After complaints, Google will make it easier to disable gen AI search in Photos



Google has spent the past few years in a constant state of AI escalation, rolling out new versions of its Gemini models and integrating that technology into every feature possible. To say this has been an annoyance for Google's userbase would be an understatement. Still, the AI-fueled evolution of Google products continues unabated—except for Google Photos. After waffling on how to handle changes to search in Photos, Google has relented and will add a simple toggle to bring back the classic search experience.

The rollout of the Gemini-powered Ask Photos search experience has not been smooth. According to Google Photos head Shimrit Ben-Yair, the company has heard the complaints. As a result, Google Photos will soon make it easy to go back to the traditional, non-Gemini search system.

If you weren't using Google Photos from the start, it can be

hard to understand just how revolutionary the search experience was. We went from painstakingly scrolling through timelines to find photos to being able to just search for what was in them. This application of artificial intelligence predates the current obsession with generative systems, and that’s why Google decided a few years ago it had to go.

Google launched the beta Ask Photos experience in 2024, rolling it out slowly in the Photos app while it gathered feedback. Google got a whole lot of feedback, most of it negative. Ask Photos is intended to better respond to natural language queries, but it’s much slower than the traditional search, and the way it chooses the pictures to display seems much more prone to error. It was so bad that Google had to pause the full rollout of Ask Photos in summer 2025 to make vital improvements, although it’s still not very good.

https://arstechnica.com/ai/2026/03/google-backtracks-on-ai-search-in-photos-adds-toggle-for-fast-classic-search/

Gemini burrows deeper into Google Workspace with revamped document creation and editing



Google didn’t waste time integrating Gemini into its popular Workspace apps, but those AI features are now getting an overhaul. The company says its new Gemini features for Drive, Docs, Sheets, and Slides will save you from the tyranny of the blank page by doing the hard work for you. Gemini will be able to create and refine drafts, stylize slides, and gather context from across your Google account. At this rate, you’ll soon never have to use that squishy human brain of yours again, and won’t that be a relief?

If you go to create a new Google Doc right now, you’ll see an assortment of AI-powered tools at the top of the page. Google is refining and expanding these options under the new system. The new AI editing features will appear at the bottom of a fresh document with a text box similar to your typical chatbot interface. From there, you can describe the document you want and get a first draft in a snap. When generating a new document, you can rope in content from sources like Gmail, other documents, Google Chat, and the web.

This also comes with expanded AI editing capabilities. You can use further prompts to reformat and change the document or simply highlight specific sections and ask for changes. Docs

will also support AI-assisted style matching, which might come in handy if you have multiple people editing the text. Google notes that all Gemini suggestions are private until you approve them for use.

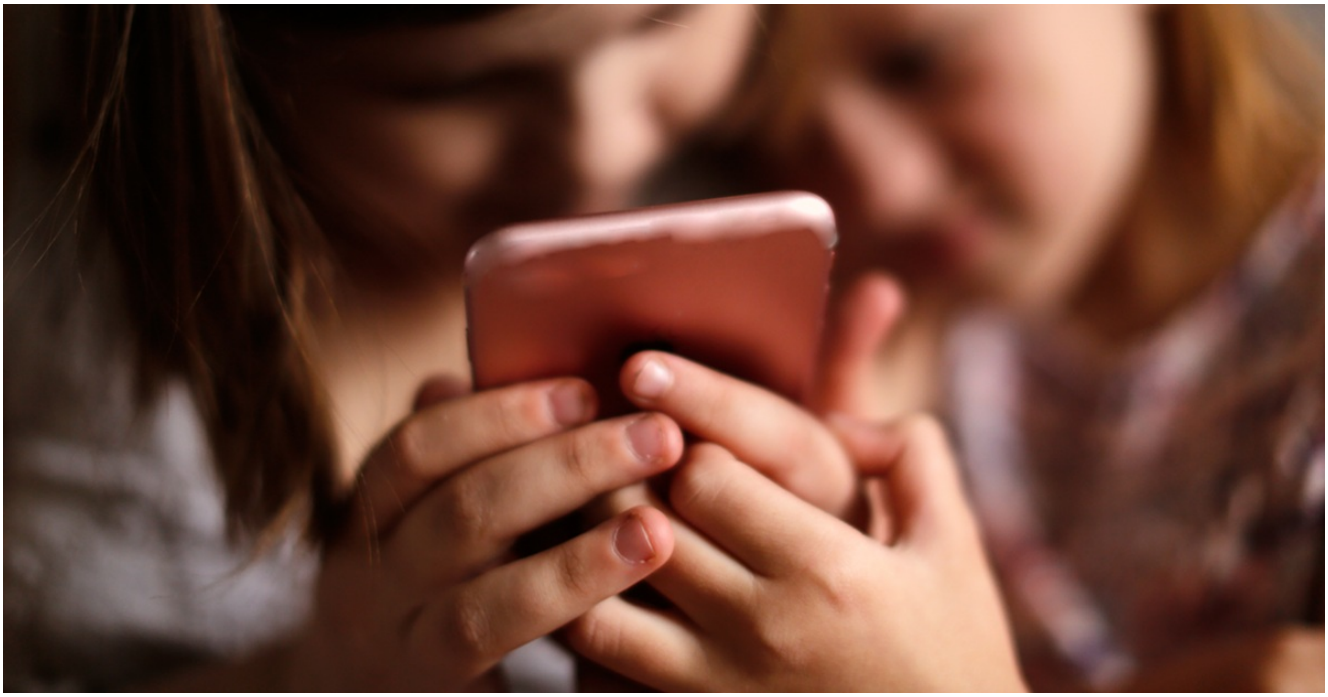
[embedded content]

Gemini in Google Workspace.

