



# Rassegna Stampa

|                           |                         |
|---------------------------|-------------------------|
| Ughi e Nunziante          | Data: 19 settembre 2025 |
| Testata: Economy Magazine | <a href="#">Link</a>    |

# Economy

di Agostino Clemente, partner di Ughi e Nunziante ed Emanuela Burgio, Associate di Ughi e Nunziante

## DeepSeek e il Garante della privacy: ancora diversi nodi da sciogliere



**DeepSeek**, la startup cinese che ha scosso l'equilibrio del mercato globale dell'intelligenza artificiale, ha fatto il suo debutto ufficiale il 10 gennaio 2025 con il lancio dell'app chatbot DeepSeek-R1 su iOS e Android. In poche settimane l'applicazione è diventata la più scaricata negli Stati Uniti, superando persino ChatGPT. Il successo è stato preceduto da una fase di sviluppo che parte dal novembre 2023, ma a consolidare la crescita ci ha pensato, nel dicembre 2024, il rilascio di **DeepSeek-V3**.

Le ragioni di tale successo su scala mondiale sono state rintracciate in due caratteristiche dichiarate: il basso numero di processori necessari per il funzionamento rispetto a modelli analoghi e il costo limitato per il training dei modelli, di molto inferiore a quello dichiarato dai concorrenti.

I produttori hanno infatti dichiarato un investimento di circa 5,6 milioni di dollari, un costo significativamente basso se si paragona con gli oltre cento milioni di dollari necessari per il training dei modelli concorrenti.

In Italia, l'Autorità garante per la protezione dei dati personali (di seguito, il **"Garante"**) il 28 gennaio 2025 ha chiesto alle due società cinesi che gestiscono la piattaforma chiarimenti su come venissero raccolti, utilizzati e trasferiti i dati degli utenti italiani, nonché su quali informazioni venissero utilizzate per addestrare il sistema di intelligenza artificiale. Inoltre, ha chiesto di precisare, in caso di raccolta tramite web scraping, come gli utenti iscritti e quelli non iscritti al servizio fossero stati informati sul trattamento dei loro dati.

Le due società hanno immediatamente risposto. Tuttavia, le risposte hanno lasciato molto perplessi, in quanto veniva negato di fornire il proprio prodotto di intelligenza artificiale sul mercato italiano e, pertanto, si sosteneva che il GDPR non trovasse applicazione in relazione alle attività di trattamento di dati personali dalle stesse poste in essere.

Evidentemente, quanto dichiarato era contrario all'evidenza. Infatti, il prodotto era accessibile tramite app su App Store e Google Play e dal web su tutto il territorio italiano. Nel contempo, ad ogni modo, le società destinatarie del provvedimento hanno rimosso l'app DeepSeek dagli app store italiani.

All'epoca, interrogando sull'accaduto la stessa chatbot DeepSeek dopo l'interlocuzione con il Garante, questa rispondeva di non essere accessibile come App scaricabile dagli store Google Play e Apple Store (cfr. *DeepSeek in Italia, il Garante della privacy dispone il blocco* / *Wired Italia*) e che si poteva utilizzare soltanto via browser. Per quanto, naturalmente, la chatbot non rappresenti la voce ufficiale del titolare della piattaforma, non si può non osservare che, fino al primo provvedimento del Garante, l'App era invece scaricabile; e che l'App è tuttora funzionante (a settembre 2025) per chi l'aveva già scaricata.

Inoltre, ciò che più rileva, la disponibilità della piattaforma sul web rendeva, e rende, applicabile il GDPR ai trattamenti dei dati personali effettuati tramite dette piattaforme, e comporta dunque che queste siano soggette all'autorità del Garante italiano. Ciò almeno sulla carta, ossia stando a quanto stabilito dallo stesso GDPR. Questo, infatti, dichiara la propria applicabilità, tra l'altro, a ogni trattamento di dati personali di interessati che si trovino nella UE, anche se il titolare non sia stabilito nella UE e anche quando il trattamento non sia svolto nella UE, se tale trattamento sia effettuato nell'ambito dell'offerta di servizi offerti nella UE (art. 3 GDPR).

