AVVERA SRL SB

NEWSLETTER 2025

AGOSTO

AI, CONCORRENZA E PRIVACY: IL CASO META AI E IL NUOVO ASSE TRA GARANTE E ANTITRUST

MICROSOFT 365 E COMMISSIONE UE: UN CASO CONCRETO DI COMPLIANCE E SUPERVISIONE EFFICACE

NYT VS OPENAI: COPYRIGHT, PRIVACY E FREE RIDING NELL'ERA DELL'IA GENERATIVA

INTELLIGENZA ARTIFICIALE E REFERTI MEDICI: COME GESTIRE I RISCHI PRIVACY IN AMBITO SANITARIO

OPENAI RILASCIA I SUOI NUOVI MODELLI OPEN-WEIGHT: COSA CAMBIA DAVVERO PER L'AI, PER LE IMPRESE E PER LA COMPLIANCE.

AVVERA | SB Società Benefit

AI, CONCORRENZA E PRIVACY: IL CASO META AI E IL NUOVO ASSE TRA GARANTE E ANTITRUST

Il 29 luglio 2025 l'Autorità Garante della Concorrenza e del Mercato (AGCM) ha comunicato di aver dato avvio a un procedimento istruttorio nei confronti del gruppo Meta (Meta Platforms Ireland Limited, WhatsApp Ireland Limited e Facebook Italy srl) per presunto abuso di **posizione dominante**, legato all'integrazione dell'assistente algoritmico **Meta AI** su WhatsApp.

L'indagine italiana, condotta in cooperazione con la Commissione europea, non è solo uno dei primi casi di applicazione delle norme antitrust in ambito IA, ma rappresenta un caso emblematico che evidenzia come la tutela della concorrenza e quella della privacy non possano più essere trattate separatamente.

Quando la regolazione incrocia l'intelligenza artificiale

Dal marzo 2025, gli utenti italiani di WhatsApp hanno trovato una novità nell'app: l'icona multicolore di **Meta AI**, il chatbot basato sul modello LLaMA 4 di Meta, posizionata nella barra di ricerca. Questa integrazione è avvenuta **senza richiesta esplicita né attivazione volontaria da parte dell'utente**, secondo quanto rilevato dall'AGCM.

L'Autorità contesta a Meta una pratica nota come **tying**: l'imposizione congiunta di due servizi distinti – WhatsApp e Meta AI – senza offrire la possibilità di accettarli separatamente. Si tratta di una condotta che può configurare una **violazione dell'articolo 102 del Trattato sul funzionamento dell'Unione europea (TFUE)**, che vieta gli abusi di posizione dominante.

Il nodo centrale è che **WhatsApp e Meta AI rispondono a funzioni molto diverse**: la prima è una piattaforma di messaggistica, la seconda un servizio di intelligenza artificiale generativa. Forzare il passaggio da uno all'altro, senza scelta effettiva, può alterare le regole del gioco concorrenziale e cristallizzare posizioni dominanti nel nascente mercato dell'IA conversazionale.

Privacy e concorrenza: due facce della stessa medaglia

Oltre al profilo antitrust, l'indagine tocca anche aspetti rilevanti in termini di **protezione dei dati personali**. L'AGCM segnala **dichiarazioni contraddittorie da parte di Meta** circa l'utilizzo delle conversazioni gestite da Meta AI: da un lato si afferma che non verranno impiegate per migliorare i modelli, dall'altro si ammette l'opposto nei documenti ufficiali.

Se confermato, ciò implicherebbe **una raccolta non trasparente dei dati degli utenti**, usata per affinare il servizio, consolidando ulteriormente il vantaggio competitivo di Meta. Si entra quindi in un territorio dove **antitrust e privacy si sovrappongono**, proprio come previsto dal protocollo d'intesa firmato dalle due Autorità italiane.

Un nuovo equilibrio tra potere economico e diritto

Il 29 luglio 2025, l'Autorità Garante della Concorrenza e del Mercato (AGCM) e il Garante per la protezione dei dati personali hanno sottoscritto un protocollo d'intesa triennale con l'obbiettivo di costruire una collaborazione strutturata nei casi in cui il trattamento dei dati personali e le dinamiche concorrenziali si intersecano, come sempre più spesso accade nel contesto dell'intelligenza artificiale e delle piattaforme digitali.