Gemini is also getting an upgrade in Sheets, and Google claims the robot’s spreadsheet capabilities are nearing those of flesh-and-blood humans in recent testing. Similar to text documents, you can tell Gemini in the sidebar what kind of spreadsheet you need and the AI will use the prompt (and whatever data sources you specify) to generate it. Gemini can also allegedly fill in missing data by searching for it on the web. In our past testing, Gemini has had a lot of trouble with spreadsheet layouts, but Google says this revamp will handle everything, from basic tasks to complex data analysis.

https://arstechnica.com/ai/2026/03/gemini-burrows-deeper-into-google-workspace-with-revamped-document-creation-and-editing/

AI e immagini generate senza consenso, il documento di 61 autorità mondiali della privacy a difesa di minori e fragili



Sessantuno autorità di protezione dei dati di tutto il mondo, tra cui il **Garante privacy italiano** e l'**European Data Protection Board** (EDPB), hanno firmato una **dichiarazione congiunta** per affrontare uno dei rischi più delicati legati allo sviluppo dell'intelligenza artificiale (AI): la generazione di immagini e video realistici di persone reali senza il loro consenso.

Il documento, coordinato dal **Gruppo di lavoro sulla cooperazione internazionale per l'applicazione delle norme** (*International Enforcement Cooperation Working Group* – **IEWG**) della *Global Privacy Assembly* (**GPA**), rappresenta un segnale forte della crescente attenzione globale verso le conseguenze sociali e giuridiche delle nuove tecnologie di generazione di contenuti basate sull'AI.

A firmare la dichiarazione per il Comitato europeo per la protezione dei dati è stata la presidente dell'EDPB **Anu Talus**, a testimonianza dell'impegno dell'Europa nel promuovere un dialogo internazionale sulla protezione dei dati e dei diritti fondamentali nell'era dell'intelligenza artificiale.

Un problema globale che cresce con l’AI generativa. A rischio minori e soggetti fragili

Negli ultimi anni, i progressi dell’intelligenza artificiale generativa hanno reso possibile creare immagini e video estremamente realistici partendo da semplici istruzioni testuali. Strumenti sempre più accessibili, spesso integrati direttamente nei social network o in piattaforme online, consentono oggi di produrre contenuti che riproducono fedelmente il volto o il corpo di persone reali.

Il problema nasce quando queste tecnologie vengono utilizzate **a insaputa** e **senza il consenso delle persone ritratte**.

Secondo le autorità firmatarie, la diffusione di immagini intime false, video manipolati o contenuti diffamatori che raffigurano individui reali, rappresenta una **minaccia concreta per la privacy, la reputazione e la dignità delle persone**.
Un rischio che diventa ancora più grave quando riguarda **minori o soggetti particolarmente vulnerabili**, esposti a fenomeni come cyberbullismo, molestie digitali o sfruttamento.

L’allarme riguarda soprattutto la rapidità con cui questi contenuti possono essere prodotti e diffusi online, spesso prima che le vittime riescano a intervenire per rimuoverli.

Il nostro **Garante per la protezione dei dati personali** aveva già adottato a gennaio un provvedimento di avvertimento nei confronti degli utilizzatori di servizi basati sull’**intelligenza artificiale**, come **Grok**, **ChatGPT** e **Clothoff** (quest’ultima piattaforma già destinataria di un provvedimento di blocco nell’ottobre scorso) e altri servizi analoghi disponibili online, proprio perché consentivano di generare e condividere contenuti a partire da immagini o voci reali, arrivando anche a **“spogliare” persone senza il loro consenso**.

I quattro principi per uno sviluppo responsabile dell’AI

Pur riconoscendo il grande potenziale dell’intelligenza artificiale per l’innovazione e lo sviluppo economico, le autorità mondiali della privacy ricordano che la tecnologia deve essere progettata e utilizzata nel rispetto delle normative sulla protezione dei dati e dei diritti fondamentali.

Nel documento vengono indicati **quattro principi fondamentali** che dovrebbero guidare lo sviluppo e l’uso dei sistemi di AI generativa:

introdurre **misure efficaci di prevenzione degli abusi**, in particolare per impedire l’uso improprio di dati personali e la creazione non consensuale di immagini intime o contenuti lesivi;

garantire massima **trasparenza**, perché le aziende che sviluppano o utilizzano sistemi di AI devono spiegare chiaramente come funzionano queste tecnologie, quali sono gli utilizzi consentiti e quali possono essere le conseguenze di un uso improprio;

la necessità di offrire **strumenti semplici ed efficaci per chiedere la rimozione dei contenuti dannosi**, soprattutto quando coinvolgono dati personali o rappresentazioni non autorizzate;

l’importanza di **gestire in modo specifico i rischi per i minori**, che rappresentano una delle categorie più esposte agli effetti negativi delle tecnologie digitali.

