: lozioni senza profumo, integratori di vitamine, e aveva calcolato una probabilità di gravidanza, con tanto di data presunta del parto.

CASO 6 - 💯 REALTÀ



CASO 6 - 💯 REALTÀ

È il celebre caso **Target** del 2012, raccontato dallo stesso statistico dell'azienda: l'analisi degli acquisti aveva rivelato una gravidanza prima che la famiglia ne fosse informata. L'azienda, dopo lo scandalo, iniziò a mescolare le offerte per renderle meno inquietanti, ma senza smettere di profilare.

I dati sono inferenza: dal "cosa compri" al "chi sei" e "cosa farai". https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-

CASO 7

Stefan era un appassionato di tecnologia ma anche una persona molto sportiva. Dopo aver acquistato uno smartwatch super-tecnologico, inizia un allenamento e controlla i progressi nell'app collegata: percorsi, frequenza cardiaca, punteggio, tutto nella sua comoda app.

CASO 7

Un giorno, osservando bene alcune zone remote del pianeta, appaiono strane scie: anelli perfetti di corridori che girano in tondo, più e più volte, nel bel mezzo di deserti e giungle dove "nessuno" dovrebbe correre. Sono **pattuglie di soldati** che si allenano intorno a **basi militari segrete**. La mappa delle loro attività rivela, con precisione millimetrica, la posizione di installazioni che non comparivano su nessuna mappa.

CASO 7 - 💯 REALTÀ



Nathan Ruser @Nrg8000 · Jan 27

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee… … It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

CASO 7 - 💯 REALTÀ

Nel 2018 la **Strava Global Heatmap**, costruita con i dati di fitness condivisi dagli utenti, rivelò percorsi e perimetri di basi militari statunitensi e alleate in Siria, Afghanistan e altrove, perché i soldati usavano i fitness tracker personali

Non esiste un "dato innocuo". Anche i dati più banali come passi, percorsi, frequenze, se aggregati diventano informazioni sensibili. Ed è esattamente questo il meccanismo della sorveglianza di massa: non serve raccogliere segreti, basta raccogliere tutto.

CASO 8

Nel 2015, un'azienda di analisi dei dati sostiene di poter costruire il profilo psicologico di una persona partendo da una manciata dei suoi "like": le pagine che segue, i meme che condivide, le canzoni che ascolta. Un modello che descrive quanto sei estroverso, coscienzioso, vulnerabile alle paure, ricettivo alla rabbia.

CASO 8

Senza che i diretti interessati lo sappiano, il profilo di decine di milioni di persone viene usato per mostrare pubblicità politiche su misura - messaggi diversi a persone diverse, ciascuno calibrato per spostare opinioni un voto alla volta. L'azienda lavora per una campagna elettorale e sembra che questa sia la mossa vincente che spopolerà. Il sogno di ogni politico.

CASO 8 - 💯 REALTÀ



CASO 8 - 💯 REALTÀ

Lo scandalo Cambridge Analytica: i dati di profili Facebook di decine di milioni di utenti (stime fino a 87 milioni) furono usati per profilazione psicografica e micro-targeting politico, inclusa la campagna USA del 2016 di Donald Trump e la Brexit. Non ci sono prove esplicite che i 2 successi politici siano esplicitamente derivanti da queste manovre.

https://it.wikipedia.org/wiki/Cambridge_Analytica

CASO 9

Un consulente tecnico, dipendente di un'appaltatrice governativa, attraversa ogni giorno i controlli di sicurezza del suo ufficio, dove i colleghi lavorano a un sistema globale che intercetta comunicazioni in massa. Il sistema non ha nomi di sospetti: raccoglie tutto, di tutti, per sempre. Dalle email alle videochiamate, dalle ricerche ai metadati.

CASO 9

Un giorno l'uomo chiede a un collega di tenere in ufficio un normalissimo cubo di Rubik. All'interno, nascoste, ci sono le schede di memoria con i documenti che provano tutto. Le porta fuori sotto gli occhi delle guardie. Poche settimane dopo, da una stanza d'albergo a Hong Kong, rivela al mondo il programma di sorveglianza di massa. Ha ventinove anni e sa che non potrà più tornare a casa.