La firma del **protocollo tra AGCM e Garante Privacy** segna un passaggio strategico per la governance digitale italiana ed europea, prevedendo:

- lo **scambio reciproco di informazioni** su casi e indirizzi strategici,
- la **segnalazione di violazioni incrociate** emerse nei rispettivi procedimenti,
- la **realizzazione di indagini congiunte** e la possibilità di elaborare **proposte comuni a Parlamento e Governo**,
- l'istituzione di un **tavolo tecnico permanente**, formato dai responsabili degli uffici, per armonizzare metodologie e approcci operativi.

L'iniziativa punta quindi a superare la storica frammentazione tra ambiti regolatori e a sviluppare **un presidio congiunto sull'economia digitale**, fondato su visione integrata e tempestività d'azione in uno scenario digitale in cui le piattaforme globali, attraverso dati e algoritmi, tendono a espandere il proprio potere trasversalmente a più mercati.

Conclusione

Per le imprese che operano nei mercati digitali, Il caso Meta AI ci ricorda che **l'integrazione dell'intelligenza artificiale nei servizi digitali non è (più) un terreno libero da regole.** L'attenzione delle Autorità si sta spostando dai modelli economici tradizionali alle dinamiche algoritmiche, e questo richiede alle imprese una nuova capacità di visione regolatoria.

Le aziende tech – ma anche tutte le realtà che sviluppano o integrano AI in prodotti e servizi – devono oggi **ripensare la governance digitale in modo trasversale:** dalla progettazione della UX, alla gestione del consenso, fino alla valutazione degli impatti sulla concorrenza.

Non basta più "essere a norma": serve adottare un approccio **proattivo**, dove la **compliance diventa anche leva competitiva**. In un contesto in cui privacy, fiducia e libertà di scelta tornano al centro, chi saprà anticipare le richieste dei regolatori potrà giocare d'anticipo anche sul mercato.

AVVERA | SB Società Benefit

MICROSOFT 365 E COMMISSIONE UE: UN CASO CONCRETO DI COMPLIANCE E SUPERVISIONE EFFICACE

Negli ultimi anni, l'adozione di strumenti cloud da parte delle pubbliche amministrazioni europee ha sollevato interrogativi sempre più rilevanti in materia di protezione dei dati personali, in particolare quando si tratta di fornitori extra-UE. Il recente caso che ha coinvolto la Commissione europea e il Garante europeo della protezione dei dati (EDPS) sul servizio Microsoft 365 fornisce un esempio concreto di come si possano affrontare (e risolvere) le criticità in modo strutturato e conforme alla normativa europea.

Un'indagine iniziata nel 2021, conclusa nel 2025

Nel 2021 l'EDPS ha avviato un'indagine sul modo in cui la Commissione europea utilizzava la suite Microsoft 365, rilevando nel marzo 2024 diverse violazioni al Regolamento (UE) 2018/1725, il testo che disciplina il trattamento dei dati personali da parte delle istituzioni, organi e organismi europei.

Le criticità riguardavano in particolare:

- la mancanza di una chiara limitazione delle finalità del trattamento;
- l'insufficiente controllo sui trasferimenti di dati verso Paesi terzi;
- il rischio di disclosure non autorizzate di dati personali da parte del fornitore o dei sub-responsabili del trattamento.

A seguito dell'adozione di specifiche misure correttive e di un lungo confronto tra Commissione ed EDPS, il Garante ha ufficialmente chiuso il procedimento l'11 luglio 2025, attestando l'avvenuta conformità.

Le misure di adeguamento adottate dalla Commissione: controllo, trasparenza, limitazione

La Commissione europea ha dimostrato, anche grazie al supporto del fornitore, che è possibile riportare l'utilizzo di una piattaforma globale come Microsoft 365 entro i confini di una governance pienamente conforme al diritto europeo.

Il percorso verso la compliance si è concretizzato attraverso un insieme articolato di interventi tecnici, organizzativi e contrattuali, di cui riportiamo gli aspetti più rilevanti:

- Limitazione delle finalità: la Commissione ha definito in modo dettagliato i tipi di dati trattati e gli scopi legittimi del trattamento, vincolando Micro-

soft e i suoi sub-responsabili ad agire esclusivamente su istruzioni documentate e per finalità pubbliche chiaramente identificate.
- Controllo sui trasferimenti internazionali: sono stati individuati i destinatari e gli scopi ammissibili per eventuali trasferimenti al di fuori del SEE. Tali trasferimenti possono ora avvenire solo:
  - ◊ verso Paesi coperti da una decisione di adeguatezza,
  - ◊ oppure in via eccezionale per rilevanti motivi di interesse pubblico, ai sensi dell'art. 50(1)(d) del Regolamento.
- Clausole rafforzate su disclosure e notifiche: nuove clausole contrattuali vietano a Microsoft di divulgare dati o omettere notifiche alla Commissione, salvo obbligo legale imposto da normative dell'UE, degli Stati membri o – se trattasi di dati trattati fuori dal SEE – da ordinamenti esteri con protezioni equivalenti.