Pensare l’AI a partire dalla

privacy by design

La dichiarazione è rivolta principalmente alle **aziende che sviluppano o utilizzano sistemi di intelligenza artificiale per la generazione di contenuti**, dalle grandi piattaforme digitali alle start-up tecnologiche.

Il messaggio delle autorità è chiaro: la tutela della privacy e della dignità delle persone deve essere integrata fin dalla progettazione delle tecnologie.

Per questo motivo i garanti della privacy invitano le imprese a **collaborare in modo proattivo con le autorità di regolamentazione**, adottando fin da subito sistemi di sicurezza e meccanismi di protezione efficaci.

L'obiettivo è evitare che l'innovazione tecnologica si trasformi in uno strumento di abuso o di violazione dei diritti fondamentali.

Cooperazione internazionale contro i rischi digitali

La dichiarazione rappresenta anche un esempio concreto di **cooperazione globale nella regolazione delle tecnologie emergenti**. Il fatto che oltre sessanta autorità di diversi continenti abbiano deciso di prendere una posizione comune dimostra quanto il problema sia percepito come urgente.

Le autorità firmatarie si sono impegnate a **condividere informazioni, strategie di intervento e buone pratiche**, con l'obiettivo di contrastare in modo più efficace i rischi legati alla diffusione di contenuti generati dall'intelligenza artificiale.

In un ecosistema digitale globale, infatti, i problemi non si fermano ai confini nazionali. Per questo la cooperazione tra

autorità di regolazione diventa uno strumento essenziale per garantire una tutela effettiva dei diritti delle persone.

Innovazione sì, ma senza sacrificare privacy e diritti fondamentali

Il messaggio che emerge è uno solo: l'intelligenza artificiale può portare grandi benefici alla società, ma il suo sviluppo non può avvenire a discapito dei diritti fondamentali. Privacy, dignità, sicurezza e tutela dei minori devono restare **principi non negoziabili** anche nell'era delle tecnologie più avanzate.

Per questo le autorità mondiali della privacy chiedono che la progettazione dell'AI segua un principio semplice ma essenziale: **il progresso tecnologico deve sempre rimanere al servizio delle persone, e non il contrario**.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/ai-e-immagini-generate-senza-consenso-il-documento-di-61-autorita-mondiali-della-privacy-a-difesa-di-minori-e-fragili/567718/

AI e valanga di falsi video della guerra in Iran. BBC: "Crollata ogni barriera"



Guerra Iran-Israele, boom di video e immagini satellitari falsi generati dall'AI

Un'ondata senza precedenti di contenuti falsi generati con l'intelligenza artificiale (**AI**) sta invadendo i social network mentre l'opinione pubblica cerca informazioni sulla guerra all'Iran di Stati Uniti e Israele. Video di bombardamenti mai avvenuti, immagini satellitari manipolate e scene spettacolari di città in fiamme, stanno accumulando milioni di visualizzazioni online.

È quanto emerge da un'inchiesta di Thomas Copeland per la *BBC*, che documenta come la **disinformazione prodotta con l'AI** stia diventando un vero e proprio modello di business per molti creator.

"La barriera per creare filmati di guerra falsi e convincenti è

crollata”

Secondo **Timothy Graham**, esperto di media digitali della Queensland University of Technology, la situazione è ormai fuori scala: “*La portata è davvero allarmante e questa guerra ha reso impossibile ignorarla*”.

Il punto è che la tecnologia ha abbattuto quasi completamente le barriere tecniche: “*Quello che prima richiedeva una produzione video professionale* – ha precisato Graham – *ora può essere fatto in pochi minuti con strumenti di AI*”.

Il risultato è una proliferazione di contenuti che sembrano realistici ma che in realtà sono completamente falsi: “*La barriera per creare filmati di guerra sintetici e convincenti è essenzialmente crollata*”, ha sottolineato l’esperto della Queensland University.

Il falso video della nave da guerra condiviso anche dal governatore del Texas (lo stesso usato dai nostri TG per l’Ucraina)

Per capire pienamente la gravità del problema, basti pensare che il 5 marzo scorso, il governatore del Texas Greg Abbott ha condiviso sul suo profilo X (poi prontamente eliminato) il video falso di una nave da guerra americana che prendeva di mira un aereo militare iraniano.

Secondo l’articolo pubblicato da Lucy Carter e Michael Workman per *ABC NEWS Verify* il video sembrerebbe provenire da un famoso videogioco di simulazione militare chiamato *War Thunder*.

Il video ha totalizzato più di 7 milioni di visualizzazioni su X.

Secondo **TJ Thomson**, esperto di media digitali e comunicazione visiva del RMIT, "*la portata di questo conflitto, unita ai rapidi progressi nella tecnologia dell'intelligenza artificiale generativa, sta rendendo sempre più difficile per le persone distinguere la realtà dalla finzione*".

"*Il rapido sviluppo della tecnologia dell'intelligenza artificiale farà sì che presto le persone non crederanno più ai propri occhi e purtroppo ci stiamo velocemente arrivando a questo punto*", ha commentato Thomson. A pensarci bene, più che un ovvio allarme generale è quasi un incubo per il futuro delle democrazie di tutto il mondo, che dipendono dall'informazione libera e di qualità.