CASO 9 - 💯 REALTÀ



CASO 9 - 💯 REALTÀ (+ FILM)

Edward Snowden e le rivelazioni del 2013 su PRISM e i programmi di **sorveglianza di massa** della NSA: la raccolta indiscriminata di comunicazioni tramite la collaborazione delle grandi piattaforme tecnologiche. È il caso che ha cambiato per sempre il dibattito su privacy, crittografia e sorveglianza di massa.

https://it.wikipedia.org/wiki/Cambridge_Analytica

CASO 10

Il destino di ogni essere umano viene scritto il giorno del concepimento: un'analisi genetica stabilisce le probabilità di ogni malattia, la longevità stimata, le attitudini. Lo Stato non vieta nulla a nessuno: si limita a "misurare", ma assicurazioni, banche e datori di lavoro hanno libero accesso al profilo, e così ogni porta si apre o si chiude in base a un referto.

CASO 10

Un ragazzo nato con una cardiopatia e una stima di vita di trent'anni sogna di viaggiare nello spazio. È la posizione sociale più bassa possibile: "non valido". Per realizzarsi acquista di nascosto l'identità genetica di un altro, e vive ogni giorno terrorizzato che un singolo capello o una goccia di sangue possano smascherarlo.

CASO 10 - GATTACA



CASO 10 - 🎬 GATTACA

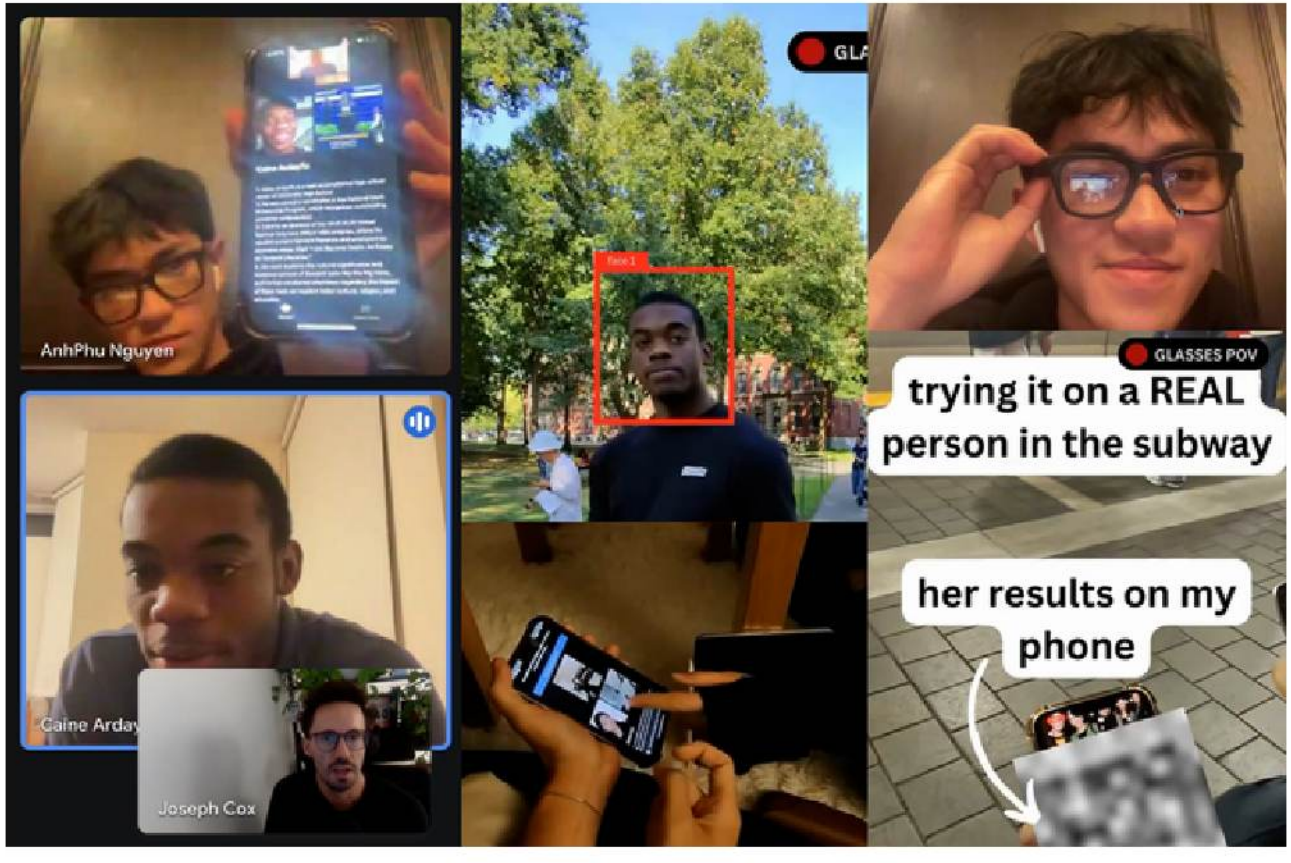
Film del 1997, regia di Andrew Niccol. Il film ha inventato un termine preciso, "genoismo", la discriminazione genetica. E la cosa che spaventa davvero non è il futuro che mostra, ma il presupposto che dai dati si possa predire il valore di una persona, così come lo sono la profilazione per la pubblicità in rete, gli algoritmi di selezione del personale, dei sistemi di credito.

