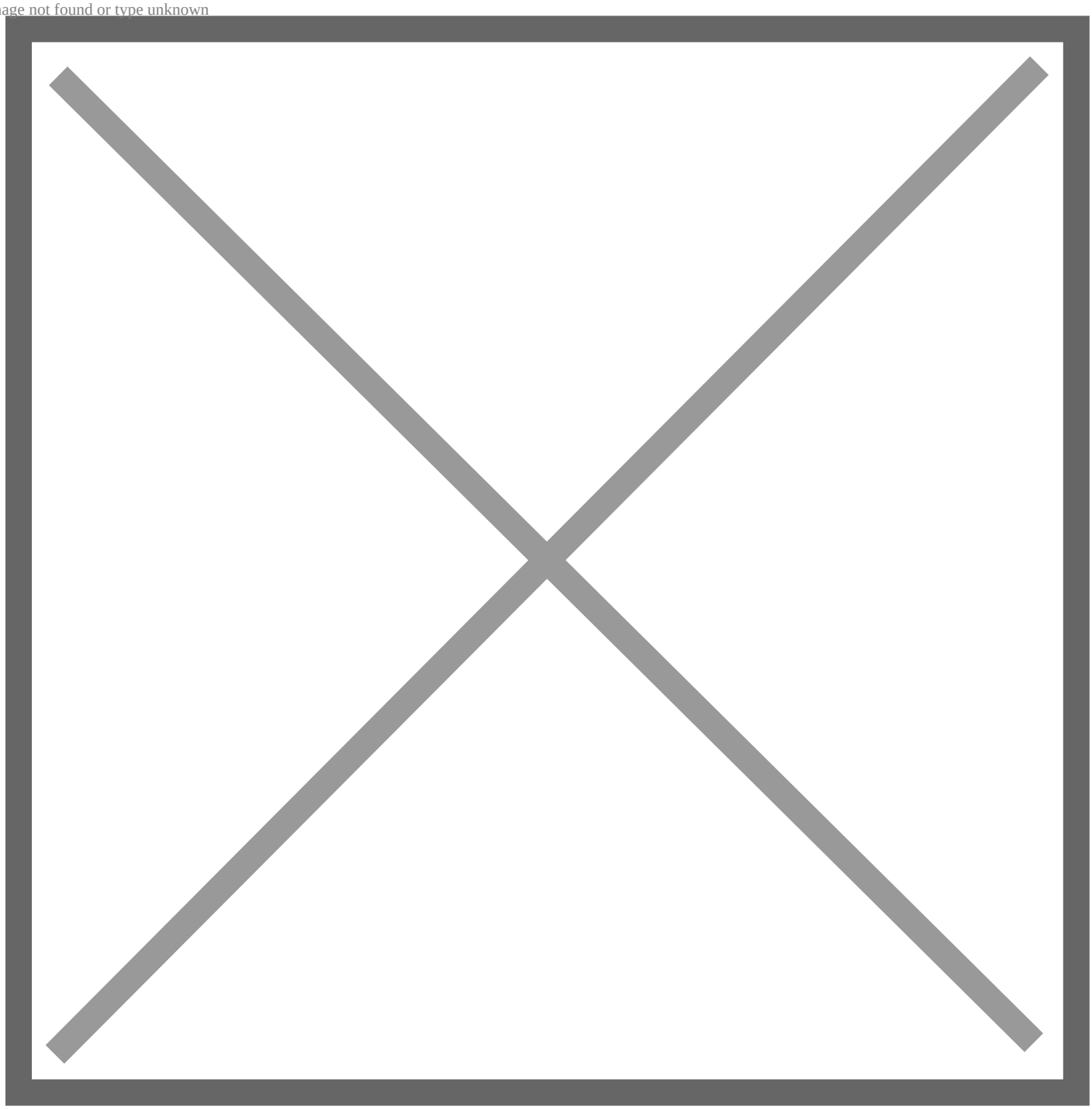
Image not found or type unknown



web

Meta usa i nostri dati per addestrare l’AI, privacy a rischio

ATTUALITà 17_04_2025

img

Image not found or type unknown

Image not found or type unknown

Ruben Razzante

Image not found or type unknown

Meta, la società madre di Facebook, Instagram e WhatsApp, ha annunciato che inizierà a utilizzare i dati pubblici degli utenti europei per addestrare la propria intelligenza artificiale (AI). Si tratta di un passaggio epocale che solleva interrogativi profondi sul futuro della nostra privacy digitale, non solo per le modalità con cui avverrà, ma anche per il contesto normativo in cui si inserisce.

Dopo mesi di attesa e trattative con le autorità europee per la protezione dei dati, in particolare con quella irlandese, Meta ha ricevuto il via libera per procedere, dichiarando di rispettare il GDPR, il Regolamento europeo del 2016 in materia di trattamento dei dati personali, entrato pienamente in vigore nel 2018. Tuttavia, sono in molti a ritenere che questa mossa rappresenti una forzatura nei confronti di un impianto legislativo pensato per tutelare i cittadini europei, non per alimentare i profitti delle big tech.