Lo stesso videogioco (sempre "*War Thunder*") è stato utilizzato dal TG1 e dal TG2 della nostra Rai nei primi giorni dell'**invasione russa dell'Ucraina** (24 febbraio 2022), spacciandolo per immagini di missili russi su Kiev durante le dirette dei giornalisti inviati sul campo.

Missili su Tel Aviv e Dubai in fiamme: i fake che diventano virali

Tra gli esempi analizzati da *BBC Verify* c'è un video AI che sembra mostrare **missili che colpiscono Tel Aviv**, accompagnati dal rumore delle esplosioni. Il filmato è stato pubblicato in oltre **300 post** e condiviso decine di migliaia di volte.

Un altro video, visto **milioni di volte**, mostra il **grattacielo Burj Khalifa di Dubai avvolto dalle fiamme**, con persone che fuggono dalla zona. Anche questo è completamente generato con l'intelligenza artificiale.

Il problema non riguarda solo i video. Si fanno strada con forza (facilmente anche) **le immagini satellitari false**. Un esempio riguarda una fotografia che circola sui social e che pretende di mostrare **gravi danni alla base della Quinta Flotta**

della Marina americana in Bahrain.
In realtà l'immagine è stata generata artificialmente a partire da una vera fotografia satellitare del 2025.

I falsi video fatti con l'AI hanno un impatto enorme sulla fiducia nel sistema dell'informazione

Secondo **Mahsa Alimardani**, ricercatrice dell'Oxford Internet Institute specializzata sull'Iran, la diffusione di questi contenuti ha conseguenze dirette sulla qualità dell'informazione: "*Video falsi come questi hanno un impatto negativo sulla fiducia delle persone nelle informazioni verificate che vedono online e rendono molto più difficile documentare prove reali*".

Alimardani osserva inoltre che il fatto che alcune piattaforme stiano iniziando a intervenire dimostra quanto il problema sia diventato evidente: "*È un segnale importante che si siano accorti che si tratta di un problema enorme*".

L'AI rende i falsi sempre più facili da creare e la pipeline verso i social è ormai automatizzata

La crescita dei fake è alimentata dalla disponibilità di nuovi strumenti di generazione automatica. Tra questi ci sono modelli come **Sora di OpenAI**, i sistemi video di **Google**, applicazioni cinesi come **Seedance** e strumenti integrati nei social network.

Secondo l'esperto di AI **Henry Ajder**: "*Il numero di strumenti disponibili per creare manipolazioni altamente realistiche è*

senza precedenti. Non abbiamo mai visto tecnologie così accessibili, così facili e così economiche da utilizzare".

Per **Victoire Rio**, direttrice della non profit tecnologica What To Fix, questo ha trasformato completamente il processo di produzione della disinformazione: "*La diffusione di contenuti AI è esplosa perché la pipeline verso i social media può ormai essere quasi completamente automatizzata*".

Il ruolo di X e il problema della monetizzazione. L'avanzata delle imprese della disinformazione?

Un elemento chiave è il **sistema di monetizzazione delle piattaforme social**, che premia i contenuti virali indipendentemente dalla loro veridicità. Su **X**, il programma *Creator Revenue Sharing* paga gli utenti che generano grandi volumi di visualizzazioni, commenti e interazioni. Secondo le stime riportate da Graham, la piattaforma potrebbe pagare: "*circa otto-dodici dollari per ogni milione di impression verificate*".

Per accedere al programma, i creator devono superare una soglia di milioni di visualizzazioni in pochi mesi e possedere un abbonamento premium. Una volta entrati nel sistema, però, la dinamica cambia completamente.

"*Una volta dentro, i contenuti virali generati con l'AI diventano praticamente una macchina per fare soldi. Hanno costruito l'impresa definitiva della disinformazione*", spiega Graham.

Secondo il responsabile dei prodotti di X, citato da *BBC Verify*, **il 99% degli account che diffondono video AI di guerra starebbe cercando di sfruttare il sistema di monetizzazione**.

La piattaforma ha annunciato che sospenderà temporaneamente

dal programma di pagamento i creator che pubblicano video di conflitti generati con l'AI senza etichettarli chiaramente.

Secondo Graham: "*La questione più profonda è che la monetizzazione basata sull'engagement e l'informazione accurata sono fondamentalmente in tensione tra loro, e nessuna piattaforma ha davvero risolto questo conflitto – e forse non lo farà mai*".

Il caso Grok: quando anche l'AI sbaglia. In pericolo i sistemi democratici?

La situazione è resa ancora più complessa dal ruolo degli assistenti basati sull'intelligenza artificiale. Diversi utenti hanno chiesto al chatbot **Grok**, integrato nella piattaforma X, di verificare l'autenticità di alcuni video. In molti casi analizzati da *BBC Verify*, però, Grok ha **sbagliato**, sostenendo che i filmati fossero reali.