Un contratto che fa scuola (e non solo per la Commissione)

Il nuovo accordo di licenza interistituzionale con Microsoft è stato reso disponibile anche per le altre istituzioni e agenzie dell'Unione Europea. L'EDPS ha espressamente incoraggiato gli altri enti a effettuare valutazioni simili e ad adottare misure tecniche e organizzative equivalenti.

Questo approccio cooperativo, che valorizza sia la funzione di supervisione dell'EDPS sia il ruolo proattivo della Commissione come lead contracting authority, rappresenta un modello concreto di governance pubblica nella gestione di servizi digitali critici.

Cosa significa per le imprese e gli enti pubblici

Questo caso offre spunti di riflessione anche per il settore privato e per le amministrazioni nazionali e locali:
- È possibile ottenere livelli avanzati di compliance contrattuale e tecnica anche da fornitori globali, se si dispone di una governance negoziale consapevole.
- I rischi legati a trasferimenti internazionali, sub-responsabili del trattamento e ambiguità nelle finalità possono essere mitigati con strumenti adeguati.
- La collaborazione con le Autorità di controllo non va vissuta solo come un obbligo, ma come un'opportunità per rafforzare trasparenza, affidabilità e sicurezza nella propria infrastruttura digitale.

Conclusione

La vicenda Commissione UE/Microsoft rappresenta un importante precedente per la regolazione dei servizi digitali nell'ambito europeo. In un contesto in cui l'adozione di strumenti cloud e soluzioni di intelligenza artificiale è in rapida espansione, la conformità ai principi fondamentali della protezione dei dati personali non può essere un elemento accessorio, ma deve diventare parte integrante della strategia tecnologica di ogni organizzazione.

AVVERA | SB Società Benefit

NYT VS OPENAI: COPYRIGHT, PRIVACY E FREE RIDING NELL'ERA DELL'IA GENERATIVA

La controversia tra il *New York Times* e OpenAI si colloca al centro di un dibattito globale sulle responsabilità legali e gli obblighi delle imprese che sviluppano intelligenza artificiale generativa.

Il procedimento giudiziario avviato nel dicembre 2023 presso la Corte Distrettuale di Manhattan, oltre ad affrontare il nodo della violazione del copyright, solleva rilevanti questioni legate alla privacy, alla concorrenza e al rapporto tra giurisdizioni internazionali.

Le origini della causa: l'uso non autorizzato dei contenuti giornalistici

Il New York Times ha citato in giudizio OpenAI accusandola di aver utilizzato **milioni di articoli protetti da copyright** per addestrare i modelli linguistici di ChatGPT, in assenza di una licenza, e quindi in violazione della proprietà intellettuale.

La difesa di OpenAI si è fondata sul concetto di **fair use**, sostenendo che l'uso fosse trasformativo e quindi legittimo secondo la giurisprudenza statunitense. Secondo l'azienda, le risposte di ChatGPT non copierebbero letteralmente gli articoli, ma ne rielaborerebbero i contenuti attraverso processi statistici.

Tuttavia, il Times ha presentato numerosi esempi di output del modello che riproducono interi articoli in modo quasi letterale, suggerendo un comportamento potenzialmente lesivo dei diritti di autore.

Il fondamento delle accuse e il tema del free riding

Il perimetro del processo, si concentra sulle **presunte violazioni del diritto d'autore** e sulla responsabilità indiretta delle piattaforme nel facilitare l'accesso a contenuti generati ma simili a quelli originali.

Fondamentale è la decisione del 26 marzo 2025 con cui il giudice federale **Sidney Stein**, ritenendo che le prove fornite dal New York Times fossero sufficienti per proseguire il giudizio, ha respinto la richiesta di archiviazione presentata da OpenAI, mentre ha accolto parzialmente la mozione della convenuta con riferimento a contestazioni minori di concorrenza sleale e interferenze contrattuali.

Le contestazioni minori fanno riferimento all'accusa di **free riding** mossa dal New York Times, che sostiene che OpenAI abbia costruito un prodotto commerciale competitivo, attraverso abbonamenti, integrazioni e prodotti business, sfruttando il lavoro giornalistico altrui, senza licenza.