Il Garante, a fronte della risposta inappagante della piattaforma, ritenne necessario

intervenire con urgenza. Nel provvedimento del 30 gennaio 2025 n. 33, rilevando la mancanza di trasparenza nel trattamento dei dati, e l'assenza di garanzie sul trasferimento delle informazioni verso la Cina, dispose "la limitazione definitiva delle attività di trattamento dei dati personali di interessati che si trovano nel territorio italiano che avvengono nell'ambito del servizio DeepSeek", e di avviare un'istruttoria.

A questo punto è accaduto qualcosa di inatteso – e anche inedito, in un ambito di così tanta rilevanza pubblica – ossia che il provvedimento non sia stato rispettato, confermando l'intenzione di DeepSeek di sottrarsi all'autorità del Garante italiano. Dunque, ancora oggi, la piattaforma è disponibile sul web anche in Italia e le stesse App sono funzionanti e aggiornate per chi le aveva scaricate entro il 29 gennaio 2025.

È il caso di ricordare che un provvedimento di analogo tenore era stato adottato in precedenza dal Garante nei confronti di OpenAI in relazione al trattamento dei dati degli interessati italiani svolto con ChatGPT. In quell'occasione, tuttavia, OpenAI aveva da subito collaborato con l'autorità e si era mostrata disponibile a chiarire tutti i profili di compliance con il GDPR. Ora, invece, il Garante sembra trovarsi nella scomoda situazione di un proprio provvedimento amministrativo disatteso.

Lo spiacevole episodio mostra quanto sia difficile, persino per un'autorità nazionale, tradurre in pratica un divieto in una rete mondiale interconnessa.

A complicare il quadro si aggiunge il contesto geopolitico. DeepSeek non è un progetto qualsiasi, ma un prodotto che arriva da un ecosistema tecnologico – quello cinese – che sta rapidamente guadagnando terreno rispetto alle piattaforme americane e che suscita diffidenze relativamente non solo al trattamento dei dati personali, ma anche alla sicurezza nazionale.

Fermi i numerosi dubbi circa lo strumento più adeguato per garantire l'enforcement extra-UE di un provvedimento amministrativo di una autorità di uno Stato membro, ci si chiede se il Regolamento (UE) 2022/2065 (Digital Service Act – DSA) possa offrire una chance in tal senso.

Difatti, agli articoli 4 ss. il DSA in parte riforma la responsabilità degli Internet Service Provider (di seguito, "ISP") già disciplinata dalla Direttiva 2000/31/CE (c.d. Direttiva e-commerce), attuata in Italia con il decreto legislativo 9 aprile 2003, n. 70. In particolare, ai sensi degli artt. 4 ss. DSA, gli ISP beneficiano di esenzioni di responsabilità declinate a seconda della tipologia di provider ricoperta (mere conduit,

caching, hosting), purch  si limitino a un ruolo tecnico e passivo, senza conoscenza o controllo sui contenuti, e intervengano tempestivamente in caso di illiceit  accertata. Le esenzioni dalla responsabilit  stabilite nel DSA lasciano comunque impregiudicata la possibilit  di azioni inibitorie di altro tipo nei confronti degli ISP, anche qualora essi soddisfino le condizioni stabilite nell'ambito di tali esenzioni. Siffatte azioni inibitorie sono disciplinate dal successivo articolo 9 del DSA e consistono in ordini di organi giurisdizionali o autorit  amministrative, emessi in conformit  del diritto dell'Unione, che obbligano a porre fine a una violazione o a impedirla, anche con la rimozione dei contenuti illegali specificati nei suddetti ordini, o la disabilitazione dell'accesso a tali contenuti.

Alla luce di quanto sopra, quindi, ci si chiede se il Garante sia legittimato ai sensi dell'articolo 9 del DSA a rivolgersi direttamente agli hosting provider che rendono accessibile DeepSeek in Italia.