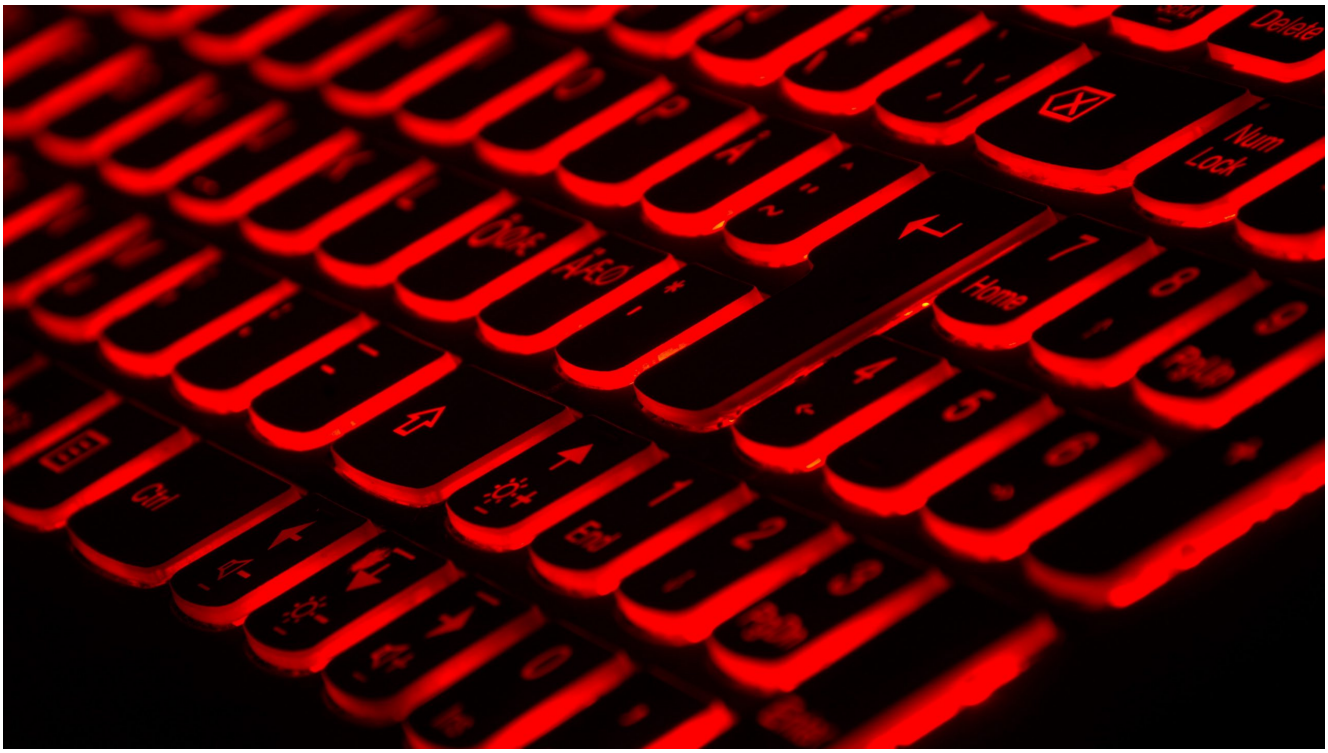
Questo dimostra quanto sia difficile distinguere i contenuti autentici da quelli sintetici anche per sistemi avanzati di AI.

In ultima analisi, va ricordato sempre che ciò che genera più attenzione (shock, paura, immagini spettacolari, violenza) tende a diffondersi più velocemente delle informazioni verificate. Un grande vantaggio per chi specula e fa profitti sulle tragedie dell'umanità.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/ai-e-valanga-di-falsi-video-della-guerra-in-iran-bbc-crollata-ogni-barriera/567734/

Guerra in Iran, quali conseguenze per il Tech europeo?



Il conflitto che coinvolge Iran, Stati Uniti e Israele, caratterizzato da attacchi aerei ad alta intensità, guerra con droni e operazioni informatiche, ha implicazioni significative e multiformi per il settore della tecnologia digitale dell'Unione Europea (UE). Sulla base dei report di inizio marzo 2026, realizzati dalla società di analisi IDC, gli impatti principali si concentrano sull'inflazione legata all'energia, sulle interruzioni della catena di approvvigionamento, sull'aumento dei rischi per la sicurezza informatica e su un potenziale rallentamento della spesa IT.

1. Inflazione e costi operativi legati all’energia

• **Costi dei data center**: poiché il conflitto interrompe la produzione di energia nella regione, l’aumento dei prezzi del petrolio e del gas in Europa (già del 40-50% in più a causa degli shock dell’offerta) sta gonfiando i costi operativi per i data center e i fornitori di servizi cloud.

• **Pressioni sulla produzione:** l’aumento dei costi energetici sta influenzando la fabbricazione di semiconduttori e la produzione di componenti IT, minacciando di aggravare le carenze esistenti.

2. Interruzioni della catena di approvvigionamento e limitazioni hardware

• **Rischi nello Stretto di Hormuz:** l’interruzione delle rotte di navigazione nello Stretto di Hormuz sta causando ritardi nella consegna dei componenti, con ripercussioni sulla catena di approvvigionamento per la tecnologia di consumo e l’hardware aziendale.

• **Carenza di componenti:** il mercato globale delle memorie (DRAM/NAND) sta subendo una pressione crescente, con un potenziale aumento dei prezzi dello storage aziendale e delle infrastrutture di intelligenza artificiale.