Questa accusa è uno dei punti più sensibili, anche in vista di una possibile monetizzazione dell'IA basata su contenuti non retribuiti, e sta sollevando interrogativi sulla **leale concorrenza, la sostenibilità del giornalismo e la necessità di nuovi modelli di redistribuzione del valore nell'ecosistema IA.**

Alcune imprese, come OpenAI stessa, stanno già correndo ai ripari, stipulando **accordi di licenza** con editori globali (Associated Press, Axel Springer, Le Monde), ma resta aperta la questione di come regolamentare strutturalmente questo fenomeno.

L'ordine di conservazione dati: un rischio per la privacy globale

Un altro dei punti più sensibili della vicenda, riguarda l'ordine di **preservation** richiesto dal New York Times ed emesso il 13 maggio 2025 dal giudice **Ona T. Wang**, che obbliga OpenAI a **non cancellare alcuna conversazione o contenuto generato** da ChatGPT o tramite le sue API, nemmeno quelli già eliminati dagli utenti o che sarebbero stati automaticamente rimossi entro 30 giorni, come previsto dalla privacy policy.

L'ordine e si applica a **tutti gli utenti globali**, salvo eccezioni contrattuali come ChatGPT Enterprise o API con Zero Data Retention e ha effetto **indefinito** ("fino a nuovo ordine del tribunale").

L'obiettivo è evitare che potenziali prove — come l'output generato da ChatGPT che riproduce articoli del Times — vengano accidentalmente o automaticamente eliminate prima della fine del processo.

Tutto ciò comporta che l'azienda dovrà conservare **tutti i dati generati da ChatGPT e API**, compresi quelli già eliminati, **senza alcuna scadenza temporale predefinita.**

OpenAI ha reagito duramente, definendo l'ordine:

- **Invasivo** della privacy degli utenti;
- **Incompatibile con il GDPR**, che impone la limitazione temporale nella conservazione dei dati personali (art. 5.1.e);
- **In conflitto con gli impegni contrattuali e reputazionali** dell'azienda verso i suoi clienti.

L'ordine è stato impugnato davanti alla Corte Distrettuale, ma resta al momento in vigore.

Riflessione in merito alle implicazioni europee

L'ordine ha sollevato **gravi criticità sul piano della protezione dei dati personali**, specie per gli utenti europei tutelati dal **GDPR**.

In **Europa**, il GDPR e le direttive sul diritto d'autore (come la Direttiva Copyright 2019/790) pongono limiti precisi all'uso di dati personali e contenuti protetti per finalità di addestramento algoritmico.

Considerate le modalità, gli effetti e le finalità perseguite dall'ordine, rilevano alcune incompatibilità con la normativa europea:

- **Durata indefinita e principio di limitazione della conservazione (art. 5.1.e GDPR):** conservare dati a tempo indeterminato — anche se cancellati dagli utenti — viola il principio secondo cui i dati devono essere trattenuti solo per il tempo necessario alle finalità dichiarate;
- **Base giuridica inadeguata (art. 6 GDPR):** l'ordine statunitense non è automaticamente riconosciuto come valida base giuridica in Europa. Un procedimento civile in una giurisdizione extra-UE non giustifica da solo un trattamento invasivo di dati personali globali;
- **Trasparenza e informazione (artt. 12-14 GDPR):** gli utenti europei non sono stati informati in modo chiaro dell'esistenza di questa retention forzata, né delle modalità di conservazione a scopo giudiziario.
- **Proporzionalità e minimizzazione (art. 5.1.c, art. 25 GDPR):** l'ordine appare sproporzionato rispetto alla finalità perseguita.

Conclusioni e prospettive future

Il caso New York Times vs OpenAI rappresenta un punto di svolta nel confronto tra tecnologia e diritti fondamentali. Non si tratta solo di stabilire se l'addestramento su contenuti protetti sia lecito, ma di **ridefinire gli equilibri tra innovazione, proprietà intellettuale e tutela della persona.** Il risultato potrebbe tracciare nuove linee guida globali per la governance dell'intelligenza artificiale generativa.

Mentre il contenzioso evolve, aziende e provider IA dovranno rafforzare la propria governance su copyright, data governance e compliance cross-border. Il rischio è che strumenti legali legittimi in un contesto locale abbiano **impatti globali non proporzionati** sul piano della privacy e dei diritti digitali.