La questione centrale riguarda quali dati verranno utilizzati. Meta ha specificato che saranno impiegati solo contenuti pubblici condivisi da utenti adulti: post, commenti, e anche le interazioni con Meta AI – l'assistente virtuale introdotto su piattaforme come Messenger, WhatsApp e Instagram. Restano esclusi, almeno formalmente, i messaggi privati e qualsiasi contenuto proveniente da minori. Ma il confine tra pubblico e privato nei social non è mai stato così sottile. Cosa succede, per esempio, se un utente condivide pubblicamente un contenuto originariamente pensato per una cerchia ristretta? Oppure se un'opera d'arte pubblicata su Instagram viene utilizzata per alimentare il modello senza che l'autore ne abbia piena consapevolezza? Le domande sono molte, le risposte poche. E la possibilità di opporsi, pur garantita, non appare così semplice né così efficace.

Meta promette di inviare notifiche a tutti gli utenti europei per informarli sull'uso dei dati e fornire un modulo di opposizione online. Compilarlo dovrebbe essere semplice, ma nella realtà molti potrebbero non accorgersene affatto o rinunciare per stanchezza, pigrizia, confusione o sfiducia. Inoltre, l'opposizione non è automatica: richiede una motivazione e una valutazione da parte dell'azienda stessa, che potrebbe rigettarla. È quindi lecito domandarsi quanto questa "scelta" sia realmente libera. Meta, dal canto suo, si giustifica affermando di seguire le orme di altri colossi come Google e OpenAI, che già hanno fatto ricorso ai dati degli utenti europei per allenare i propri modelli.

Ma questo paragone non basta a rassicurare, soprattutto perché non tiene conto di un contesto normativo – e culturale – profondamente diverso tra le due sponde dell'Atlantico. In Europa il principio della protezione dei dati personali è sancito come un diritto fondamentale, e il GDPR rappresenta ancora oggi uno dei tentativi più avanzati di normare il potere delle grandi piattaforme. Ma ora anche questo baluardo sembra vacillare.

La Commissione europea sta infatti discutendo una riforma del GDPR che potrebbe portare a un ammorbidimento delle regole, con l'intento dichiarato di favorire l'innovazione e la competitività europea nel campo dell'intelligenza artificiale. Tuttavia, c'è chi teme che si stia aprendo la porta a un futuro in cui le garanzie individuali saranno subordinate agli interessi economici delle aziende. È il caso emblematico del progetto di Meta, che appare come il primo grande test di questa possibile svolta normativa. A preoccupare non è solo l'uso dei dati, ma anche la trasparenza e la governance del processo. Quali dataset verranno creati? Dove saranno conservati? Chi avrà accesso? E con quali strumenti di controllo? Per ora, le risposte ufficiali sono vaghe. E l'idea che ogni

contenuto pubblicato su Facebook o Instagram possa finire in pasto a un'intelligenza artificiale generativa – magari usato per creare nuovi prodotti, servizi o persino forme di comunicazione automatizzata – fa emergere un senso di profonda vulnerabilità. È l'ennesima evoluzione del "se sei online, sei merce", ma con un livello di sofisticazione e pervasività che lascia pochi spazi di manovra.

Se un tempo ci si poteva illudere di proteggere la propria privacy impostando il profilo come "privato" o limitando i propri contatti, oggi quella soglia è stata superata. Il concetto stesso di pubblico, così come lo intende Meta, è sempre più sfumato e ridisegnato a seconda delle esigenze dell'azienda. E mentre la società promette di non utilizzare contenuti privati, resta il fatto che tutto ciò che viene definito "pubblico" è già oggi alla mercé degli algoritmi. Non si tratta più solo di profilazione per fini pubblicitari, ma della costruzione stessa dell'intelligenza che guiderà le future interazioni online. A tutto questo si aggiunge un elemento di profonda asimmetria: gli utenti forniscono i dati, spesso inconsapevolmente, ma non ricevono alcun compenso o riconoscimento.

Anzi, si trovano a contribuire – gratuitamente – allo sviluppo di tecnologie che genereranno profitti miliardari per una cerchia ristretta di aziende. È un modello di business che solleva questioni etiche, ma anche giuridiche. Non a caso, in Italia è ancora in corso un'indagine della Procura di Milano sull'ipotesi di evasione fiscale legata al mancato pagamento dell'Iva sui servizi digitali. Il nodo è se i dati forniti dagli utenti in cambio dell'uso "gratuito" dei social possano essere considerati una forma di pagamento in natura. Se la giustizia dovesse dare una risposta affermativa, potrebbe aprirsi un nuovo capitolo nella regolazione delle piattaforme.

Intanto, ai cittadini europei non resta che agire in prima persona: compilare il modulo di opposizione, informarsi, fare pressione sulle istituzioni affinché non allentino le tutele in nome dell'innovazione a tutti i costi. Perché è chiaro che in gioco non c'è solo un algoritmo in più, ma il futuro stesso del nostro diritto alla riservatezza, alla libertà di espressione e, in ultima analisi, alla dignità digitale.