• **Costi logistici:** i costi di assicurazione e trasporto per i prodotti tecnologici sono in aumento, il che potrebbe rallentare l’implementazione di nuove infrastrutture digitali.

3. Accelerazione delle minacce alla sicurezza informatica e aumento dei budget

• **Aumento dei rischi informatici:** le organizzazioni dell'UE devono far fronte a crescenti minacce da parte di gruppi di hacker affiliati all'Iran, che potrebbero prendere di mira infrastrutture critiche, inclusi, potenzialmente, data center e fornitori di servizi IT, come misure di ritorsione.

• **Riallocazione del bilancio:** in un contesto di rischi più elevati, si prevede che le aziende dell'UE accelereranno la spesa per la sicurezza, in particolare per il rilevamento e la risposta gestiti (MDR), la modernizzazione dei centri operativi di sicurezza (SOC) e le architetture zero-trust.

• **Vulnerabilità dei data center:** il conflitto ha evidenziato la vulnerabilità fisica dei data center all'instabilità regionale, rendendo necessaria una rivalutazione delle strategie di backup multiregionale.

4. Rallentamento della spesa IT e rivalutazione strategica

• **Investimenti ritardati:** si prevede che la combinazione di incertezza economica, prezzi elevati dell'energia e pressioni inflazionistiche porterà a ritardi nei progetti IT e, in alcuni casi, a una riduzione della spesa tecnologica discrezionale.

• **Dare priorità ad AI/Cloud:** sebbene la crescita complessiva della spesa IT possa rallentare, è probabile che gli investimenti strategici nelle infrastrutture di AI e nella migrazione al cloud persistano, anche se forse con una rivalutazione delle sequenze di progetto in caso di aumento dei costi dell'hardware.

• **Focus sulla sovranità digitale:** il conflitto rafforza la spinta dell'UE verso la *"sovranità tecnologica",* rafforzando le capacità e riducendo la dipendenza da attori stranieri per le infrastrutture digitali critiche.

5. Impatto sul personale e sulle operazioni tecnologiche

• **Cambiamenti operativi:** le principali aziende tecnologiche si stanno affrettando a proteggere dipendenti e strutture nella più ampia regione del Medio Oriente, con alcune che stanno implementando protocolli di emergenza, che potrebbero avere un impatto indiretto sulle operazioni da remoto delle aziende europee collegate alla regione.

• **Attacchi alle infrastrutture digitali:** il potenziale, o l'effettivo, attacco ai data center, come si è visto con le reti iraniane, indica una nuova fase di guerra digitale che potrebbe compromettere la continuità dei servizi per le piattaforme globali utilizzate all'interno dell'UE.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/guerra-in-iran-quali-conseguenze-per-il-tech-europeo/567684/

Google's new command-line tool can plug OpenClaw into

your Workspace data



The command line is hot again. For some people, command lines were never *not* hot, of course, but it's becoming more common now in the age of AI. Google launched a Gemini command-line tool last year, and now it has a new AI-centric command-line option for cloud products. The new Google Workspace CLI bundles the company's existing cloud APIs into a package that makes it easy to integrate with a variety of AI tools, including OpenClaw. How do you know this setup won't blow up and delete all your data? That's the fun part—you don't.

There are some important caveats with the Workspace tool. While this new GitHub project is from Google, it's "not an officially supported Google product." So you're on your own if you choose to use it. The company notes that functionality may change dramatically as Google Workspace CLI continues to evolve, and that could break workflows you've created in the meantime.

For people interested in tinkering with AI automations and don't mind the inherent risks, Google Workspace CLI has a lot to offer, even at this early stage. It includes the APIs for

every Workspace product, including Gmail, Drive, and Calendar. It’s designed for use by humans and AI agents, but like everything else Google does now, there’s a clear emphasis on AI.

The tool supports structured JSON outputs, and there are more than 40 agent skills included, says Google Cloud director Addy Osmani. The focus of Workspace CLI seems to be on agentic systems that can create command-line inputs and directly parse JSON outputs. The integrated tools can load and create Drive files, send emails, create and edit Calendar appointments, send chat messages, and much more.

https://arstechnica.com/ai/2026/03/googles-new-command-line-tool-can-plug-openclaw-into-your-workspace-data/

Musk fails to block California data disclosure law he fears will ruin xAI



“It is not lost on the Court the important role of datasets in AI training and development, and that, hypothetically, datasets and details about them could be trade secrets,” Bernal wrote. But xAI “has not alleged that it actually uses datasets that are unique, that it has meaningfully larger or smaller datasets than competitors, or that it cleans its datasets in unique ways.”

Therefore, xAI is not likely to succeed on the merits of its Fifth Amendment claim.

The same goes for First Amendment arguments. xAI failed to show that the law improperly “forces developers to publicly disclose their data sources in an attempt to identify what California deems to be ‘data riddled with implicit and explicit biases,’” Bernal wrote.

To xAI, it seemed like the state was trying to use the law to influence the outputs of its chatbot Grok, the company argued, which should be protected commercial speech.