INTELLIGENZA ARTIFICIALE E REFERTI MEDICI: COME GESTIRE I RISCHI PRIVACY IN AMBITO SANITARIO

L'utilizzo crescente di sistemi di Intelligenza Artificiale (IA) generativa per l'interpretazione di referti medici rappresenta una sfida importante per la tutela della privacy e della sicurezza dei dati sanitari. Il Garante per la Protezione dei Dati Personali ha recentemente lanciato un allarme sui rischi connessi a questa pratica, invitando a un uso consapevole e regolamentato di tali tecnologie.

È sempre più diffusa, infatti, la prassi di caricare analisi cliniche, radiografie e altri referti medici su piattaforme di IA generativa per ottenere diagnosi o interpretazioni. Tuttavia, queste piattaforme spesso non sono progettate né autorizzate come dispositivi medici, e ciò può comportare rischi elevati per la salute e la privacy delle persone.

Rischio di perdita di controllo sui dati sanitari

I dati sanitari sono informazioni che riguardano la salute fisica o mentale di una persona, come diagnosi, terapie ed esami. La loro diffusione o uso improprio può causare discriminazioni, danni alla reputazione e al benessere personale. Per questo il GDPR prevede una protezione rafforzata, imponendo regole stringenti sul loro trattamento, che deve sempre garantire sicurezza, trasparenza e rispetto dei diritti dell'interessato.

Prima di caricarli su piattaforme di IA, è fondamentale verificare le informative sulla privacy fornite dai gestori dei servizi per capire se e come i dati verranno trattati:

- Saranno cancellati dopo l'uso?
- Oppure conservati per l'addestramento degli algoritmi?

La trasparenza è un elemento chiave per garantire il controllo dei dati personali.

La supervisione umana qualificata: un requisito imprescindibile

Il Garante Privacy e il Regolamento europeo sull'IA (AI Act, art. 14) sottolineano che l'uso di sistemi di IA in ambito sanitario deve prevedere sempre una supervisione umana qualificata da parte di professionisti medici.

La supervisione umana non si limita all'utilizzo clinico finale, ma si estende a tutto il ciclo di vita del sistema di IA: dallo sviluppo e progettazione, passando per l'addestramento degli algoritmi, fino ai test e alla validazione pre-implementazione. Solo con questa presenza qualificata è possibile identificare e correggere tempestivamente eventuali errori, evitare diagnosi errate e ridurre i rischi per la salute dei pazienti.

Inoltre, la supervisione medica garantisce che le decisioni basate sull'IA siano sempre integrate con il giudizio clinico e il contesto individuale del paziente, evitando un affidamento esclusivo e potenzialmente pericoloso a risposte generate automaticamente. Questo approccio coniuga il potenziale innovativo dell'IA con la responsabilità e la tutela della persona, elementi fondamentali in ambito sanitario.

Obblighi normativi fondamentali

L'uso di sistemi di IA in ambito medico richiede il rispetto di rigorosi obblighi di compliance, fondamentali per la protezione dei dati personali. In primo luogo, il trattamento dei dati sanitari deve basarsi su un presupposto di liceità solido, come previsto dagli articoli 6 e 9 del GDPR, garantendo che i dati siano gestiti in modo legittimo e trasparente.

È inoltre obbligatoria una valutazione d'impatto sulla protezione dei dati (DPIA) preventiva, che consente di identificare e mitigare i rischi per i diritti degli interessati fin dalle fasi iniziali del progetto.

Gli utenti devono essere informati con chiarezza sulle finalità e modalità del trattamento, rispettando gli obblighi di trasparenza per assicurare un'informazione completa e accessibile.

Infine, devono essere adottate misure di sicurezza adeguate, come crittografia e controlli di accesso, per proteggere i dati da accessi non autorizzati, perdite o alterazioni, garantendo così riservatezza e integrità delle informazioni.

Questi obblighi sono essenziali per tutelare i diritti delle persone e assicurare un utilizzo responsabile e affidabile dell'IA in ambito sanitario.

Attenzione alla raccolta massiva di dati (web scraping)

Un rischio significativo connesso all'uso dell'intelligenza artificiale riguarda la raccolta massiva di dati personali da fonti online tramite pratiche di web scraping. Questa modalità di acquisizione automatica di grandi quantità di informazioni può facilmente violare i principi fondamentali del GDPR, quali la minimizzazione dei dati, la liceità del trattamento e la trasparenza verso gli interessati.