https://it.wikipedia.org/wiki/Cambridge_Analytica

CASO BONUS

Due studenti universitari comprano un paio di occhiali intelligenti che chiunque può trovare in commercio, li collegano a un servizio di riconoscimento facciale e a database di foto pubbliche. Il costo dell'operazione è irrisorio rispetto a ciò che ottengono: passeggiano per la metropolitana, e basta guardare una persona perché sul loro display compaiano nome, cognome, indirizzo, numero di telefono, profili social e persino il numero di matricola universitaria.

CASO BONUS - 💯 REALTÀ



CASO BONUS - 💯 REALTÀ

È "I-XRAY" (settembre 2024): due studenti di Harvard hanno collegato gli occhiali Ray-Ban Meta a sistemi di riconoscimento facciale per identificare in tempo reale sconosciuti in pubblico e recuperarne i dati, pubblicando la dimostrazione come avvertimento

https://www.dagospia.com/cronache/occhio-privacy-studenti-harvard-dimostrato-gli-occhiali-smart-ray-ban-410273

IL GIOCO È TERMINATO



QUALI SONO I RISCHI DELLA TECNOLOGIA DI "OGGI"?



QUALI SONO I RISCHI DELLA TECNOLOGIA DI "OGGI"?

- **Profilazione** e **Sorveglianza**
- Telefoni e **dipendenza**
- **Persuasione** dei sistemi di IA
- **Un account ovunque:** viviamo in piazze digitali con un cartellino di riconoscimento
- **Obsolescenza:** dispositivi che durano poco, con spinta al consumismo e allo sfruttamento dell'ambiente

"AI MIEI TEMPI..."



"AI MIEI TEMPI..."

- **Profilazione e Sorveglianza:** pubblicità online ridotta e profilazione quasi inesistente
- **Più consapevolezza:** la tecnologia era solo per persone esperte che dovevano imparare
- **Accesso libero:** su molti siti o servizi online non c'era bisogno di creare un account (vedi ora il paywall)
- **Riuso:** l'hardware si riparava di più e non c'erano limitazioni software

LA SOLUZIONE?



SOFTWARE LIBERO



SOFTWARE LIBERO

- software che posso **usare, studiare, modificare, condividere**
- **no vincoli** a vita con un'azienda/entità (lock-in)
- **sovranità digitale**: ho potere su ciò che è mio

~~**PROFILAZIONE E SORVEGLIANZA**~~

FEDIVERSO

- **decentralizzazione:** nessuna gestione centrale, ma tante comunità senza scopo di lucro (federazione)
- **contenuti cronologici:** niente algoritmi, per ridurre dipendenza e uso tossico dei social
- **protocolli aperti** e portabilità dei dati
- moderazione delegata alla **comunità:** ogni piazza ha le sue regole

Parole chiave: Mastodon, Pixelfed, Peertube

~~TELEFONO E DIPENDENZA~~

MENO "WOW", PIÙ CONSAPEVOLEZZA

- **notifiche ridotte all'osso:** nessuno ti deve vendere alcunché
- **uso intenzionale:** scegli tu le app, non quelle preinstallate
- **educazione digitale:** capire come funzionano le cose attraverso gruppi come il nostro (LUG, repair cafè, ecc)

Parole chiave: F-Droid

~~UTENZE OVUNQUE~~

SERVIZI LIBERI CON SOFTWARE LIBERO

- **niente utenze dove non serve:** per modificare un PDF non devo creare un utente su una piattaforma o accettare cookie di profilazione da 300 broker di dati
- **portabilità:** scegli i formati aperti
- **self-hosting:**preferire applicazioni che archiviano i dati a casa propria