Over the past year, Grok has increasingly drawn global public scrutiny for its antisemitic rants and for generating nonconsensual intimate imagery (NCII) and child sexual abuse

materials (CSAM). But despite these scandals, which prompted a California probe, Bernal contradicted xAI, saying California did not appear to be trying to regulate controversial or biased outputs, as xAI feared.

“Nothing in the language of the statute suggests that California is attempting to influence Plaintiff’s models’ outputs by requiring dataset disclosure,” Bernal wrote.

Addressing xAI’s other speech concerns, he noted that “the statute does not functionally ask Plaintiff to share its opinions on the role of certain datasets in AI model development or make ideological statements about the utility of various datasets or cleaning methods.”

“No part of the statute indicates any plan to regulate or censor models based on the datasets with which they are developed and trained,” Bernal wrote.

Public “cannot possibly” care about AI training data

Perhaps most frustrating for xAI as it continues to fight to block the law, Bernal also disputed that the public had no interest in the training data disclosures.

https://arstechnica.com/tech-policy/2026/03/musk-fails-to-block-california-data-disclosure-law-he-fears-will-ruin-xai/

AI startup sues ex-CEO,

saying he took 41GB of email and lied on résumé



Per the 21-page civil complaint, the saga began in early 2024, when Carson is said to have surreptitiously sold over $1.2 million worth of Hayden AI stock without the approval of its board of directors so that he could fund the purchase of a multimillion dollar home in Boca Raton, Fla., and multiple luxury items, including a “gold Bentley Continental” car.

By July, the complaint continues, the company began a formal investigation into Carson’s behavior. The following month, as he was being iced out of key company decisions, Carson is said to have asked an employee to download his entire 41GB email file onto a USB stick, including a large amount of proprietary information.

Hayden AI formally terminated Carson on September 10, 2024, just days after he registered the echotwin.ai domain name.

Beyond the alleged financial fraud, Hayden AI claims that Carson’s entire professional background, ranging from the

length of his US military service to his having founded a company called “Louisa Manufacturing” (as depicted on LinkedIn), is also bogus. The complaint calls Carson’s CV a “carefully constructed fraud.”

According to Carson’s LinkedIn profile, he completed a doctorate from Waseda University in Tokyo in 2007.

“That is a lie,” the complaint states. “Carson does not hold a PhD from Waseda or any other university. In 2007, he was not obtaining a PhD but was operating ‘Splat Action Sports,’ a paintball equipment business in a Florida strip mall.”

https://arstechnica.com/tech-policy/2026/03/ai-startup-sues-ex-ceo-saying-he-took-41gb-of-email-and-lied-on-resume/

6G grande assente al Mobile World Congress di Barcellona (surclassato da AI e satellite)



L’AI ha fatto la parte del leone al MWC26, ma la cosa più interessante di questa edizione della kermesse globale del mobile appena chiusa a Barcellona è la pressoché totale assenza del 6G. E così mentre AI, GPU e reti edge sono sulla bocca di tutti fra gli stand della fiera catalana, fa ancora più rumore la quasi totale assenza di novità ri qualche rilievo sul fronte del 6G.

L’analisi di ABI Research

A farlo notare il Senior Research Director di ABI Research **Dimitris Mavrakis** che punta il dito su questa assenza significativa.

Anche se mancano ancora anni alla prima specifica normativa 6G, atteso sul mercato non prima del 2030, il settore sta iniziando a gettare le basi attraverso alleanze iniziali, strategie concorrenti e investimenti tecnologici fondamentali.

• Le prime iniziative 6G annunciate da aziende come **NVIDIA**,

Qualcomm e **AMD**

• Il divario emergente tra strategie 6G basate sui dispositivi e sulle infrastrutture

Perché tecnologie fondamentali come Integrated Sensing and Communication (ISAC) e reti native basate sull'intelligenza artificiale stanno diventando centrali per la prossima generazione di telecomunicazioni.

Pochi annunci 6G al MWC26

Al MWC26 sono stati fatti alcuni annunci sugli sviluppi del 6G, ma nessuno era definitivo o indicava un consenso di mercato sulla forma finale della nuova generazione. **NVIDIA** ha annunciato una nuova iniziativa 6G, **Qualcomm** ha annunciato una nuova coalizione 6G e **AMD** sta guidando una nuova alleanza per sviluppare sistemi di intelligenza artificiale Open Telco che saranno sicuramente utilizzati per il 6G.

Siamo ora nel 2026, 3 anni prima che il 3rd Generation Partnership Project (3GPP) pubblichi la sua prima specifica normativa nella Release 21. Alcuni potrebbero dire che il ciclo di aggiornamento decennale delle generazioni cellulari sia interrotto, ma possiamo facilmente controbattere osservando il ciclo di sviluppo del 5G e gli eventi del MWC. Nello specifico, il 2015 è stato 3 anni prima della pubblicazione del primo standard 5G e i temi del MWC15 sono stati Long Term Evolution-Unlicensed (LTE-U), nuovi smartphone e Realtà Virtuale (VR). Al MWC di quest'anno si è parlato poco del 5G, e ancor meno delle novità sul 6G. E il fattore più importante è che le aziende che hanno dominato il 5G non erano le stesse che hanno fatto da headliner al MWC15. Lo stesso si può dire anche del 6G.