In particolare, raccogliere dati sanitari o altre informazioni sensibili senza un valido fondamento giuridico o senza informare gli interessati comporta gravi rischi di non conformità e può compromettere la tutela della privacy delle persone coinvolte. Per questo motivo, sviluppatori di sistemi IA e operatori del settore sanitario devono adottare misure rigorose per garantire che i dati impiegati per l'addestramento degli algoritmi siano acquisiti, trattati e conservati nel pieno rispetto delle normative vigenti.

Conclusioni e raccomandazioni

L'adozione di sistemi di IA in ambito medico offre opportunità significative, ma comporta anche rischi rilevanti per la privacy e la sicurezza dei dati sanitari. Per minimizzare tali rischi, è indispensabile:

- Informare e sensibilizzare gli utenti sui limiti e pericoli dell'uso di IA generativa per diagnosi;
- Garantire la supervisione umana qualificata;
- Rispettare scrupolosamente gli obblighi normativi di protezione dati;
- Verificare con attenzione le informative privacy dei fornitori di IA;
- Evitare la condivisione indiscriminata di dati sanitari con piattaforme non certificate.

Solo attraverso un approccio integrato di compliance e governance si potrà garantire un uso sicuro e responsabile dell'intelligenza artificiale in ambito sanitario.

OPENAI RILASCIA I SUOI NUOVI MODELLI OPEN-WEIGHT: COSA CAMBIA DAVVERO PER L'AI, PER LE IMPRESE E PER LA COMPLIANCE.

Dopo oltre 5 anni di chiusura, OpenAI ha scelto di fare un passo significativo verso l'apertura. Lo scorso 5 agosto, l'azienda guidata da Sam Altman ha annunciato il rilascio dei suoi primi modelli linguistici **open-weight: gpt-oss-120b e gpt-oss-20b**. Una mossa che segna un'inversione di rotta rispetto al modello proprietario e centralizzato seguito con GPT-3 e GPT-4, accessibili solo via cloud e API.

La notizia ha avuto grande risonanza non solo nel mondo tech, ma anche in quello legale e aziendale, perché apre la strada a un'adozione più libera dell'intelligenza artificiale, con ricadute pratiche, normative e strategiche che meritano un'analisi attenta.

Dal cloud al controllo locale: cosa cambia

Con questo rilascio, OpenAI mette a disposizione due modelli linguistici di grandi dimensioni – 120 e 20 miliardi di parametri – che possono essere **scaricati ed eseguiti localmente**. Significa che sviluppatori, imprese, centri di ricerca o startup potranno utilizzare l'intelligenza artificiale senza passare per le infrastrutture cloud di OpenAI.

Ciò però non va a discapito delle prestazioni: Il modello gpt-oss-120b raggiunge prestazioni quasi equivalenti a OpenAI o4-mini nei principali benchmark di ragionamento, garantendo un'esecuzione efficiente su una singola GPU da 80. Il loro addestramento si basa su un mix di apprendimento per rinforzo e tecniche informate dai modelli interni più avanzati di OpenAI, tra cui o3.

Non è un ritorno completo all'open source nel senso classico del termine: i modelli sono "open-weight", ovvero con pesi accessibili ma con licenze d'uso specifiche. Il rilascio sotto la licenza permissiva Apache 2.0 ne consente l'ampio utilizzo commerciale, la modifica e la ridistribuzione. La portata della decisione è comunque significativa. Si tratta di un gesto che va nella direzione di **una maggiore trasparenza, autonomia e controllo** da parte degli utenti, in un contesto sempre più attento alla governance e alla sovranità tecnologica.

Un'apertura che sa di strategia

Per capire il peso di questa scelta, basta ricordare che OpenAI aveva interrotto la pubblicazione dei modelli open dopo GPT-2, nel 2019, citando rischi di abuso e necessità di controllo. Ora, con gpt-oss, l'azienda sembra voler rispondere a più spinte contemporaneamente: la pressione della comunità open source, l'ascesa di concorrenti più "aperti" (come Meta, DeepSeek, Alibaba), e una crescente richiesta di trasparenza anche da parte dei legislatori.