Parole chiave: ServiziLiberi.it, LibreOffice

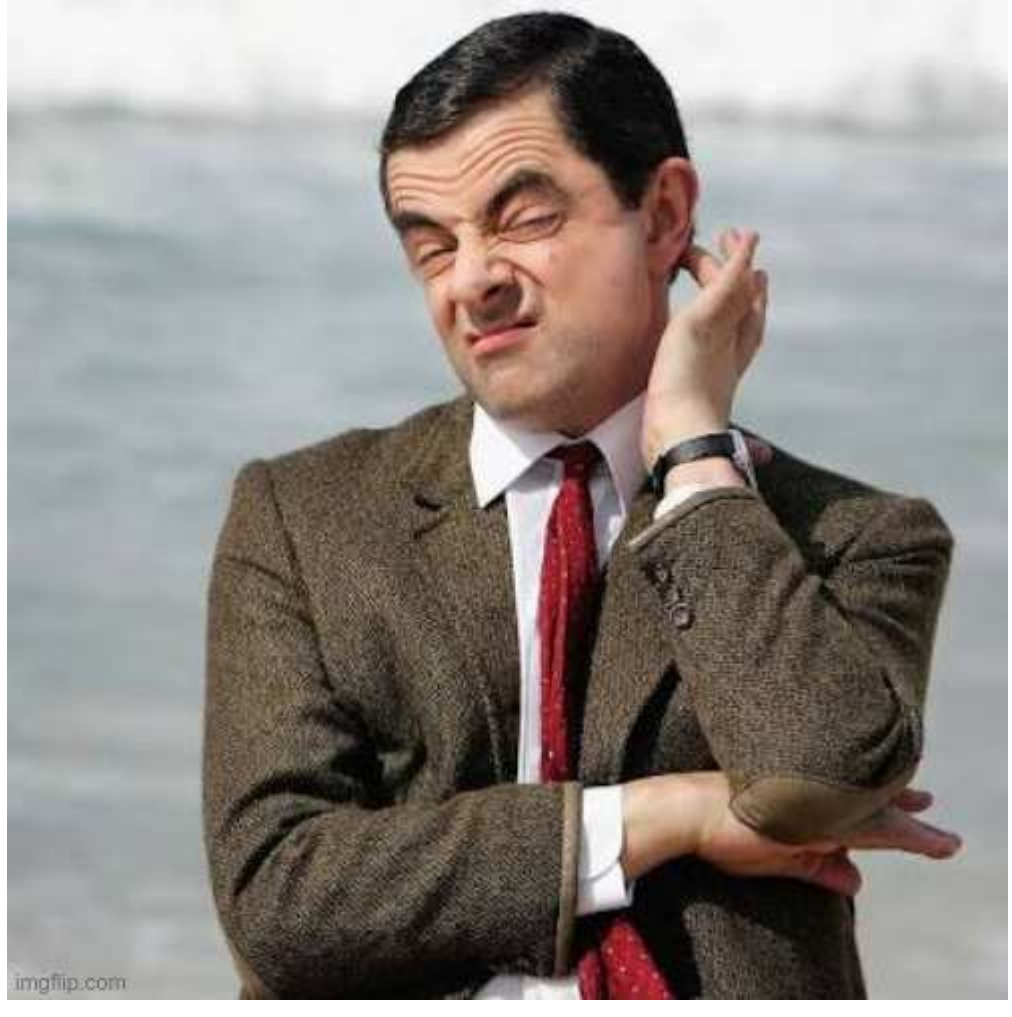
~~**OBSOLESCENZA**~~

RIUSO

- **nessun vincolo di licenza:** se l'hardware funziona, non devo essere limitato da vincoli software (vedi Windows 10)
- **riuso:** un pc del 2015 può fare ancora tante cose con Linux e Software Libero
- **hardware riparabile:** scegliere in base a riparabilità e libertà. No computer sigillati dove si può solo comprare il nuovo modello (Apple)

Parole chiave: /e/OS, Linux

DA DOVE INIZIARE?



DA DOVE INIZIARE?

- **Zorin OS**: sistema operativo GNU/Linux per pc, facile ~~(Windows, MacOs)~~
- **LibreOffice**: applicazioni per ufficio ~~(Microsoft Office365)~~
- **Firefox**: browser per la navigazione ~~(Edge, Chrome, Safari)~~
- **Thunderbird**: programma di posta elettronica ~~(Outlook)~~

DA DOVE INIZIARE?

- **uBlock**: estensione Firefox per ridurre la profilazione
- **K-9 Mail**: app di posta elettronica ~~(Gmail)~~
- **Organic Maps**: app per la navigazione su telefono ~~(Outlook)~~

GRAZIE!



ESTE.LINUX.IT

Gruppo Telegram (discussione):
ILS Este - Gruppo

XMPP:
ILS Este (chat.serviziliberi.it)

Matrix:
ILS Este - Gruppo (server: matrix.org)

Repository e Progetti su GIT:
codeberg.org/este-linux