Eppure la portata e l’ambizione del 6G è superiore al 5G

Ciò nonostante, la portata e l’ambizione del 6G sono molto più grandi del 5G, nonostante il comportamento moderato degli operatori di telefonia mobile e la loro riluttanza – per ora – a impegnare budget ingenti per la nuova generazione. Gli studi sul 6G includono argomenti innovativi che ampliano le funzionalità principali della rete di telecomunicazioni, piuttosto che cercare di applicarne le capacità a mercati adiacenti (ad esempio, il network slicing 5G per la chirurgia a distanza). Alcune di queste funzionalità includono:

• **Integrated Sensing and Communication (ISAC)**, che mira a consentire alla rete di rilevare l’ambiente senza alcun input dal dispositivo.

• **Higher-order Multiple Input, Multiple Output (MIMO)**, che include antenne con apertura molto più ampia che consentono la comunicazione in prossimità, consentendo così un controllo spaziale molto più preciso della capacità nelle aree trafficate.

• **Interfaccia aerea AI/Machine Learning (ML)**, automazione a circuito chiuso e convergenza delle capacità di telecomunicazione e di elaborazione in una piattaforma convergente.

Esistono anche molti altri studi e proposte tecniche, molti dei quali non troveranno posto nelle specifiche ufficiali, e ancora meno troveranno applicazione nelle implementazioni commerciali. C’è anche l’urgenza di investire immediatamente nello sviluppo di questi pilastri fondamentali per preparare la rete a gestire la prossima generazione di carichi di lavoro, che sarà probabilmente dominata dal traffico AI Agentic e Physical, non soltanto dalla banda larga mobile.

Dispositivi 6G vs capacità di rete

Sembra inoltre che ci sia una certa competizione tra infrastruttura di rete e capacità dei dispositivi nell'ambito della standardizzazione, come previsto. **Qualcomm** è stata la più accanita sostenitrice del 6G in fiera, segnalando il suo impegno verso la nuova generazione, poiché ha bisogno del 6G per mantenere il suo slancio di mercato e la sua redditività.

Ericsson ha assunto una posizione notevolmente diversa, annunciando il proprio silicio appositamente progettato con acceleratori di rete neurale integrati, anziché affidarsi alle GPU NVIDIA. Questo presenta una spaccatura filosofica: Qualcomm ha bisogno di dispositivi 6G, Ericsson ha bisogno di infrastrutture 6G, e nessuna delle due dipende completamente dalla stessa coalizione. Queste due aziende incarnano la frattura tra dispositivi e reti, ma probabilmente raggiungeranno un compromesso nel 3GPP.

6G, la discussione giusta al momento giusto

Allargando lo sguardo, il 6G è stato probabilmente trascurato al MWC26, ma sono state sottolineate altre innovazioni e progressi del settore. Ad esempio, l'automazione a circuito chiuso senza intervento umano sta iniziando ad affermarsi nel settore, mentre il cloud sta diventando l'infrastruttura di base più efficiente per le reti mobili. Queste piattaforme indicano un'evoluzione a lungo termine che costituirà sicuramente il sottostato del 6G, su cui verranno implementate nuove innovazioni, inclusi i servizi ISAC e AI. Gli sviluppi del 6G stanno affrontando sfide tecniche e fondamentali davvero impegnative, e questo potrebbe essere il motivo del debole entusiasmo degli operatori. ABI Research prevede che il MWC27 ospiterà una pletora di attività e annunci sul 6G, con l'inizio del ciclo di hype per il 6G.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/6g-grande-assente-al-mobile-world-congress-di-barcellona-surclassato-da-ai-e-satellite/567424/

Workers report watching Ray-Ban Meta-shot footage of people using the bathroom



“You understand that it is someone’s private life you are looking at, but at the same time you are just expected to carry out the work,” an anonymous Sama employee reportedly said.

Meta confirms use of data annotators

In statements shared with the BBC on Wednesday, Meta confirmed that it “sometimes” shares content that users share with the Meta AI generative AI chatbot with contractors to review with “the purpose of improving people’s experience, as many other companies do.”

“This data is first filtered to protect people’s privacy,” the statement said, pointing to, as an example, blurring out faces in images.

Meta’s privacy policy for wearables says that photos and videos taken with its smart glasses are sent to Meta “when you turn on cloud processing on your AI Glasses, interact with the Meta AI service on your AI Glasses, or upload your media to certain services provided by Meta (i.e., Facebook or Instagram). You can change your choices about cloud processing of your Media at any time in Settings.”

The policy also says that video and audio from livestreams recorded with Ray-Ban Metas are sent to Meta, as are text transcripts and voice recordings created by Meta’s chatbot.

“We use machine learning and trained reviewers to process this data to improve, troubleshoot, and train our products. We share that information with third-party vendors and service providers to improve our products. You can access and delete recordings and related transcripts in the Meta AI App,” the policy says.

Meta’s broader privacy policy for the Meta AI chatbot adds: “In some cases, Meta will review your interactions with AIs, including the content of your conversations with or messages to AIs, and this review may be automated or manual (human).”

https://arstechnica.com/gadgets/2026/03/workers-report-watchin

g-ray-ban-meta-shot-footage-of-people-using-the-bathroom/