Il contesto geopolitico non è secondario. L'AI è oggi terreno di confronto tra modelli politici ed economici diversi. E che le scelte tecniche hanno, inevitabilmente, anche **implicazioni culturali, industriali e regolatorie.**

Opportunità concrete per aziende e sviluppatori

Sul piano pratico, i vantaggi sono evidenti. Avere un modello potente che può girare localmente consente di sviluppare:

- soluzioni AI **on-premise**, ideali per settori sensibili o regolati (sanità, legale, finance);
- applicazioni che rispettano il principio della **privacy-by-design**, trattando i dati direttamente sul dispositivo;
- strumenti capaci di funzionare anche **offline**, ad esempio in ambienti ad alta sicurezza o a connettività limitata;
- sistemi completamente **personalizzabili**, tramite tecniche di fine-tuning, per rispondere a esigenze molto specifiche.

Questi scenari, finora possibili solo con tool open source di terze parti o con forti compromessi prestazionali, diventano ora accessibili anche con modelli del calibro di quelli sviluppati da OpenAI.

Ma cosa comporta tutto questo dal punto di vista legale?

La maggiore libertà tecnica porta con sé **nuove responsabilità giuridiche.** L'esecuzione e la modifica di modelli AI su sistemi locali richiede attenzione su più livelli: **responsabilità degli output, gestione dei dati personali, conformità alle licenze, sicurezza operativa.**

Controllo significa responsabilità

Se con i modelli in cloud l'onere della sicurezza e della qualità è in parte delegato al fornitore (OpenAI, in questo caso), l'esecuzione locale ribalta la prospettiva. Chi scarica e utilizza un modello gpt-oss diventa il principale responsabile degli usi, degli abusi e delle conseguenze dei suoi output.

Questo implica la necessità di:

- implementare **meccanismi di monitoraggio e auditing degli output generati;**
- stabilire chi controlla e verifica i prompt, soprattutto in ambito aziendale;
- gestire il rischio di "allucinazioni" o risposte scorrette in contesti professionali o regolati.

Nel quadro del nuovo **AI Act europeo**, i modelli general purpose ad alto impatto – anche se open-weight – potrebbero comunque essere soggetti a obblighi di trasparenza, documentazione tecnica e governance.

Dati personali e trattamento locale: più sicuro, ma non esente da rischi

Il fatto che un modello venga eseguito in locale non esclude affatto gli obblighi imposti dal GDPR. Anzi, in certi casi, li amplifica.

Qualsiasi trattamento di dati personali, anche tramite AI offline, richiede:

- una valutazione di impatto (DPIA) se c'è un rischio elevato per i diritti degli interessati;
- misure tecniche e organizzative adeguate (inclusa la pseudonimizzazione o l'anonimizzazione);
- una **base giuridica** chiara per il trattamento, soprattutto se l'AI analizza documenti, email, conversazioni o altri contenuti personali.

L'autonomia tecnica non esonera dalla responsabilità normativa.

Attenzione alle licenze: non tutto è concesso

OpenAI ha scelto di rilasciare i modelli gpt-oss con licenze proprie, diverse da quelle OSI o Creative Commons. Questo significa che, prima di integrarli in un prodotto o servizio, è necessario:

leggere attentamente le clausole sulle limitazioni d'uso (es. restrizioni per armi, frodi, disinformazione);
verificare i diritti di riutilizzo e redistribuzione;
valutare le condizioni relative alla modifica e al fine-tuning del modello.
La mancata compliance con le licenze può comportare rischi legali concreti, anche in termini di responsabilità contrattuale o di violazione della proprietà intellettuale.

Verso un'AI più accessibile, ma anche più complessa da gestire

L'apertura dei modelli gpt-oss rappresenta una **nuova fase nel rapporto tra imprese**, AI e diritto. Più potere decisionale (e operativo) agli utenti significa anche più attenzione ai temi di compliance, sicurezza e responsabilità.