Ebbene, l'autorit  amministrativa competente in Italia a dare attuazione al DSA   l'AGCOM, in quanto questa   stata designata **Coordinatore dei servizi digitali (Digital Services Coordinator – DSC)**, ossia l'autorit  responsabile della vigilanza e dell'applicazione del DSA in Italia. Sembrerebbe quindi, che soltanto l'AGCOM sia l'autorit  legittimata ad emettere l'ordine di cui all'articolo 9 del DSA, ai sensi del combinato disposto dell'articolo 49 DSA e dell'articolo 15 del D.L. 15 settembre 2023, n. 123. Questi ultimi, infatti, demandano al DSC le questioni relative alla vigilanza e all'applicazione del DSA compreso, quindi, l'ordine di cui all'articolo 9 DSA.

Verosimilmente, allora, il Garante della protezione dei dati personali dovrebbe rivolgersi all'AGCOM per richiedere un ordine di contrasto ai contenuti illegali.

Dall'altro lato, volendo indagare fonti della disciplina della Data Protection, neanche il GDPR offre alcuna soluzione al problema dell'enforcement dei provvedimenti delle autorit  nazionali e pertanto sembra esserci un vero e proprio vuoto normativo.

Tale gap   stato pure riscontrato dall'EDPB, che il 12 settembre 2025 ha pubblicato il testo, sottoposto ora a consultazione pubblica, delle linee guida 3/2025 circa l'interazione tra il GDPR e il DSA. Tra i temi affrontati vi   proprio quello della cooperazione tra i coordinatori dei servizi digitali, la Commissione europea e le autorit  di protezione dei dati, anche nel caso in cui queste ultime non siano designate come autorit  coordinatrici dei servizi digitali a livello nazionale.

Infatti, l'EDPB riconosce la cooperazione come elemento fondamentale per garantire un'applicazione coerente del DSA e del GDPR.

Tuttavia, l'EDPB non individua soluzioni pratiche al problema dell'enforcement di provvedimenti emessi da una autorità nazionale diversa dal coordinatore dei servizi digitali, lasciando agli Stati membri il compito di individuare meccanismi di cooperazione efficaci che consentano di razionalizzare il lavoro dei diversi attori che potrebbero dover intervenire nei contesti contemplati dal DSA. Nel frattempo, emergono anche i profili di rilevanza per l'impiego della piattaforma da parte dei "deployer", nell'ambito delle cui attività si facesse uso della chatbot, per volontà aziendale o per scelta più o meno meditata dei dipendenti (si pensi, ad esempio, alla condivisione di dati personali, magari in contesti delicati come quello lavorativo o sanitario).

Ci sembra di poter rilevare che, a tale riguardo, fare uso di una chatbot della cui affidabilità il Garante della protezione dei dati personali dubiti, possa comportare una responsabilità diretta per i deployer sotto la cui autorità viene utilizzata, salvo il caso di utilizzo per scopi personali.

Infatti, secondo l'approccio risk based dell'AI Act e del GDPR, e nell'ambito della accountability da essi implicata, in caso di danni o pregiudizi che possano verificarsi in conseguenza dell'inserimento su DeepSeek di dati personali o di altri materiali protetti, si incorre in una responsabilità nei confronti degli interessati, degli autori e, se in contesto lavorativo, dell'azienda e dei dipendenti.

Inoltre, ai sensi dell'articolo 4 dell'AI Act che stabilisce l'obbligo di una "AI literacy" del personale, una responsabilità potrebbe sorgere anche per omissione, qualora non siano stati adeguatamente formati i dipendenti e non siano state illustrate le pratiche di AI vietate.

In conclusione, restano aperte questioni di grande rilevanza, che evidentemente non si pongono soltanto nei confronti di DeepSeek ma possono riguardare anche altre piattaforme: è davvero possibile regolare in modo efficace l'accesso a un servizio digitale offerto dall'estero e raggiungibile con pochi clic? Quali strumenti hanno le autorità europee per far rispettare le regole europee a società stabilite fuori dalla UE, talvolta anche prive di sede o rappresentanza nel territorio UE?