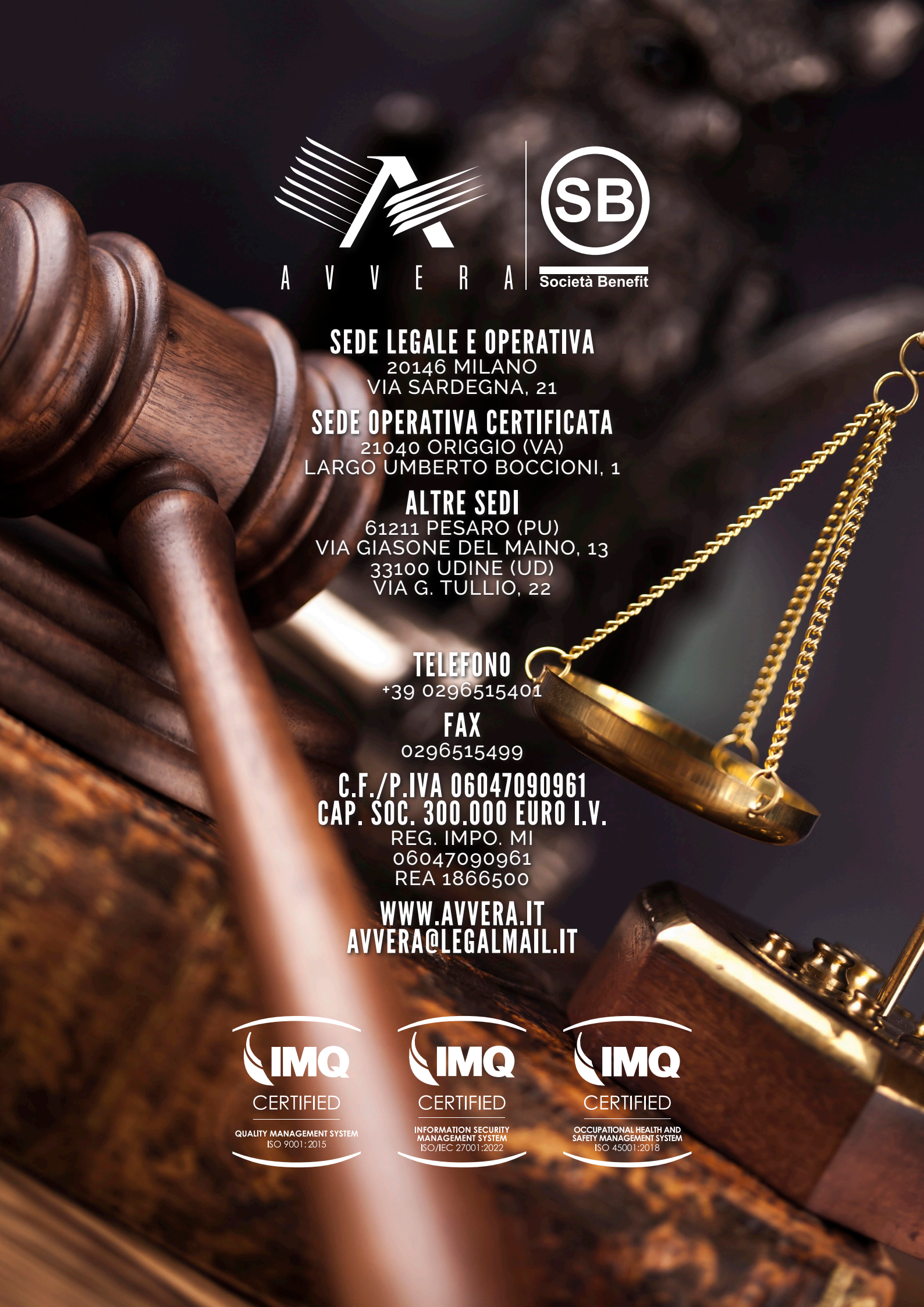
In questo scenario, le organizzazioni devono dotarsi di strumenti adeguati: policy interne sull'uso dell'AI, procedure di valutazione del rischio, audit regolari, formazione per i team legali e tecnici.

In conclusione

Il rilascio dei modelli open-weight da parte di OpenAI è una notizia positiva per l'ecosistema dell'intelligenza artificiale: una maggiore apertura, flessibilità e spazio per l'innovazione, a cui però corrisponde un'esigenza a trattare l'AI **con consapevolezza legale e strategica.**

I modelli verranno condivisi su Hugging Face e su altre piattaforme, con il report tecnico, il documento sulla sicurezza, la scheda di sistema e le guide per gli sviluppatori per effettuare il fine-tuning in modo responsabile.

AVVERA | SB Società Benefit



AVVERA

Società Benefit

SEDE LEGALE E OPERATIVA
20146 MILANO
VIA SARDEGNA, 21

SEDE OPERATIVA CERTIFICATA
21040 ORIGGIO (VA)
LARGO UMBERTO BOCCIONI, 1

ALTRE SEDI
61211 PESARO (PU)
VIA GIASONE DEL MAINO, 13
33100 UDINE (UD)
VIA G. TULLIO, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

IMQ CERTIFIED
QUALITY MANAGEMENT SYSTEM
ISO 9001:2015

IMQ CERTIFIED
INFORMATION SECURITY MANAGEMENT SYSTEM
ISO/IEC 27001:2022

IMQ CERTIFIED
OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM
ISO 45001:2018